

Forensic analysis of Mobile device and Social Media:

To make an impact in the area of cybercrime

BY

Debanjana Saha

ID- 152-15-5696

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Dr. Fernaz Narin Nur

Assistant Professor

Department of CSE

Daffodil International University

Co-Supervised By

Ms. Nazmun Nessa Moon

Assistant Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY DHAKA, BANGLADESH

APPROVAL

This Project titled “**Forensic analysis of social media & cybercrime: To make it more impactful**”, submitted by Debanjana Saha to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain

Professor and Head

Department of CSE

Faculty of Science & Information Technology Daffodil

International University

Chairman

Dr. Sheak Rashed Haider Noori

Associate Professor and Associate Head

Department of CSE

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Md. Zahid Hasan

Assistant Professor

Department of CSE

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Dr. Mohammad Shorif Uddin

Professor

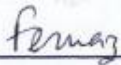
Department of Computer Science and Engineering Jahangirnagar University

External Examiner

DECLARATION

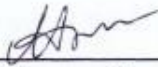
I hereby declare that; this project has been done by us under the supervision of **Dr. Fernaz Narin Nur, Assistant Professor, Department of CSE**, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for an award of any degree or diploma.

Supervised by:



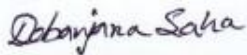
Dr. Fernaz Narin Nur
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised by:



Ms. Nazmun Nessa Moon
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:



Debanjana Saha
ID-152-15-5696
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty GOD for his divine blessing makes us possible to complete our final year project successfully. But there are others, without their support, encouragement, and appreciation we would not be able to bring our project into the light of success. We, from the core of our heart, want to thank them all.

We want to thank our honorable **Supervisor Dr. Fernaz Narin Nur, Assistant Professor**, Department of Computer Science & Engineering, Daffodil International University. Deep knowledge and keen interest of our supervisor in the field of “Networking & cybersecurity” to carry out this project. Her endless patience, encouragement, expert advice and above all his friendly behavior towards us have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain, Professor and Head**, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

Next, we must thank and acknowledge our university, Daffodil International University. We also want to thank our beloved classmates and other students of the university who took part in the research purpose for our project and appreciated our work.

Lastly, we want to thank our beloved families, who were always by our side and kept faith in us. Without our family support, we could never be here, we cordially thank them for this. We also thank our friends for their support and help to us.

ABSTRACT

In this research work, we are focusing to do a digital forensic analysis of social media through mobile devices to determine the main criminal. We considered accused people mobile device as the main evidence of cybercrime and tried to find out is this accused person is really a criminal or not. The find out is the probability of being a criminal. Here the main data is the deleted file and the keywords of the social media what we will get after the forensic analysis of the mobile device. It will also make further development to find out the main culprits in the investigation of cybercrime. We are trying to propose a better develop way in the forensic analysis by which we can do our forensic analysis in less time. Like using the time stamps to determine when there is most probably to occur a crime. For example, most of the cybercrime happens on the weekends. We are doing our investigation using the cookies and the logical image of the device which is left behind by the cybercriminals.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	ii
Declaration	iii
Acknowledgement	iv
Abstract	v
 CHAPTER 1: INTRODUCTION	 01-04
1.1 Introduction	01
1.2 Motivation	02
1.3 Objectives	03
1.4 Expected Outcome	03
1.5 Report Layout	04
 CHAPTER 2: BACKGROUND STUDY	 05-08
2.1 Introduction	05
2.2 Literature Review	05
2.3 Research Summery	07
2.4 Scope of the Problem	08
2.5 Challenges	08
 CHAPTER 3: RESEARCH METHODOLOGY	 09-18
3.1 Introduction	09
3.2 Creating Zone for measuring probability	09
3.2.1 Green Zone	09
3.2.2 Yellow Zone	10
3.2.3 Red Zone	11

Timestamp of using social network of a criminal	12
Steps for Digital Forensics	12
Collection phase	12
Examination phase of the collected data	12
Analysis phase after examination of the data	13
Reporting of all the information	13
File System Forensics	14
Steps needed for Storage Media Investigation	14
Data Mining for Digital Forensics	15
Data Mining Algorithm for Data set calculation the probabilities	16
Proposed digital forensic tool	17
 CHAPTER 4: DESIGN, IMPLEMENTATION	 19-27
AND TESTING	
Introduction	19
Using data cable to connect the device	19
Analyzing result of memory card and Imaging device	20
Recovered Documents	22
Recovered images	22
History of the device	23
Browser history	23
Search History	23
Confusion matrix of collected data	24
Class accuracy	25
Trained Data of the data set	25
Run time information	26
 CHAPTER 5: CONCLUSION AND IMPLIATION	 28-30
FOR FUTURE RESEARCH	
Conclusion	28
Implication for Future Study	28

REFERENCES	29
APPENDICES	30

LIST OF FIGURES

FIGURES	PAGE NO
Figure 3.1: Showing a green zone based on search keywords	10
Figure 3.2: Showing a yellow zone based on search keywords	11
Figure 3.3: Showing a green zone based on search keywords	11
Figure 3.4: The digital forensic investigation processes	13
Figure 3.5: Block diagram of proposed system	18
Figure 4.1: Examined mobile device & info screen	19
Figure 4.2: Screen Showing “Mount” request	20
Figure 4.3: Drive Selection for the device to connect FTK	21
Figure 4.4: FTK Imager is showing the result screen.	21
Figure 4.5: Retrieved Images from the deleted file	23
Figure 4.6: Browser history	23
Figure 4.7: Search history	24
Figure 4.8: Confusion matrix of collection data	24
Figure 4.9: Accuracy by class of the data	25
Figure 4.10: Describing the data set after training	26
Figure 4.11: Run time information	27

CHAPTER 1

INTRODUCTION

Introduction

Digital Forensics is one of the trustworthy investigation processes in the field of cybercrime, typically it is co-related to computer crime. It mostly works with the evidence we found in the accused device. Computer forensics or digital forensic also known as cyber forensics. It includes applying computer examination and investigation systems to illuminate a criminal offense and supply verification to help a case. This is the method of distinguishing, conserving, analyzing and offering the digital proof in such a fashion that the evidence is lawfully acceptable. By using cyber rhetorical tools it's terribly straightforward to probe the evidence. It involves numerous applications like analyzing the standard of food and predicting the hearth disasters etc. Most of the primary criminal cases that concerned computers were for money frauds that are currently overcome by Biometric revolving credit. Energizing cybersecurity with statistics & Digital Forensics. Biological proof conjointly plays a major role in crime investigation. It contains Deoxyribose macromolecule (DNA), that connects associate degree bad person to a criminal offense scene. It examines proof from crime scenes to determine if biological material is a gift. Biological traits include fingerprint, hair, Olfactory, teeth, palm veins, DNA, skin, bones, blood, nails, exhaled breath, etc. Nowadays Digital forensics becoming the DNA test of cybercrime [1].

Numbers of cybercrimes in social media is increasing day by day. In 2013, the exchange lost quite \$130 billion in price due to one event. No, it wasn't a world crisis. War hadn't broken out. And, there have been no changes to financial or financial policies. Instead, digital image processing was attributed to one source: social media. Hackers picked up the board of the Twitter record of the Related Press partner degree report an erroneous "news story" that a bomb had been exploded inside the White House in Washington, D.C. The imaginary tale made the Dow drop a hundred and fifty, generally reminiscent of \$136 billion, however, it, in the end, bounced back [2]. This is one example of how social networks are used for

mischievous functions, and there are lots of others. Scammers used actor Robin Williams' death to encourage individuals to share a pretend video that ultimately caused a fake file to be downloaded to users' devices. Criminals on pretend Instagram accounts announce photos of supposed lottery winners, giving to share their bounty with anyone WHO followed their account. Once the account grew to a large following, the account house owners sold-out the account and every one of its followers to some other person. On Twitter, cybercriminals typically post malicious URLs that look legitimate in hopes of obtaining users to click - and later infect their devices. And so on. So, it is high time we should take some steps to make a change.

Motivation

The world is changing with the technologies and so the people. Criminals are also becoming smarter with the technologies and continuously finding a new way to hassle people. Cybercrime becoming the new threats to the whole world. Nowadays cybercrime getting a lot of attention. Those attentions prove that, in those recent years, the number of cyber crimes is increasing. We have much news to prove that, the number is increasing and very alarming for us. And these are not only online crimes, but also cost many people lost too much money. Worldwide cybercrime made a huge money loss. If we calculate this, it is an estimated \$600 billion USD a year. That is up from \$500 billion USD in 2014, the last time an antivirus company McAfee and assume tank the Center for Strategic and International Studies released a similar study. The new estimate amounts are to 0.8 percent of world GDP, up from 0.7 percent in 2014 [3]. Cybercrime is relentless, undiminished, and not going to stop. One of the most alarming parts of this is, it is very easy to do a crime via online, doesn't matter intentionally or without any intention. But it is very hard to prove them, and the rate of punishment is very low.

Let's take a appear at some of the most common sorts of cybercrimes impacting social media networks. The occurrence of social media utilization and the capacity to have interaction anonymously are two of the biggest motives why cybercrimes on social networking websites

have gone wild. Here are a few examples of the most famous sorts of assaults perpetrated on social media.

- Profile Hacking (Unusual interference to other's profile)
- Photo Morphing (Converting the photo)
- Offer and Shopping Scams (False link or offer)
- Romance and Dating Scams (Taking personal information)
- Link Baiting (Going to a website without any kind of search)
- Information Theft (Collection people's information without their concern)
- Cyber Bullying (Harassing or insulting people over the internet)
- Using it for other criminal work

These are the most occurred crimes nowadays in social media. Many criminals don't get any kind of punishment due to lack of evidence. I always have some interest to work against the cybercrime. To reduce the percentage and to let the criminal know, it is now not easy to go away after doing any crime in social media, I am working on these research work.

Objective

- The objectives of this project to find out and analyze a technique which can help in the investigation of cybercrime.
- Make people aware of cybercrime.
- Analyzing phone in proposed technics to find out evidence.
- Analyze the percentage of finding out the result of a person become cybercriminals introducing three Zone (Red, Green, Yellow)
- Make the investigation more effective

Expected Outcome

People are using social media and current digital techniques rapidly. Criminals are always targeting the general people. But people have very few ideas about how they can be careful and can be safe from this criminal. Most of the time the investigation lag behind due to insufficient evidence and lack of proper analysis of the digital device. This research work will give a proper direction in the investigation of a device and will give us better result in finding out the criminals.

Report Layout

Chapter 1: Introduction

In the introduction chapter, we have mentioned about the introduction of the topics, motivation of the work, goals and predicted the outcome of the challenging work and the document layout that we have worked for the full thesis work.

Chapter 2: Background Study

In the background chapter, we mentioned about the heritage state of our work, that actually describes the background work and the work history of this work. We also provide the literature study of various project scope and the summary of the work. Also tried to give an overview of the difficulties and challenges of the system.

Chapter 3: Thesis Methodology

The Thesis Methodology chapter is all about the technique used to construct the system. This area has the strategies and steps, the records collection procedure, some statistical evaluation of the proposed system.

Chapter 4: Experimental results and discussion

Experimental results and discussion chapter have all the experimental end result that has been executed with the aid of the proposed system is mentioned alongside the overall performance evaluation and a precis of the result is covered.

Chapter 5: Conclusions

Conclusions chapter contains the conclusion part and the ideas of the implication of further study on this topic. This chapter also containing the overall end result with the summary of this thesis work.

CHAPTER 2

BACKGROUND STUDY

Introduction

In this chapter, we talk about several numbers of lookup work accomplished via researchers in the vicinity of forensic evaluation of social media on the device.

Smartphones or anyone personal phone is very private properties of a person. People generally kept their mobile phones in their own surveillance. Phones kept in close bodily proximity to their owners. Mobile phones are one of the great parts, that is conceivable sources of digital evidence, like computers as people install and keep much personal information there. This is the reason why a mobile phone enhances the possible price of digital proof specially located on smartphones. An e-suspects might also interact with them always at some point of the day and may additionally take them or can use them to the crime scene. In addition if we want to keep traces of the suspect's communications, a suspect's phone may also comprise evidence that may be connected to their location, and with the introduction of the smartphone, they may additionally connect the same rich variety of digital evidence which may be observed on computer systems and can help lot in the field of digital evidence.

Literature Review

Mobile telephones and their functions are very important for their user. But there are many crimes that are done on a mobile phone. If we give a look there are a large range of crook cases, consisting of fraud, theft, money laundering, illicit distribution of copyrighted fabric or child pornographic images, or even distribution of malware in cybercrime instances [4]. Even before contemporary smartphones, SMS text messages saved in the GSM SIM card were a vital target for forensic examiners. With current smartphones, mobile functions conveying messaging functionality can also supplement or even supplant SMS, which means that there may also be a couple of message fountains on the telephone for inspectors to recover. The mainstream of new smartphones is transported with the Android consecutively system. There have been many ones of a kind method to the forensic acquisition of secondary storage of Android units in the literature because of 2009,

surrounding both logical and physical acquisition, with some strategies requiring greater conceivable modification to the Android device under examination than others [5].

The logical acquisition can be approved out on an Android system via a number of backup utilities and requires no amendment of the device or its gadget software. Physical acquisition strategies described in the literature, on the other hand, regularly require the setup of a rootkit (modifying the device's system partition) in order to facilitate full, get entry to the device's secondary storage for acquisition through a device like dd, as in Lessard and Kessler [6].

Meanwhile these rootkits are regularly of unidentified origin (in fact, they are most naturally traced from the hacking community), and considering that any change to a device under examination ought to be minimized if now not outright avoided, Vidas et al. proposed that the Android healing partition would perhaps be superior carefully overwritten with a recognized protected forensic boot surrounds to facilitate physical acquisition of the remaining partitions [7].

By doing so, the device divider is not adapted by way of the rootkit, however, full get admission to the device's secondary storage is got by way of rebooting the device into a modified recuperation mode incorporating the crucial software to operate a physical acquisition. This is comparable to how a boot CD would perhaps be used to enable forensic attainment on a pc system. From a wholeness viewpoint, physical acquisition is usually better to the logical acquisition, as a physical picture will include any information which exists in unallocated space, such as files that have been deleted but not but overwritten. Despite this, logical acquisition can nevertheless yield significant quantities of digital proof and is nonetheless employed in many types of research in the literature [8].

Mobile applications for famous instant messaging or social networking systems have been the problem of several research in digital forensics literature. Early work on instantaneous messaging applications on smartphones, such as Husain and Sridhar's find out about on the iPhone, examined platforms which have been at the start released for the Personal Computer (PC) moreover as a standalone application or by way of the web. Computer forensic policies are labeled in the literature for the examination of artifacts from AOL Instant Messenger (AIM) [9], different established on the spot messaging roles, web procurers for popular instant messaging functions [10], and immediately messaging features of social networking websites such as Facebook. As these immediately messaging structures from the PC world traveled to the smartphone with their

very own cellular applications, so did the digital forensics community move on to investigate endeavor traces left through these functions on cellular gadgets.

In addition to these imports from the PC, immediately messaging and social networking applications have been developed mainly for the smartphone. An instance of a cell messaging software is WhatsApp. Anglano examined WhatsApp on software-emulated. Android elements in current work supplying forensic examiners with information about what information is saved on the Android gadget by the WhatsApp application, facilitating the reconstruction of contact lists and text conversations [11].

Most of the functions examined in this work fall into the matching category as WhatsApp in that they are first and important smartphone applications, not PC port overs to Android. Given the popularity of smartphones, it is not stunning that they have become goals for cyber attacks. Smartphone malware is a developing concern, and the sheer volume of cellular purposes brings with it a plethora of achievable attack vectors. For example, Dimopoulos et al. developed malware which carried out DNS poisoning on the iPhone's tethering (also recognized as a private hotspot) feature and uncovered essential consumer facts (such as place and account credentials) when the person employed the Siri service. In their work on Android inter-application conversation and its attendant attack vulnerabilities, Chin et al. observed 1414 vulnerabilities in the top 50 paid and pinnacle 50 free applications then reachable for Android on what was then known as the Android Market. Instant messaging smartphone purposes are no exception, as proven by way of Schrittwieser et al. who examined a set of nine famous instantaneous messaging functions for Android and iPhone, and observed vulnerabilities to account hijacking, spoofing, unrequested SMS, enumeration or other assaults on all of them.

Research Summary

From all the research work we can understand that there is much information we kept in our phone such as our personal information professional information. It is the same for general people also the same for the people who have some intention to do any cybercrime. So, a mobile device is always good evidence in the field of forensic science. Their bad intention is a very bad risk to the other consumer. Consumer privacy is being violated by this criminal While some of these protection flaws might also aid the digital forensics community to get better extra digital proof from these devices, it is clear that the practical for the exploitation of these vulnerabilities via

malicious sellers will lead to greater incidents of cybercrime targeting mobile devices. Our work complements current literature by employing deleted files and digital forensics as well as machine forensics to provide a greater holistic view of what evidence may be obtained from messaging functions on Android devices. Our work also sheds a light on the conceivable privacy problems that arise from weak safety implementations in the examined applications and show the chance of an everyday consumer becoming cybercriminal.

Scope of The Problem

The scope of the proposed research work will always give a boost to the forensic analysis of the mobile device. Investigation of a mobile device sometimes miss out some small details which may be very important. For example, the deleted photos, the keywords suspected person search may give a new dimension to the investigation.

Challenges

Forensic analysis of a mobile phone is a hard thing for a student. Because most of the tool are not openly used and most of them are very private and confidential. Finding out the analyzing tool is one of the hardest parts of this research work to get a proper data set.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

In this chapter, we focused on the work and research methodology we make. We generally work on our method and focused on how we can make our method more flawless to make an impactful effect on the field of cybercrime. This method is describing how can we make the best use of the data, information, what we have received after the forensic analysis.

Creating a Zone for measuring the probability

In this research work First, we have worked on the phone. Forensic analysis of phone gave us the logical dd image of the phone. From the forensic analysis, we got the information of the deleted files, passwords, browser history, and search keywords in the different search browser. This information helps us to make the data set. With the keywords, we find out the probability of a suspected person in the danger zone. For example, here we work with three zone

1. Green Zone
2. Yellow Zone
3. Red Zone

Green Zone

In this research work, we work with three Zone. Green Zone stands for one of the probabilities of clean hearted person, who have no intention or any bad record of having a cybercrime. After analyzing the keywords, we get the result that if a person has no unethical work in his social networking site, he will be declared as a green zone people with a clean image. This type of person has a near to zero probabilities of becoming a cybercriminal. Figure 3.1 is showing the result we got after searching. The searched keyword belongs to the green zone. For that, it is showing the result of the green zone.



Figure 3.1: Showing a green zone based on search keywords

Yellow Zone

Yellow Zone stands for one of the probabilities of the mid-level person in the area of cybercrime. who have no some unethical work in his social networking site, which may not be a serious crime but have a possibility to convert into a serious crime intention or any bad record of having a cybercrime. It also can happen he can also become a clean hearted person. The main motto of creating this zone is to determine, who have possibilities to become both good and bad. So, it is the authority's responsibilities to bring him on the right path. After analyzing the keywords, we get the result that if a person has some unethical work in his social networking site, he will be declared as a yellow zone people. This type of person has a near to some probabilities of becoming a cybercriminal and also can become good. Figure 3.2 is showing the result we got after searching. The searched keyword belongs to the yellow zone. For that, it is showing the result of the yellow zone.



Figure3.2: Showing a yellow zone based on search keywords

3.2.2 Red Zone

Red Zone stands for one of the probabilities of a people, who can be a person has connections to some critical cybercrime. He has intentionally or unintentionally has done some critical; cybercrime or can have possibilities to have some bad record of having a cybercrime. After analyzing the keywords, we get the result that if a person has some unethical work in his social networking site, he will be declared as a green red people with. This type of person can do many cybercrimes or already has done some of them. Figure 3.3 is showing the result we got after searching. The searched keyword belongs to the red zone. For that, it is showing the result of the red zone.



Figure3.3: Showing a green zone based on search keywords

Timestamp of using the social network of a criminal

The timestamp of a suspected person's using social media is one of the most important parts. In this research work, we find out that the probability of doing a cybercrime is much higher in the weekends rather than weekdays. In weekends people generally have more time than weekdays, no pressure of work lead a person to do unethical work for no reason. Which may result in many cyberbullying in social media and occurs cybercrime in the social networking site. So, in this research work, we are working with the timestamp of a user.

Steps for Digital Forensics

Digital forensics is a step-based work. We must follow all the step. Each and every step is very important. We can't skip one step before going to another. It is very important for collecting errorless data.

Collection phase

The initial step in the digital forensic analysis is the collection phase. This phase is to predict the sources of records and gather forensic information from them that may help us in the next step. Main foundations of records are collected from computers, storage media like memory cards, external an internal memory, phone storage, routers, cell phones, digital camera, file manageme nt system, etc. This step is developed to give an overall presentation of data keep in mind to accordance with their importance, explosiveness, and quantity of exertion in a go [12]. We have work on this step to collect our data also in the initial step without the step it is hard to collect data

Examination phase of the collected data

It is very important to run this phase after the data collecting. This phase is called the second phase of forensic analysis named Examination phase. This phase is mainly for examining all the data in a proper way, which involves measuring the important data and removing the irrelevant types of information from the collected data, to make sure the given result will be right. The examinatio n needs to be done in super surveillances to have the actual result of information. Otherwise, all the work can go in vain and also can give us a different result what we didn't expect

Analysis phase after examination of the data

The analysis phase is done after the execution of the examination. Depending on the information we get from the examination phase, the analysis phase mainly works with the information and extracted and applicable data is being examined in this phase and draw a conclusion to make the best decision. There are many additional data as well. Sometimes they need a detailed study. Analysis phase also works with and call for dept data collection if it is needed. Dept data collection's main work is to create an accurate result. Analyzing part is one of the most important parts of this work. If any part of it went wrong. It may end up in a different result [13].

Reporting of all the information

Reporting phase is the last part of digital forensics. Reporting phase is kind of the procedure of showing the output of Analysis Phase. What happened in the whole research work, data set, analysis of data set, the outcome of the data? It shows the result of the work in a presentable way. Figure 3.4 is showing the steps of Digital Investigation.

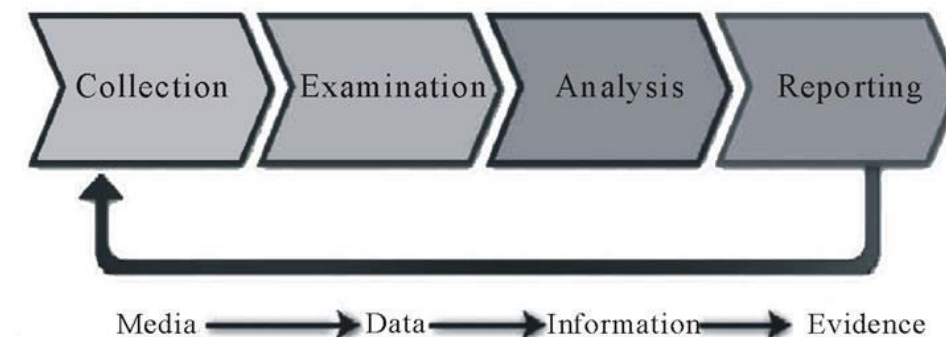


Figure 3.4. The digital forensic investigation processes

Digital Forensic Science concealments many sectors of digital analysis. For example, it includes, Computer forensics, Disk forensics, Network forensics, Firewall forensics, Device forensics, Database forensics, Mobile device forensics, Software forensics, live systems forensics, etc [13]. Those part actually come from many phases, following the overall process of digital investigation.

Each and every part is very important in this sector. For forensic analysis, everyone needs to follow this. In our research work, we also follow each and every step very carefully.

File System Forensics

Digital forensic required data. Without file or file system forensic is near to impossible. Documentation of digital evidence is very important. Documentation is done by file system forensics. It is also doing the documentation of series and analytical evidence from the storage media.

If we need any digital evidence, there is the best option is to execute a forensic analysis of a mobile phone. Our required information we can only find on the person's device. File system forensic work with the file storage of the device to find the actual result. By which actual result can be located from the vast number of data & information.

Steps needed for Storage Media Investigation

Storage media investigation has some rules and regulations. It follows these steps and phase. All of the phases and steps are very important. If we skip one of those or make any mistakes, it is impossible to get the desired result.

1. Reproduction of forensic logical picture: Nonintrusive procurement of a simulated photograph of information removed from the wondered device. That can be collected from the deleted files.
2. For veracity perform it requires Hash price control of calculation.
3. Directing a file-fragment renovation manner to get better documents and files to an original place of the device. That may help to preserve the evidence.
4. Inspect all documents especially deleted files and hidden files, that we get after the forensic analysis.
5. Reviewing common evidentiary objects that are very common, objects are given below:
 - a. Examine unrestricted spaces of the phone, slack spaces and horrific areas.
 - b. Application software program folders that are installed and rapidly used by the user.
 - c. Digital camera, printer and subsidiary devices, those objects may be lead us to the connection point of the crime.

- d. E-mails, Games & Graphics images, these parts are important to examine the communication process of the accused person.
 - e. Internet chat tabs & Network pastime tabs can give a brief idea about the history and the words the criminal used the most.
 - f. Recycled Folders, analyzing of a recycled folder can give an idea about the past history of that person.
 - g. System and file date/time objects, system file give a brief idea about the system the accused person used, and time object can give a brief idea about the time he was using the system.
 - h. User-created directories, folders, and files, those custom files and path are one of the directions to the evidence. Because criminals don't keep information in the local files.
 - i. Latest information abstraction from the page, temp, and archive space, those can help to find the recently used file.
6. Copying the content of the evidentiary item into textual content folders, the content of the file can explain the reason of creation that file.
 7. Searching for keywords strings to understand the strings used in the device.
 8. Reviewing file notations to understand the file notation used most on that device.
 9. Inspecting applications or indicating file of as folders annihilations, folders encryption, folders compressors or folders hiding efficacies to ensure the used file for a specific application.
 - 10 Making proof of synopses, revelations, reports, and professional findings based totally on evidentiary excerpts and analytical investigation. Those proof actually give the basic summary.

Data Mining for Digital Forensics

We get our information set from the evaluation end result of the phone. From these records set we, in reality, determine the suspected person's crime zone. We did our facts mining evaluation related to these points.

- i. Entity extraction of a mobile device has been castoff to mechanically recognize the user and his using activity throughout the session. login ID, Password, ID no, IP of the system of the person from his mobile device. Sometimes it is also possible to find out the personal home's information from reports or logs. It can be founded from the google devices he used.
- ii. Clustering procedures for example "concept space" have been castoff to robotically subordinate extraordinary, exceptional & uncommon items (for example user's, administrations, hardware structures) in criminal archives. That helps to find out the person if he did any kind of crime later.
- iii. Deviation recognition has been useful in scam recognition, community interruption recognition, and additional crime investigates that include tracing unusual things to do
- iv. Association instruction has been useful to discover relations, associations and sequential patterns between web transactions, connections & communications. That information is processed and is primarily based on the Apriori Algorithm and later decision making an algorithm for making a decision.

All the data need to be mining to get a result. Data Mining results show and effect reasons, motive, sample and counts of comparable kinds of assaults came about all through a period. This result comes after a lot of examinations and analyzing of data.

Data Mining Algorithm for Data set calculation the probabilities

- 1) Classify itemset from a case description (my planned structure stores this itemset as characteristics of tables, filesystem table, network table).
- 2) Item sets for the algorithm we are working on $I = \{I_1, I_2, I_3 \dots I_m\}$.
- 3) Set of actions we needed to execute the system $D = \{t_1, t_2, t_3 \dots t_n\}$.
- 4) Here we discover the common item sets via the Apriori algorithm. Engagements an interesting level to discover the set of common item groups.
- 5) We make Association Rules for our item set to have an accurate result.

- 6) We set the important and necessary SQL queries based on the instructions we set for that itemset.
- 7) This step is important and actually, give us the main results. We recover data from this.
- 8) Run Decision making an algorithm for making decisions.

Proposed Digital Forensic Tool

This proposed forensic tool, first of all, depends on the phone analysis. First, we need to do a basic forensic analysis of the phone or the mobile device of the accused person. After analyzing the phone, we will get a bunch of data from the mobile device. That may have any kinds of data, stored files, images, stored documents, deleted document, deleted images, search history, browser history, search documents. That information is the overall information of the accused person.

After that the file manager analyzer working with the analyzing part to analyze what data is important and what not. This phase is giving us the important information we need to look upon. From the file analyzer, we get the information about the deleted files and the documents. After analyzing those it states the information if it is related to the criminal occurrence or not. If it is, we need to do further investigation about those otherwise we work with the other options.

Information from the browser history is an important aspect of this thesis work. We get our data set from this history and search history. That information can state what kind of word he searched. This could make a relationship if those words are related to the cybercrime or not. From the keywords, we made a data set and trained the data set with our requirement. That trained data is actually given us the result of the probability of a criminal occurrence. From the trained data set we run a decision-making algorithm to make a decision about him. In which zone actually the criminal has his probability. This whole proposed tool and method describe what is the probability of becoming a criminal. Figure 3,5 showing us the block diagram of our proposed system. How actually we did our whole work

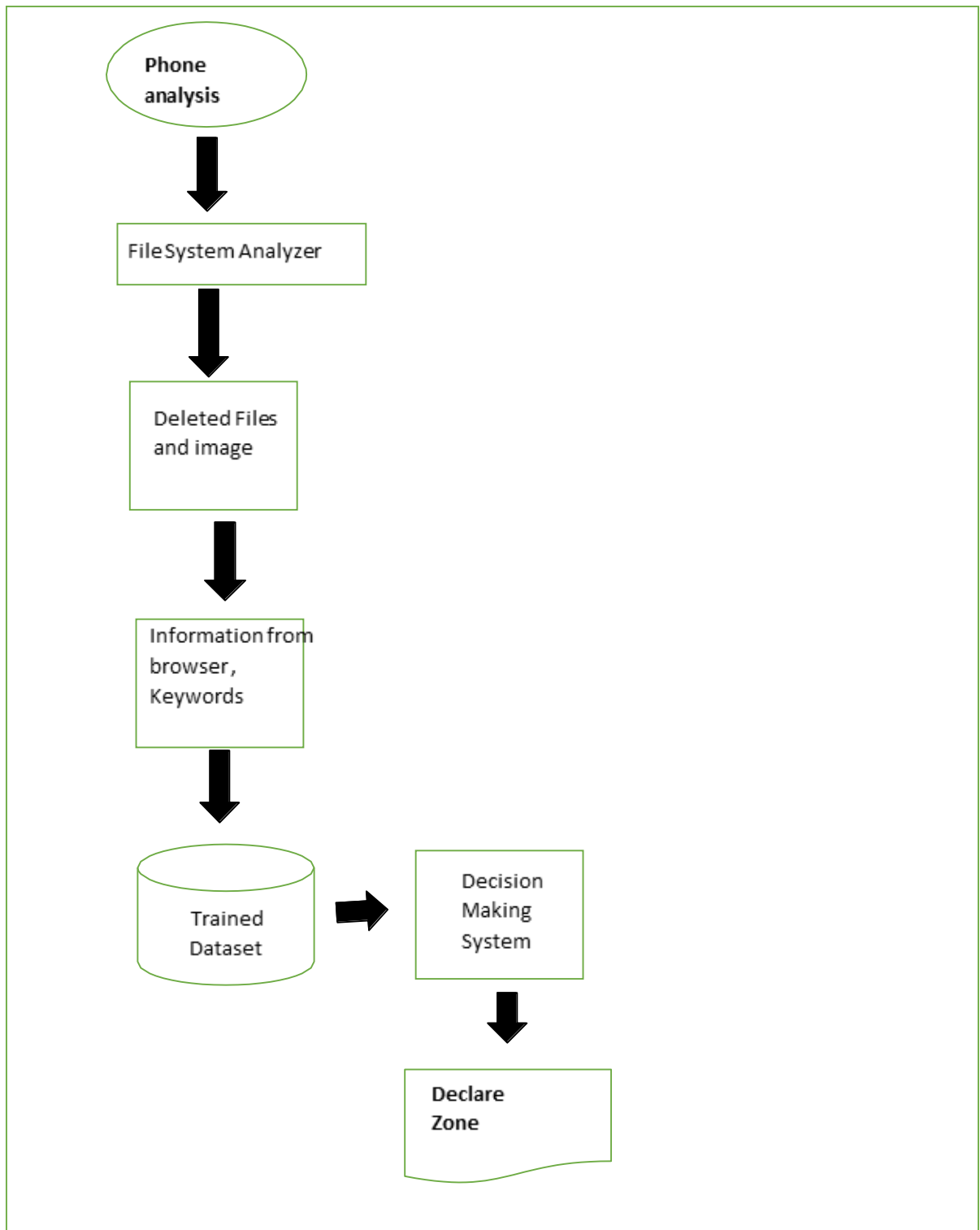


Figure 3.5: Block diagram of the proposed system

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

Introduction

In this research work first, we are working with a phone device to find out the deleted photos and file of a phone. From deleted files, it is easier to understand the probability of a suspected person to be a part of a certain crime. We are taking a mobile device Sprint HTC Hero for our forensic analysis. Figure 4.1 is showing the examined mobile device we used for our work.



Figure 4.1: Examinated mobile device & info screen

Using data cable to connect the device

Though the proofs chain for the Device is a patented HTC cable, a normal mini-USB cable worked with figures, facts, files, information, statistics transmissions. The HTC cable holds jogging song and audiovisual done through USB and would be preferred for customer requests & system however it is now not compulsory for at all to any kind of digital forensics evaluation we did in the mobile device. But in this evaluation, we used this method, regarding this device a criminal device. The USB cable is only used for transferring data. Not for any forensic analysis of a certain thesis.

Analyzing the result of memory card and Imaging device

Though an examination of the changeable external card of the device has its restriction. It generally inserted to the phone externally. Buildup phone system data is not obliged to store data & documents to the memory card. But we can use this instrument with the phone & memory card for creating a logical image, what we used in the analysis part, from the device's external card. It is fairly humble and usual actions for imaging a device internal and external memory what can be used in the digital forensics. Those imaging processes are very important in digital forensics. In the investigation here, Access Data's FTK Imager v2.5.1 was employed. This tool is used for making the imaging process of the data.

The first step is to connect the phone to the inspection mechanism for the analyzing, via a transcribe blocker to confirm the truthfulness of the data & information. When the handset is associated, the device declares in the screen that, a USB cable of the phone is allied and request the operator to choice to reproduce files to/from the host computer or the determined file user want to analyze, Then additional screen seems to request the operator to mount the phone. Figure: 4.2 is showing the “Mount” request the phone set after it got connected with the USB cable.



Figure 4.2: Screen Showing “Mount” request.

When linked, the phone will search for any essential suitable drivers, that is logical to this process. If questions ascend, drivers are made accessible on HTC's website. From the drivers, it is very easy to generate an image. It can be easily downloaded from the website. After it got downloaded it can be a good option for the all-digital forensics.

Nowadays in FTK Imager drive to the File pulldown set menu, and choose the Add Evidence sweeping, and then select Physical Drive. Choose the drive that is suitable for the Android Phone. Without the drive, it is not possible to get the data. It needs to be remembered that the phone will be similar dimensions to the memory card. Here there is a 4GB microSD external card in the phone. Figure 4.3 is showing the Drive selection of the FTK Imager.

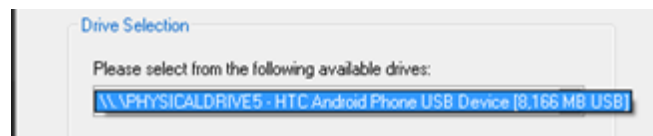


Figure 4.3: Drive Selection for the device to connect FTK.

Except for the picture by using the Folder, Transfer disk image choice. We need to type sure to capture a physical image of the whole drive somewhat than a rational image of the divider. Here, PHYSICALDRIVE5 was designated and imaged, transfer the production to a raw dd image file. As with any image file, we need to be certain to confirm the hash prior to any follow ing examination. Note that the SD card should be put aside and not substituted in the device. FTK file generally gives us a photo summary of the phone. Figure 4.4 is showing the result screen and the summary of the imagining information we get.

General	
Name	sdcard2.001
Sector count	15949624
MD5 Hash	
Computed hash	e3cbc7b88bc00cbc30227c528f31ade2
Report Hash	e3cbc7b88bc00cbc30227c528f31ade2
Verify result	Match
SHA1 Hash	
Computed hash	6c86800c1841e4a0aa80d1783248660d7ff06594
Report Hash	6c86800c1841e4a0aa80d1783248660d7ff06594
Verify result	Match

Figure 4.4: FTK Imager is showing the result screen.

The reputation of digging the device in order to obtain a dd image. The ability to give physical image memory is the holy grail of mobile device forensics. The device's memory can contain tremendously valuable data, such as the contact list, call logs, text messages, and other phone

information. Without examining the phone, we may miss any important data that is so important for the examination. But in this process, it is a very rare case to miss data. Extra material can also be covered and hidden, such as Web history, e-mails, images viewed on the phone, passwords, and fragments of other data is a very important part of the case. Admittance to memory can be skilled by rooting the phone.

Recovered documents

Maximum enhanced documents were not of a physical evidentiary charge. A huge percentage of the HTML records were announcements and required for the image analyzer of this work and only four files were comprehensive snapshots of Web pages. The HTML files included 20 Exchangeable Image File (EXIF) data for JPEGs; this material can be helpful to determine what exact camera acquired an image. It is an important part. all the data and information are collected through the analyzer

Recovered images

Most of us use a personal computer. On a representative regular computer, that Android phone had nearly 10,000 images, only some of which would be exciting in a forensics inspection and very important evidence for the investigation. Those images are very important. The primary notable images originate were the ones showed as the phone is striking up. First, we need to boot up the device. Without the booting of the phone, it is impossible. There are three different images for a different type of image we found on the phone. Those three pictures are the screenshot of three important times, while we are using that device. That recovered image is very important in forensic analysis. Because it describes many things for us. DD image can describe the origin so that we can determine many things from it. Those help us to obtain a huge amount of information. Any screenshots, the deleted image can explain the nature of the user to describe his intention. That helps us to determine the criminals. Also in this work, we bear in mind that, our analysis always go on the right track that we never determine an innocent people a criminal and criminal never get rid of the law and enforcement. Figure: 4.5 is showing the recovered image we got after the digital forensic analysis.



Figure 4.5: Retrieved Images from the deleted file

History of the device

History of mobile data is one of the most important forensic analysis of mobile devices. It actually gives an overview of a user online. From that history, we collect our data set and trained the data set for experimental work.

Browser history

From Browser history, we can understand what kind of social site and what the user browses.

From that, we understand if the user has any access over any harmful site or not.

128	419	http://www.facebook	http://www.facebook	1	1259724574607	0
129	420	http://www.youtube	http://www.youtube	1	1259766087329	0
130	421	http://m.youtube.co	http://m.youtube.co	1	1259766119161	0
131	422	http://www.newegg	http://www.newegg	1	1259794961773	0

Figure 4.6: Browser History

Search History:

From the search history, we actually made our data set. From those, we made some keywords and divide them into three zones for making a decision. From those data set we can give the probability to being in a certain color zone we mention in our work.

237	237	where the wild partie	1259461432984
238	238	pulp fiction soundtra	1259465046279
239	239	ball and chain lyrics	1259469379237
240	240	sublime scarlet bego	1259469890406
241	241	party hard lyrics	1259472218623

Figure 4.7: Search history

Confusion matrix of collected data

This matrix showing the matrix of the data set we collected from the browser history and the search history some of the mobile devices. This matrix is describing the trained data set we got for our experiment. From this matrix, we got the data set in a trained way that we can use for further experiment. Figure 4.8 is showing the confusion matrix of our data set.

=== Confusion Matrix ===

```

a b c d e f g h i j k l m n o p q r s t u v  <-- classified as
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | a = Identity theft
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | b = Phishing
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | c = Piracy
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | d = Malware
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | e = Spam
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | f = Theft
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | g = Bioterrorism
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | h = Spammer
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | i = Sexting
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | j = Pornography
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | k = Hackers
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | l = Hacking
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | m = Laundering
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | n = Spamming
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | o = Nuclear
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | p = Terrorism
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | q = Viruses
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | r = Firewalls
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | s = Wiretapping
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | t = Criminal
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | u = Drug traffic
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | v = Spyware

```

Figure 4.8: Confusion matrix of collected data

Class accuracy

Class accuracy is very important in the matter of analyzing data. We worked on the class accuracy to determine the class we are showing is right or not. From this class accuracy, we got that the data set we used had maximum class accuracy we needed to run the data set. Figure 4.9 is showing the accuracy rate of the data set that we used to make our experimental result. From that, we can explain and understand that the data set right or wrong.

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
	0.000	0.905	0.000	0.000	0.000	-0.549	0.048	0.045	Identity theft
	0.000	0.143	0.000	0.000	0.000	-0.087	0.024	0.045	Phishing
	0.000	0.000	?	0.000	?	?	0.024	0.045	Piracy
	0.000	0.000	?	0.000	?	?	0.024	0.045	Malware
	0.000	0.000	?	0.000	?	?	0.048	0.045	Spam
	0.000	0.000	?	0.000	?	?	0.071	0.045	Theft
	0.000	0.000	?	0.000	?	?	0.024	0.045	Bioterrorism
	0.000	0.000	?	0.000	?	?	0.024	0.045	Spammer
	0.000	0.000	?	0.000	?	?	0.024	0.045	Sexting
	0.000	0.000	?	0.000	?	?	0.071	0.045	Pornography
	0.000	0.000	?	0.000	?	?	0.024	0.045	Hackers
	0.000	0.000	?	0.000	?	?	0.143	0.050	Hacking
	0.000	0.000	?	0.000	?	?	0.071	0.045	Laundering
	0.000	0.000	?	0.000	?	?	0.024	0.045	Spamming
	0.000	0.000	?	0.000	?	?	0.048	0.045	Nuclear
	0.000	0.000	?	0.000	?	?	0.143	0.050	Terrorism
	0.000	0.000	?	0.000	?	?	0.024	0.045	Viruses
	0.000	0.000	?	0.000	?	?	0.048	0.045	Firewalls
	0.000	0.000	?	0.000	?	?	0.071	0.045	Wiretapping
	0.000	0.000	?	0.000	?	?	0.024	0.045	Criminal
	0.000	0.000	?	0.000	?	?	0.119	0.045	Drug traffic
	0.000	0.000	?	0.000	?	?	0.024	0.045	Spyware
g.	0.000	0.048	?	0.000	?	?	0.052	0.046	

on Matrix ===

Figure 4.9: Accuracy by a class of the data

Trained Data of the data set

Trained data set is very important for experimental work. If we didn't train our data, it doesn't give the right result. In our experimental work, we trained out data set to have an accurate result. After training the data we make them ready for the experiment and run them for having a result. Figure 4.10 is showing the train data set of our work.

Crime																
Identity theft	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Phishing	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Piracy	1.1815	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455
Malware	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456
Spam	1.1793	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Theft	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Bioterrorism	1.1815	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455
Spammer	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457
Sexting	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Pornography	1.1793	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Hackers	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456
Hacking	1.1815	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455
Laundering	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Spamming	1.1793	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Nuclear	1.1815	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455	1.0455
Terrorism	1.1793	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Viruses	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Firewalls	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Wiretapping	1.1793	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Criminal	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456
Drug traffic	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456	1.0456	1.0456
Spyware	1.1793	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0456	1.0457	1.0456	1.0456
[total]	25.954	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026	23.0026

Time taken to build model (full training data) : 1.86 seconds

Figure4.10: Describing the data set after training

Run time information

In our research work, we took 52 data set to determine the probability of cybercrime. We divided it into three class to showing the probabilities. From the result, we can claim that we can claim that 4 people have the possibility of 13% and 11 people have 7% of the become cybercriminal. Rest of the people are innocent. Figure 4.11 showing the probabilities of the people to become a cybercriminal.

```
Time taken to build model (full training data) : 0.38 seconds

=== Model and evaluation on training set ===

Clustered Instances

 0      2 ( 13%)
 1      1 (  7%)
 2      1 (  7%)
 3      1 (  7%)
 4      1 (  7%)
 5      1 (  7%)
 6      1 (  7%)
 7      1 (  7%)
 8      1 (  7%)
 9      2 ( 13%)
10      1 (  7%)
11      1 (  7%)
12      1 (  7%)

Log likelihood: -2.63059
```

Figure 4.11: Run time information

CHAPTER 5

CONCLUSIONS AND FUTURE RESEARCH

Conclusions

Cell phones are becoming even more erudite and able. It should be, otherwise it will be the worst most possible thing can be happened. Cybercrime will be increased but no proper way to detect the crime. Both law administration and the private sector need to participate time and money into learning about new operating systems and developing new forensic methods. Otherwise, the new technologies will be a great threat for us. And we will have no choice.

In this research work, we are mainly working with the evidence we got after the forensic analysis of the phone. This forensic analysis gives us the information about the suspected person phone. We got information about his browser history and his search history. From that result, we can give the probability of becoming him a criminal.

Implication of the further study

In our future work, we will work on the keywords and the data set to establish a website. In this website, if any normal person searches any keywords, the website will give the probability for this word, being used in cybercrime.

As future work, we plan to design and integrate a near real-time cyberthreat situational awareness dashboard. To this end, we will automate the approach presented in this paper. In addition, based on the observations found in the evolution of badness scores for domains and connected IPs, we aim to assess the empirical periods to consider domains badness persistence and IPs badness.

REFERENCES

- [1] K. Kent, S. Chevallier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST SP800-86 Notes, 2006.
- [2] S. K. Brannon and T. Song, "Computer Forensics: Digital Forensic Analysis Methodology," Computer Forensics Journal, Vol. 56, No. 1, 2008, pp. 1-8.
- [3] D. Klieiman, K. Timothy and M. Cross, "The Official CHFI Study Guide for Forensic Investigators," 2007.
- [4] B. Carrier, "File System Forensic Analysis," Addison Wesley Professional, 2005.
- [5] C. Kaiwee, "Analysis of Hidden Data in NTFS File System," Whitepaper.
- [6] M. Alazab, S. Venktraman, and P. Watters, "Effective Digital Forensic Analysis of the NTFS Disk Image," Ubiquitous Computing and Communication Journal, Vol. 4, No. 3, 2009, pp. 551-558
- [7] N. Meghanathan, S.R. Allam and L. A. Moore, "Tools and Techniques for Network Forensics," International Journal of Network Security & Its Applications, Vol. 1, No. 1, 2009, pp. 14-25.
- [8] E. Casey, "Network Traffic as a Source of Evidence: Tool Strengths, Weaknesses, and Future Needs," Journal of Digital Investigation, Vol. 1, No. 1, 2004, pp. 28-43.
- [9] H. Achi, A. Hellany and M. Nagrial, "Network Security Approach for Digital Forensics Analysis," International Conference on Computer Engineering & Systems, 25-27 November 2008, pp. 263-267.
- [10] A. R. Arasteh, M. Debbabi, A. Sakha and M. Saleh, "Analyzing Multiple Logs for Forensic Evidence," Digital Investigation, Vol. 4S, 2007, pp. S82-S91.
- [11] H. Chen, W. Chung, Y. Qin, M. Chau, J. J. Xu, G. Wang, R. Zheng, and H. Atabakhsh, "Crime Data Mining: An Overview and Case Studies," Proceeding of ACM International Conference, Vol. 130, 2003, pp. 1-5.
- [12] V. Justickis, "Criminal Datamining," Security Handbook of Electronic Security and Digital Forensics, 2010.
- [13] Roman, Rodrigo Fernando Morocho, et al. "Digital Forensics Tools." International Journal of Applied Engineering Research 11.19 (2016): 9754-9762

APPENDICES

Appendix A: Research Reflection

The purpose of this Appendix is to provide an introduction to Research reflection. The group research project was a challenging and enjoyable experience typical of the course as a whole. We have had little exposed to group work at university. So, it was a nice change to be part of an effective and dynamic team.

The experience of our work taught us many things. In the beginning, we were very much confused about our work. We change plan in many times. But in the end come to a result.

Forensic analysis of mobile device

ORIGINALITY REPORT

22%

SIMILARITY INDEX

19%

INTERNET SOURCES

13%

PUBLICATIONS

18%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Daffodil International University

Student Paper

5%

2

file.scirp.org

Internet Source

4%

3

www.dfrws.org

Internet Source

3%

4

Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitingner. "Network and device forensic analysis of Android social-messaging applications", Digital Investigation, 2015

Publication

2%

5

Submitted to Georgetown University

Student Paper

2%

6

ro.ecu.edu.au

Internet Source

2%

7

networkingnexus.net

Internet Source

1%

Submitted to Westwood College - ATM

Aamo Iorliam. "Chapter 5 Proposed Digital Surveillance Software", Springer Nature, 2019

Publication

Submitted to Champlain College

Student Paper

K. Sindhu, K., and B. B. Meshram. "Digital Forensics and Cyber Crime Datamining", Journal of Information Security, 2012.

Publication

ir.unimas.my

Internet Source

eprints.utm.my

Internet Source

leanpub.com

Internet Source

Sari Sultan, Ayed Salman. "FCT: Digital Forensics E-Learning System with Dynamic Examination Support", 2018 IEEE Conference on Application, Information and Network Security (AINS), 2018

Publication

amsdottorato.unibo.it

Internet Source

17	Silveira, M. M., J. J. Oliveira, and A. C. Luchiari. "Dusky damselfish <i>Stegastes fuscus</i> relational learning: evidences from associative and spatial tasks : learning in <i>stegastes fuscus</i> ", <i>Journal of Fish Biology</i> , 2015. Publication	<1 %
----	---	------

18	scholarcommons.usf.edu Internet Source	<1 %
----	--	------

19	dspace.daffodilvarsity.edu.bd:8080 Internet Source	<1 %
----	--	------

Exclude quotes	Off
Exclude bibliography	Off

Exclude matches	Off
-----------------	-----