**DE-ANONYMIZING PROTOCOL FOR SOCIAL MEDIA NETWORK**

A dissertation submitted for the degree of

Master of Science in Information Security



K.G.LAKSIRI GEETHAL

University of Colombo School of Computing

Sri Lanka

2018

DECLARATION

The thesis is my original work and has not been submitted previously for a degree at this or any other university or an institute. To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name: K.G.LAKSIRI GEETHAL

Signature: .............................

Date:..................................

This is to certify that this thesis is based on the work of Mr. K.G.L.Geethal Under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by: Supervisor Name: Dr. Kasun De Zoysa

Signature: .............................

Date:..................................

ACKNOWLEDGMENT

This work was carried out as a part of the Master of Science in Information Security degree program at University of Colombo School of Computing. I would like to thank all who helped me in various ways to make this work a success. Especially I am truly grateful for the valuable guidance and assistance given by my supervisor, Dr. Kasun De Zoysa, Senior Lecturer at University of Colombo School of Computing, SDIG Mr.Lathiff (STF), SDIG Mr. Ravi Senevirathne (CID), DIG Sanjeewa Darmarathna (Training and Personnel) and DIG Nagahamulla (CID). I would like to thank my panel members Dr. D.A.S.Atukorale, Dr. C.I.Keppetiyagama, Dr.G.D.S.P.Wimalaratne and Dr. H. A.Caldera and rest of the staff members at UCSC for their valuable comments and support throughout the work. And also, I am grateful to my Colleagues for the maximum support and courage given me during the time to make this very success.

ABSTRACT

The development of information technology is not only beneficial but also harmful for human development. This has become a topic that is mostly spoken in the society. It usage has gone unlimited to the extent that we cannot imagine of its precincts.

Society is not only a group of people but it also means an interpersonal communication among them. Communication means exchange of information among the people within the society. People within the society communicating with each other via internet happen through social media. As such, the criminal elements especially those who tend to commit sexual harassments and sexual crimes are moving freely in this sphere and commit various crimes by hiding their identity (anonymously). It is a severe threat to the society. The damage that is caused to the female children and to the male children is immeasurable. In this background, we would focus our attention as to how we could rescue them from the threat of Anonymity and committing sexual related Cybercrimes through the social media.

Today the World has become a global village because of the social media. Facebook, Instagram, Whatsapp, YouTube, Vimeo, E-mail, LinkedIn, Reddit and Pinterest are examples for social communications.

|  |  |
| --- | --- |
| Contents | Page No |
| TABLE OF CONTENTS | v |
| LIST OF FIGURES | viii |
| LIST OF ABBREVIATIONS | ix |
|  |  |
| 1 INTRODUCTION | 1 |
| 1. Problem Domain | 1 |
| 1. The Problem | 2 |
| 1. Objectives | 2 |
| 1. Scope | 3 |
| 1. Thesis Outline | 3 |
| 1.5.1 CHAPTER 1 INTRODUCTION | 3 |
| 1.5.2 CHAPTER 2 LITERATURE SURVEY | 3 |
| 1.5.3 CHAPTER 3 DESIGN | 3 |
| 1.5.4 CHAPTER 4 IMPLEMENTATION | 3 |
| 1.5.5 CHAPTER 5 EVALUATION | 4 |
| 1.5.6 CHAPTER 6 CONCLUSION | 4 |
|  |  |
| **2 LITERATURE SURVEY** | 5 |
| 1. Literature Review | 5 |
| 1. Social Media Networks/ Social Communications | 5 |
| 1. Anonymity of Social media Networks | 6 |
| 1. Committed Crimes through the Social Media Networks | 6 |
| 1. Cyber Crime and Evolution | 9 |
| 1. Bullying in Cyberspace | 11 |
| 1. Click fraud | 11 |
| 1. Cyber Stalking | 11 |
| 1. Defamation | 12 |
| 1. Email Spoofing | 12 |
| 1. Identity Fraud | 12 |
| 1. Impersonation | 13 |
| 1. Lottery Scam | 13 |
| 1. Nigerian 419 Fraud Scheme | 13 |
| 1. Packet Sniffing | 14 |
| 1. Phishing & Spoofing attacks | 15 |
| 1. Pornography | 15 |
| 1. Smishing | 16 |
| 1. Social Engineering | 16 |
| 1. Vishing | 16 |
| 1. Related Projects/ Previous Research | 17 |
| 1. Legislations & Legal Provisions for Social Media Crime Investigation | 18 |
| 1. Computer as Target | 18 |
| 1. Computer as Tool | 18 |
| 1. Computer as Accomplice | 18 |
| 1. Computer crime act on 24 of 2007 | 18 |
| 1. Notable Provisions defined in section 1 and 2 | 19 |
| 1. Crimes are defined in section 3 to 14 | 19 |
| 1. Special Procedures defined in section 15 to 25 | 20 |
| 1. Other Acts related to the Computer Crime | 20 |
|  |  |
| 1. Positives and Negatives of social Networks | 20 |
| 1. Positives of social Networks | 21 |
| 1. Negatives of social networks | 21 |
|  |  |
| 1. Prevention of Crimes Committed through the Social Media network | 22 |
| 1. Safety on Social networking sites | 22 |
| 1. Safety on electronic mail | 23 |
| 1. Precautions for safe guarding children becoming online Victims | 24 |
| 1. Measures to be taken in the event of Victimization | 25 |
| 1. Immediate Measures to be taken | 25 |
|  |  |
| **3 DESIGN** | 26 |
| 1. De-anonymizing Tool Design | 26 |
| 1. Draft Design Model | 26 |
| 1. Hosting Server Design Model | 29 |
| 1. Client Server Design Model | 31 |
| 1. De-anonymizing System Architecture | 32 |
| 1. Detection overview of the De-anonymizing Tool | 32 |
|  |  |
| **4 IMPLEMENTATION** | 33 |
| 1. Technologies and Tools | 33 |
| 1. JAVA as the programming language | 33 |
| 1. Links base approach | 34 |
| 1. Browsing history base approach | 34 |
| 1. Text base approach | 34 |
| 1. Investigation Protocol | 35 |
|  |  |
| **5 EVALUATIONS** | 37 |
| 1. Evaluation of the De-anonymous tool and Protocol. | 37 |
| 1. The Selected Case for the Evaluation. | 38 |
|  |  |
| **6 CONCLUSION** | 41 |
| 1. Future Work | 42 |
| BIBLIOGRAPHY | 43 |

|  |  |
| --- | --- |
| LIST OF FIGURES | Page No |
| Figure 2.1 Social Media Network Users in Sri Lanka | 5 |
| Figure 2.2 Statistics from Sri Lanka CERT/CC | 7 |
| Figure 2.3 Statistics from Criminal Investigation Department of Sri Lanka | 7 |
| Figure 3.1 the selected page for the Draft | 27 |
| Figure 3.2 Downloaded the selected page and preparing other files | 27 |
| Figure 3.3 content of the downloaded file | 28 |
| Figure 3.4 content of the embedded file | 28 |
| Figure 3.5 The JAVA scripts which is calling targeted Meta data | 28 |
| Figure 3.6 The JAVA scripts which is calling targeted IPs | 29 |
| Figure 3.7 The JAVA scripts of PHP file and writing data into Text file | 29 |
| Figure 3.8 Configurations of the hosting server | 30 |
| Figure 3.9 Uploaded files to server | 30 |
| Figure 3.10 Draft message sent via SMN | 31 |
| Figure 3.11 Configuration of the Client Server | 31 |
| Figure 3.12 the De-anonymizing system architecture | 32 |
| Figure 3.13 the network architecture | 32 |
| Figure 5.1 selecting website to download | 38 |
| Figure 5.2 sent message via SMN | 39 |
| Figure 5.3 Received Meta data from opposite party | 39 |
| Figure 5.4 ISP details of the detected network system | 40 |
| Figure 5.5 Recovered email from the computer of the suspect or anonymous user | 40 |

|  |  |
| --- | --- |
| LIST OF ABBREVIATIONS | |
| LEO | Law Enforcement Officer |
| SMN | Social Medial Network |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| CERT | Computer Emergency Readiness Team |
| CID | Criminal Investigation Department |
| PHP | Programming language |
| JAVA | Programming language |
| URL | Uniform Resource Locator |

Chapter 1

**INTRODUCTION**

* 1. **Problem Domain**

Social networks are now so well established, that there are now a core 'top 5' social networks which doesn't change much from year-to-year. But, as we'll see, the most popular social media sites vary a lot by level of usage in different countries and demographics. So understanding these differences in popularity of different social networks is really important when targeting specific audiences. When comparing the most popular social networks some social networks are growing more rapidly than others while some are now in decline some individuals or groups due to some abuses, stalkers and perpetrators misuse a variety of online spaces to harass victims. Misuse of Facebook to harass or stalk can include an abuser or stalker threatening or harassing someone through posts or private messages; posting personally identifying information or pictures without the person’s consent in order to cause harm or distress; or accessing the victim’s account without permission to monitor activity; or impersonating the victim were reported to law enforcement agencies in a fast manner. Although these tactics of abuse are not acceptable, unfortunately, not all of these behaviours may violate Social media’s Terms of Service and, by itself, may or may not be illegal. Because of that, it is important for Survivors to know what their options are and what recourses are available when someone is harassing them through Facebook. Most of the time the users of the Social media were anonymously engages to harass others, who are against them. Therefore de-anonymizing of account users of the Social media is very important and necessary to identify the real person or legitimate account user to build a fence and to bring them before the court for necessary actions. Once the police have enough evidence against a person, they will lay criminal charges and a judge will decide if the accused should be released or remanded. Therefore the project focuses on “De-anonymizing Protocol for the social network users” to identify the real identity.

* 1. **The Problem**

There are over 1.3 billion users on Facebook, out of which around 81 Million users are Fake (Fake Facebook profiles). Somebody creating a Fake profile of yours is not a Big deal for Social media network unless you represent a law enforcement agency or an Expensive Legal firm. Most fake Social media network profiles are set-up by adolescents in relationships seeking to destroy the reputation of their ex-partner or harass the people. The Law enforcement agencies often receive such complaint from people who find themselves or their relatives in this situation. Identity theft is common on Social media networks, but somebody using your image to harass or play with other people they know; thereby defaming them is really embarrassing and malicious. While can always report such imposters profile to Social media network providersusing their Report form, it takes hell lot of time for Social media network providers to review the profile and disable it. Also, Social media network providers will never disclose any details about the fake profile, like when it was created and from which Computer it was operated.

The Social media network providers will provide Information regarding fake profile only when there is Police intervention and this is a very long process. Moreover, police will not go through the hassle of contacting Social media network providersand behave like loyal dogs to track down the imposter unless the matter is very serious.

Once have the **IP address of fake profile user**, then need to get a court order for the ISP to reveal the information and billing address of the person involved. If the fake profile user had used a proxy server to hide real-IP, it would be very difficult to track down the real IP address. Here in, can **Find an IP address of a fake Facebook user** and even nab the culprit.

* 1. **Objectives**
* To identify the anonymous Social media user account.
* Conduct an investigation on the anonymous user account.
* Collect the Evidence, this was against the suspected user account.
* After conduct the all investigations and identify the real Suspect of the anonymous account.
* File a case and produce the suspect to before the court.
* Overall objective is detection and control the people who are misused the social media by anonymous.
  1. **Scope**

The de-anonymizing protocol is a detection and investigation system of an anonymous social media account user and a single user environment. The detection could be success who is the investigator could build a relation with the anonymous account user to continue the conversation without make any suspicions. The detection system of the De-anonymizing Protocol is always modify and change according to the social media account and nature of the fraud but the Investigation methodology no need to modify or change.

* 1. **Thesis Outline**

This thesis includes six chapters which provide a broad description of the research carried out to achieve the objectives and the way to implement the anonymous social media detection protocol which detects anonymous account and real user of the account.

* + 1. **CHAPTER 1 INTRODUCTION**

The Introduction chapter will provide the background of the project and the objectives which are going to achieve at the end of the project.

* + 1. **CHAPTER 2 LITERATURE SURVEY**

The Literature Survey chapter provides the background study, concepts and the technologies used through the De-anonymizing protocol for Social media network.

* + 1. **CHAPTER 3 DESIGN**

The Design chapter discusses the detection of the anonymous Social media network and detailed discussion about the methodologies which are applied in each and every Step.

* + 1. **CHAPTER 4 IMPLEMENTATION**

Chapter four contains the Implementation chapter; it discusses the actual implementation of the anonymous Social media network detection system.

* + 1. **CHAPTER 5 EVALUATION**

Evaluation Chapter describes the approaches taken to evaluate the detection system. This will include the testing criteria.

* + 1. **CHAPTER 6 CONCLUSION**

Chapter six, Conclusion will discuss the extent of the achievement of the final objectives, limitations of the anonymous Social media network detection system as well as future enhancements.

Chapter 2

**LITERATURE SURVEY**

1. **Literature Review**
2. **Social Media Networks/ Social Communications**

Society is not only a group of people but it also means an interpersonal communication among them. Communication means exchange of information among the people within the society. People within the society communicating with each other via internet happen through social media. Today the World has become a global village because of the social media. Facebook, Instagram, YouTube, Vimeo, E-mail, LinkedIn, Reddit and Pinterest are examples for social communication. Social communication can be categorized as follows:

* Social Networking - Facebook, LinkedIn, Google +
* Micro blogging - Twitter, Tumbir
* Photo sharing - Instagram, Whatapp
* Video Sharing - you tube, Facebook live, periscope, Vimeo

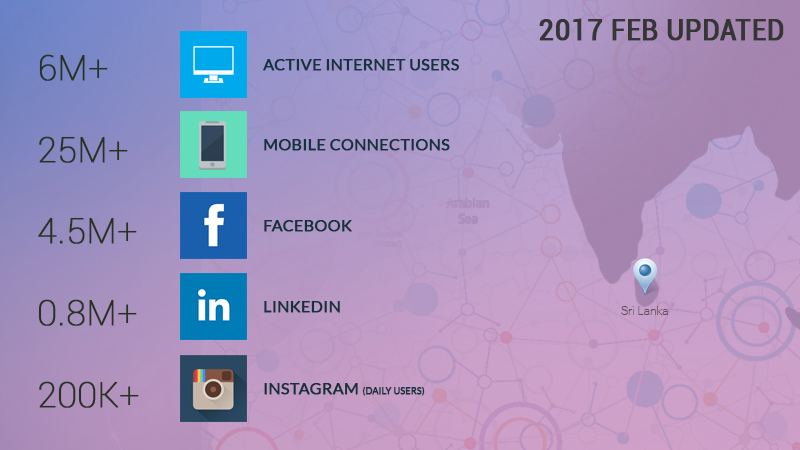
Data Sources: from: [www.digitalmarketer.lk](http://www.digitalmarketer.lk/) and [www.interworldstats.com](http://www.interworldstats.com/)

Figure 2.1 Social Media Network Users in Sri Lanka

1. **Anonymity of Social media Networks**

People often surf the web under the illusion that their actions are private and anonymous. Unfortunately for them such is not the case. Each time you visit a site, you leave a visiting card that reveals where you are coming from; what kind of computer you use; and various other details. Each visit of yours is logged! An anonymizer or an anonymous proxy is a tool that attempts to make activity on the internet untraceable. It empowers you to surf the web without revealing any personal information. Not only does it hide your IP address and internet history but also unblocks the restricted websites and lets you navigate past web-filters. The problem arises when individuals use this to avoid the consequences of engaging in criminal, disruptive or socially unacceptable behavior online.

1. **Committed Crimes through the Social Media Networks**

Cyberspaces are built by the Human beings as such none could imagine its delimitation. Human beings use these spaces to cause nuisance other than for good cause. A crime that is committed through the use of internet is called cybercrimes. They are committed via websites, chat rooms, forums, E- mail, dating sites.

Especially the children in this modern society dealing in cyberspace create a dangerous situation for themselves. In Sri Lanka, a schoolgirl committed suicide because of a relationship she developed within the cyberspace. She took her life because she could not bear the mental agony she underwent. According to the incidents which were reported to the Child protection Authority, some school girls became mothers while some went to abroad because they could not face the society. This situation has created a great danger within this society. This is a common situation is not only in Sri Lanka but in other countries as well.

Statics of the reported cybercrimes up to 2014 according to Sri Lanka CERT/CC and Criminal Investigation Department of Sri Lanka as follow.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Cybercrimes** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| Phishing | 05 | 10 | 05 | 06 | 06 | 03 |
| Insult | 03 | 10 | 20 | 02 | 08 | 08 |
| Spam | 05 | 11 | 10 | 03 | 06 | 18 |
| malware | 11 | 12 | 05 | 01 | 02 | 02 |
| Distortion | 14 | 15 | 08 | 20 | 15 | 16 |
| Threatening | 06 | 08 | 12 | 03 | 06 | 08 |
| Unlawful Access | 06 | 08 | 12 | 03 | 06 | 08 |
| False Account | 1425 | 1100 | 1200 | 1320 | 1450 | 1565 |
| **Total** | **1475** | **1174** | **1272** | **1558** | **1499** | **1628** |

**Figure 2.2 Statistics from Sri Lanka CERT/CC**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **YEAR** | **SOCIAL MEDIA ASSOCIATED CRIMES** | **Unauthorized access (Computer Crimes)** | ***Email related Crime (Hacking , Phishing and Spoofing)*** | **TOTAL** |
| **2009** | **34** | **02** | **08** | **44** |
| **2010** | **61** | **06** | **15** | **82** |
| **2011** | **115** | **12** | **34** | **161** |
| **2012** | **62** | **11** | **31** | **104** |
| **2013** | **23** | **06** | **16** | **45** |
| **2014** | **80** | **12** | **22** | **114** |
| **2015** | **175** | **15** | **30** | **220** |
| **2016** | **170** | **17** | **35** | **222** |

**Figure 2.3 Statistics from** **Criminal Investigation Department of Sri Lanka**

These data shows only reported cybercrimes but the numbers that are not reported is higher. Hence, it is very important to consider crimes committed in related to the social media. When you upload your personal data to the social media, chat sites, dating sites or the E-mail it may affect to your privacy. When you surf within the cyber space through the various sites, you may become the victims of the cybercrime. Criminal acts committed by using social media sites, websites, E-mail, chat rooms, dating sites interpreted as cybercrimes. Someone or some group commit crime directly or indirectly against someone or some group, using computer or computer related technology it can be called as cybercrime.

About 556 million people become victims of the cybercrime in a year and about 1.1million people become victims every day. The cybercrimes identified as a passive crimes. Those passive crimes recognized as follows: Crimes commit using E-mails, offensive speech, deformation, use privacy data without authority; false information publishing and false information against women and children could be identified as grave crime in this 21st century. Smuggling of child’s phonographic pictures had become a global business.Most of the reported cybercrimes are money transactions by fraud using E-mails, Online dating sites, spam messages, credit cards and electronic cheque. Globally most countries implemented legal policy to regulate these kinds of criminal behaviours. In this way, various measures have been taken to prevent cybercrime at the states level and internationally.

When comparing with European Countries and South Asian countries gave less attention in this regard. However, a dialogue is being conducted at present in this regard. Therefore, cybercrimes growing rapidly and it is a grave risk for women and children to become victims.

Following crimes have been reported to law enforcement officials and other government and semi government institutes. Though social media network crimes are a wider area, we are going to focus on the nature of the risk that mostly women and children have to face because of the anonymous social media users/ accounts (fake accounts). My intention by this thesis is to identify the anonymous users / accounts through the profound investigation of these Social media network and detect the culprit / fake account user and mean while educate the victims on how to use internet wisely to evade from the dangers of social media network crimes and to build a protocol for investigators to investigate the anonymous account users in the social media networks

1. **Cyber Crime and Evolution**

In less than two decades, the Internet has grown from a curiosity to an essential element of modern life for millions. As with other aspects of globalization, its rapid expansion has far exceeded regulatory capacity, and this absence of authority has left space for many abuses. The problem is compounded by the fact that the Internet was fashioned on a military system designed to circumvent interference and external controls. But even those who most loudly champion its creative anarchy have come to realize that the Internet can only reach its full potential if some basic ground rules are established and if antisocial behaviour is vigorously discouraged. The challenge remains how, exactly, to do this. “Cybercrime” has been used to describe a wide range of offences, including offences against computer data and systems (such as “hacking”), computer-related forgery and fraud (such as “phishing”), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content). It has evolved from in different parts of the world to the mischievous one-upmanship of cyber-vandals to a range of profit-making criminal enterprises in a remarkably short time. Of course, criminals, like everyone else with access, make use of the Internet for communication and information gathering, and this has facilitated a number of traditional organized crime activities. But the growing importance of the Internet and our collective dependence on it has also created a number of new criminal opportunities. The well-established fraud of identity theft and pornography are the top trend of the crimes through the internet. The former is an acquisitive crime, an updated version of check kiting. The latter is a kind of electronic trafficking, transmitting contraband across borders through the Internet. A key question at the outset is whether these two activities could or should be classed as organized crime. Both are offences that tend to favor lone or small groups of perpetrators. Among the great advantages cyberspace offers to criminals are anonymity and the ability to allow otherwise unassociated individuals in different parts of the world to network on a transactional basis (through the use, for example, of bulletin boards, typical in both offences).

The inherent limitations in organizing identity theft and child pornography for the profit of standing criminal groups are discussed further below. Other forms of cybercrime, particularly intellectual property violations, may be more attractive to standing groups, and evidence has been increasing that organized cybercrime groups of some longevity are operating in areas like software piracy and other forms of copyright infringement. And there are a number of reasons why cybercrime in general and organized cybercrime in particular might increase in the near future. First, the technology of cybercrime has become more accessible. Software tools can be purchased online that allow the user to locate open ports or overcome password protection. These tools allow a much wider range of people to become offenders, not just those with a special gift for computing. For example, the proprietors of the recently discovered “Mariposa” botnet (a network of “enslaved” computers), perhaps the largest in history, were said not to have advanced hacking skills. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices. While skilled cyber thieves would likely see no advantage in working for a standing organization, these tools could allow criminal groups to employ large numbers of relatively unskilled individuals to labour on their behalf.

Second, In Sri Lankan profile of Internet users is changing. In 2017, the number of Internet users in developing countries surpassed the number in industrial countries. If these new users were no more likely than those in developed countries to be predators, the number of predators should continue to expand rapidly. But the number of high-value victims, largely located in richer areas, will remain more or less the same. As a result, the intensity of the attacks on this unchanging victim pool will likely grow. The Internet has made high value victims as accessible as local ones for perpetrators in the developing world.

Finally, each new offender can increase the number of attacks exponentially through the growing use of automation. Many millions of unsolicited bulk spam messages can be sent out by automation within a short time frame. Hacking attacks are often also now automated11 with as many as 80 million hacking attacks every day12 due to the use of software tools that can attack thousands of computer systems in hours. Recently, a botnet was detected involving 12.7 million infected computers, include those of many of the world’s biggest corporations. The capacity to launch millions of attacks is relevant for two reasons: It makes viable criminal strategies that would otherwise be unprofitable due to the high failure rate. For example, despite widespread knowledge of the nature of advance fee fraud and phishing schemes, these remain profitable because the perpetrators need only succeed in locating one or two marks in millions of attempts. It allows cyber thieves to fly under the radar by taking only a small amount of money from a large number of victims, decreasing the chances of detection.

1. **Bullying in Cyberspace**

Cyber bullying is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. And Cyber bullies may also disclose victims' personal data (e.g. real name, address, or place/schools) on websites. This could be done via

1. Text messages or images,

2. Personal remarks posted online,

3. Hate speeches,

4. Instigating others to dislike and gang up on the target by making them the subject of ridicule in forums, and

5. Posting false statements in order to humiliate or embarrass another person.

1. **Click fraud**

Click-fraud is occurs when a person (or an automated computer program) sham-clicks on a pay-per-click Advertisement. This is done for the purpose of generating a charge per click without having an actual interest in the ad’s content. Click fraud is done by companies to deplete their competitor's advertising budget or by websites to gain revenue. Some web sites pay people from remote places to make fraudulent clicks on an ad in order to inflate their customer's bills. Click bots can also be used for click fraud. These small pieces of code can be spread like viruses on many computers in order to generate clicks from different IP addresses. The most intelligent scams involve a malware that adopts a low profile and generates only a few clicks per computer in order to avoid detection. These bots are generally controlled remotely by the person who wishes to limit the clicks to ads that can generate a boreal profit. Hard to detect in the beginning but can be spotted eventually. The reason is that sham-clicks increase an advertiser's pay-per-click fees but don't generate sales.

1. **Cyber Stalking**

Cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats

against the victim's immediate family. Cyber stalking is also referred to as online harassment and online abuse. A cyber-stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

1. **Defamation**

A person's reputation is his or her property and sometimes even more valuable than physical property. Defamation is injury to the reputation of a person. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. e.g. Sameera publishes defamatory matter about Sujatha on a website or sends e-mails containing defamatory information to Sujatha's friends. The three essentials of defamation are:

1. the statement must be false and defamatory,

2. the said statement must refer to the victim, and

3. the statement must be published.

1. **Email Spoofing**

A spoofed email is one that appears to originate from one source but actually has been sent from another source e.g geetha has an e-mail address [geetha@asianlaws.org](mailto:pooja@asianlaws.org). Her ex-boyfriend, Sameera spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Geetha, her friends may take offence and relationships may be spoiled for life.

1. **Identity Fraud**

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity. This is done typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft can suffer adverse consequences if held accountable for the perpetrator's actions. Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number without permission and commits fraud or other crimes. It’s a type of fraud which involves stealing money or gaining other benefits by pretending to be someone else. Having your identity stolen can be both financially and emotionally devastating.

1. **Impersonation**

Online impersonation is one of the most dangerous kinds of online reputation problems. It happens when someone else assumes your identity and communicates using your real name, photograph or avatar. Impersonator could either hack into your real accounts; or just create fake profiles or comments purporting to be “you.” The motivation behind the act may be revenge, sadism, extortion, or playing some kind of twisted prank. The damage to reputation caused by impersonating someone online can be substantial and hard to cope with.

1. **Lottery Scam**

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification that says "You have won!" a large sum of money in a lottery. The recipient of the message — the target of the scam — is usually told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but will never receive any lottery payment. Victims who do actually pay the requested fees will probably find that they receive continuing payment demands to cover "unexpected expenses". The requests for money will go on until the victim realizes what is happening or has no further money to send. In some cases, the scammers give victims the option of opening an account at a particular bank as an alternative to paying upfront fees. However, this "bank" which is completely bogus, will insist on an initial deposit Money as a requirement for opening the account. The fake bank will have a legitimate looking website to reinforce the scam. Many email lottery scams use the names of legitimate lottery organizations or other legitimate corporations/companies, but this does not mean the legitimate organizations are in any way involved with the scams.

1. **Nigerian 419 Fraud Scheme**

A Nigerian 419 scam is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. The term, "419" comes from the section of the Nigerian Penal Code outlawing fraudulent criminal activities by its citizens. While the scam is not limited to Nigeria, Nigerians have become so associated with this fraud that it is widely known as Nigerian scam or 419scam. In 2005 Lagos in Nigeria was widely considered the world's leading place for scam crimes.

Few methods used: A new scam targets people who have posted their resumes on job sites. The scammer sends a letter with a falsified company logo. The job offer usually indicates exceptional salary and benefits and requests that the victim needs a "work permit" for working in the country and includes the address of a (fake) "government official" to contact. The "government official" then proceeds to fleece the victim by extracting fees from the unsuspecting user for the work permit and other fees till the victim realizes the scam. A modern activity is advertising automobiles on websites. They list a (non-existent) high value car with a low price as bait to attract buyers eager to buy quickly. The scammer says "I am not in the country, but if you pay me first, a friend will drive the car around to you". The payment required may be the full price, or a deposit, but it would not be an insignificant fee. The victim never sees the car, as it does not exist. The scammers use email only, as they know that the sound of their voice and their attitude will give them away as being high risk. The con artist approaches the victim on an online dating service, an Instant messenger, or a social networking site. The scammer claims an interest in the victim, and posts pictures of an attractive person. The scammer uses this communication to gain confidence, and then asks for money. The con artist may claim to be interested in meeting the victim, but needs cash to book a plane, hotel room, or other expenses. In other cases, they claim they're trapped in a foreign country and need assistance to return, to escape imprisonment by corrupt local officials, to pay for medical expenses due to an illness contracted abroad, and so on.

1. **Packet Sniffing**

All network data travels across the Internet, and then into and out of PCs, in the form of individual, variable size, "data packets". Since the typical PC user never "sees" any of this raw data, many spyware systems covertly send sensitive information out of the user's computer without their knowledge. Packet sniffing is a method of tapping each packet as it flows across the network i.e., it is a technique, in which a user sniffs data belonging to other users of the network. Packet sniffers can be used as an administrative tool or as a hacking tool. It depends on the user. Network sniffers can capture passwords and other sensitive pieces of information passing through the network.

1. **Phishing & Spoofing attacks**

In the 19th century, British comedian Arthur Roberts invented a game called Spoof, which involved trickery and nonsense. This gave the English speaking world a new word that today symbolizes a gamut of hacking technologies. Spoofing attacks primarily include e-mail spoofing, SMS spoofing, IP spoofing, and web spoofing. Spoofing attacks are used to trick people into divulging confidential information (e.g. credit card data) or doing something that they would usually not do (e.g. installing malicious software on their own computers). Such use of spoofing attacks is commonly referred to as Phishing. Sending an e-mail from somebody else’s e-mail ID is the simplest form of **Email spoofing**. Innumerable tools exist on the Internet which can easily be used to send e-mails appearing to have been sent by somebody else. The effects are intense. **SMS spoofing** is very similar to e-mail spoofing. The major difference being that instead of an email ID, a cell phone number is spoofed and instead of a spoofed e-mail, a spoofed SMS is sent. **DNS spoofing** involves manipulating the domain name system to take unsuspecting victims to fake websites (that look identical to the original ones). Sitting at the computer you may type in www.asianlaws.org but the site that opens up may be a fake site! This can and has been done at the local organizational level (e.g. by host file rewriting or by a network administrator with malicious intentions) or at the national or international level (by hackers exploiting vulnerabilities in the BIND software that runs most of the world’s domain name servers).

1. **Pornography**

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in Sri Lanka. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Sri Lankan Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as “offensive to modesty or decency; lewd, filthy, repulsive.

1. **Smishing**

This is morphology of SMS and phishing – SmiShing. It is the same as "phishing," in which you receive an email that seems to be from a reputable source, asking for your credit card data, password, or other private information. Only instead of an email, smishing takes place through the SMS text messages you

receive on your cell phone.

1. **Social Engineering**

In the realm of computers, it is a non-technical technique- the act of obtaining or attempting to obtain secure data by deceiving individuals into revealing secure information is social engineering. It is the art of psychologically manipulating victims of social engineering into performing actions or revealing confidential information without realizing it’s a fraud. In most cases the attacker never comes face-to-face with the victims. They rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. A social engineer runs what is to be called a con game. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Social engineering techniques appeal to the victims’ kindness, appeal to vanity, appeal to authority, appeal to greed, and old-fashioned eavesdropping.

1. **Vishing**

With the growth of mobile banking and the ability to conduct financial transactions online, Vishing attacks have become even more attractive and lucrative for cyber criminals. It is the

telephone equivalent of phishing. The term is a combination of “voice” and phishing. Vishing is

the criminal act of using voice email, VoIP (voice over Internet Protocol), landline or cellular telephone to gain access to private, personal and financial information from the public for the purpose of financial reward by committing identity theft. It is typically used to steal credit card numbers by a scammer who usually pretends to be in legitimate business, and fools the victim into thinking he or she will profit. Vishing is very hard for legal authorities to monitor or trace. Thus it is onto the consumers to protect themselves, by being highly suspicious when receiving messages directing them to call and provide credit card or bank numbers. When in doubt, calling a company's telephone number listed on billing statements or other official sources is recommended instead of calling numbers from messages of dubious authenticity.

1. **Related Projects/ Previous Research**

The related Projects or Previous Researches could not be found in university level or web sites according to my searching capacity but some different approaches have been explained in some sites as followings. When do a deep search one approach regarding to finding Facebook users IP Address through chat and email header before but none of these two works. The Facebook chat runs on XMPP protocol now which is not peer-2-peer, so it is not possible to determine the IP address of the user through Facebook Chat using **Netstat** command. By using some social engineering skills and default ‘**Banner grabbing**' technique of a web server could be get information in a computer system. The **Banner Grabbing** is an enumeration technique used to get information about a particular computer system on a network/internet (Information like Operating system, browser, IP address, etc.) but some social media networks run on XMPP protocol then this technique could not use to identify the anonymous account users.

Another approach is while the use of cookies and other tracking mechanisms used to track computers is widespread and well understood, it is often believed that the data collected is effectively de-identified; that is, the cookies track the computer browser, not the person using the computer. This is the message often promulgated by the advertising industry: tracking cookies allow targeted advertising without compromising personal privacy.

In the new study ***'*De-anonymizing Web Browsing Data with Social Networks*'*** the researchers show that de-identified web browsing histories can be linked to social media profiles using only publicly available data. Once the social media profile associated with a browsing pattern is known, the person is known.

"Users may assume they are anonymous when they are browsing news or a health website," but my work adds to the list of ways in which tracking agencies may be able to learn their identities." "All the evidence we have seen piling up over the years showing the strong limits of data anonymization is really emphasizes the need to rethink our approach to privacy and data protection in the age of big data." The problem goes beyond simple user privacy, since it could be used to target persons of interest. "The idea would be to look at something such as social media account and to determine what links which have being seeing And then, could be to find the 'User X' with the highest correlation between site visits and links seen

1. **Legislations and Legal Provisions for Social Media Crime Investigation**
2. **Computer as Target**

* Using a Computer to attack victim computers
* Attacks on the confidentiality, integrity or availability of information or systems

1. **Computer as Tool**

* Fraud
* Gambling
* Pornography
* Piracy
* Harassment

1. **Computer as Accomplice**

* Personal information (diaries, downloaded e-mails)
* Contraband (porn)
* Stolen Information (trade secrets, credit cards)
* Key evidence unknown to suspect

The cyber crimes are increasing in day by day; generally this crime is based on internet. As well as there is no limit to this kind of crime they impact on entire world. So that Effective Legal system must be established for stopping that computer related crime. Accordingly Sri Lanka Government introduced an act called computer crime act on 24 of 2007. Following captions were covered and discussed by this act and other computer related crimes have been covered other acts.

1. **Computer crime act on 24 of 2007**

The provisions of this Act shall apply where

(*a*) A person commits an offence under this Act while being present in Sri Lanka or outside Sri Lanka;

(*b*) The computer, computer system or information affected or which was to be affected, by the act which constitutes an offence under this Act, was at the material time in Sri Lanka or outside Sri Lanka;

(*c*) The facility or service, including any computer storage, or data or information processing service, used in the commission of an offence under this Act was at the material time situated in Sri Lanka or outside Sri Lanka ; or

(*d*) the loss or damage is caused within or outside Sri Lanka by the commission of an offence under this Act, to the State or to a person resident in Sri Lanka or outside Sri Lanka.

1. **Notable Provisions defined in section 1 and 2**

* On the occasion of a person committing a crime under this Act while residing in Sri Lanka or outside Sri Lanka.
* A Computer/Program affected as a result of an Act committed which amounts to an offence under the Act “in Sri Lanka or outside” during the relevant period.

1. **Crimes are defined in section 3 to 14**

* Section 3 – An Act resulting in accessing the computer system illegally.
* Section 4 – An act committed in order to illegally access the system to commit a crime.
* Section 5 – Performing a computer function without proper authority.
* Section 6 – Crimes against national security (National Security, National Economy and Public Security).
* Section 7 – Using data obtained illegally.
* Section 8 – Obtaining date illegally.
* Section 9 – Providing illegal assistance to commit a crime.
* Section 10- Revealing data without proper authority to access.
* Section 11 – Attempting to commit a crime.
* Section 12 - Aiding and Abetting a crime.
* Section 13 – Conspiring to commit a crime.
* Section 14 – Offering financial grant as a reward for profit or loss consequent to committing a crime.

1. **Special Procedures defined in section 15 to 25**

* Sections 15 and 16, the applicability of provisions of sections 15 and 16 of Crime Act No.15 of 1979 are defined.
* Section 17, a specialist is defined. (A special committee appointed by the Minister consisting of academics of the University. Powers delegated to persons above the rank of Sub Inspector for investigation and checking of premises).
* Section 18 – Powers to check and confiscate.
* Section 19 – Powers to protect data and systems involved in the investigation.
* Section 21 - Arrest (Should be by an officer not below the rank of SI (Sub Inspector) nominated as per gazette notification issued by the IGP (Inspector General of Police) who in his opinion has enough credentials to check and forfeit.

Section 25 - Jurisdiction (Delegated to the Supreme Court).

1. **Other Acts related to the Computer Crime**

* PAYMENT DEVICES FRAUDS ACT No. 30 OF 2006
* OBSCENE PUBLICATION ACT No. 22 OF 1983
* CODE OF CRIMINAL PROCEDURE ACT No. 15 OF 1979
* PEANAL CODE No. 02 OF 1883
* ELECTRONIC TRANSACTIONS ACT No. 19 OF 2006
* INFORMATION AND COMMUNICATION TECHNOLOGY ACT No. 27 OF 2003
* INTELLECTUAL PROPERTY ACT No. 36 OF 2003
* PAYMENT AND SETTLEMENT SYSTEMS ACT No. 28 OF 2005

1. **Positives and Negatives of social Networks**

Relatively a social networking is new advance in technology, they are various sites that people can make personal profiles, share their pictures, videos to their family, friends and other people from the entire world. So it's easy to get carried away with interactions and attentions you can have 24 hours per day on social networks sites, but there are many positives or negatives of these social networks on our social life.

1. **Positives of social Networks**

1. The main goal of the social network is to be able to keep in touch to families and friends in today's fast-paced and ever changing worlds.

2. Social networking is a wonderful method to finding people with common interests

3. Social networks are invaluable promotional tool. Organizations, Musicians and artists can meet an impossibly great and varied amount of audience using social network sites. This helps them to deliver their products in a way that has never been seen before.

4. By social network sites breaking news and other important information spreads unbelievable quickly.

5. Social networks helps to catch and convict criminals. Sometime people often do not take in their account the consequences of what they post in their social site. When they doing illegal things that things also Photograph by themselves, or even they bragging to share about crimes they have committed are all things that law enforcement use to persecute these criminals. Also, they use these social sites to identify and solve existing cases.

1. **Negatives of social networks**

1. Social networks perpetuates false and unreliable information, within hours or days anything can diffusion to millions of people on social networks. Unluckily, this also includes things that are not true or made up. this information can cause scare and intense misinformation in society.

2. Social networks causing great relationships problems. Although the social networks are used to starting new relationships, but forget many others. It is so easy to communicate and share plans or pictures with a person on social networks and keep it completely under wraps. This new seduction have been leading wedges into people's offline relationships, real life, oftentimes ending them for good.

3. Cyber bullying is a growing problem in social networks. Not always having access to people's lives at all times is a good thing. A new direction of cyber bullying is wreaking destruction all across the world. This is particularly true with young kids. They are publicly inconvenience one another, and posting defamatory things which are broadcasted to the entire cyber bullying world.

.

4. Social networks are used to profile and discriminate in the job world. Everyone has a social networks account that shows what they look like, the type of life that they live, what they look like, and how old they are. Workers are using to their benefits is some very worrying ways. The Jobs that are looking for some standard of person, but cannot legally express these standards, are using social networks to pre-screen their applications.

5. The addiction is real in social networks. One of the major problems with the social networks craze is that people are becoming more and more addicted to using it. It is the first time waster at job, at home, and in school.

1. **Prevention of Crimes Committed through the Social Media network**

It is very essential to educate especially the schoolchildren of this danger via a popular network. It is pertinent to mention that there is increase in the crimes committed via Facebook. It is the most popular network, which can easily disseminate the information to the society. Any pictures or video could be loaded into this network and passed on to the society. More than 300 million people are using the Facebook. Nearly 6 billion minutes are spent on Facebook in a day. Like schoolchildren, young people also uploading unlimited pictures are sharing among the friends. In this instance, they must segregate good ones from bad and upload only good ones. Mostly female children are more vulnerable for cybercrimes. There are several matters to be concerned when using cyberspace.

1. **Safety on Social networking sites.**
2. Do not share your personal information such as date of birth, residence, contact details on cyberspace.
3. Except your intimate friends, do not add unknown people on your list. Think not only twice but several times when inviting unknown people to Facebook and Skype. Under no circumstances, do not accept invitations from outsiders or unknown people on cyberspace. Treat them as suspicious characters. Their intention may be to fulfill their sexual desires. It is important to tell the female children not to have any contacts with such people. Do not give any opportunity to meet such people. This may create a dangerous situation.
4. Be vigilant about the people who will on the pretext of helping in education take you to the social activities. Some elders may invite you by enticing you with the promise of scholarship. Avoid them in such situation.
5. Even with the same age group of friends, do not have unnecessary communication via cyberspace. Until you verify the authenticity of the person who make a friend request, avoid having any communication with the suspicious characters.
6. Be vigilant of any emails that you receive from suspicious characters.
7. Avoid chatting with unknown people. Do not provide any information disclosing your identity. Do not upload any photograph of yours to them.
8. When dealing with Facebook, have a password that cannot be presumed by anyone. Changed the password very often. We always have a password with a familiar words or numbers which could be presumed easily.
9. Only enter into a computer, which could be trusted. When using a computer outside if your password is shared, make sure you lockout carefully from the computer. This is very important to remember.
10. Be vigilant of the people who would identify themselves by different manes.
11. A strong password is a necessity and it has to be changed regularly. Be attentive when using passwords on emails.
12. If a suspicious person has sent a mail or photograph, do not erase them from the system.
13. When you give your mobile phone to someone, remember to remove the sim card and other data. When you are reloading your mobile phone if you had shared your mobile number with him, reject any calls or cyberspace communication from him.
14. **Safety on electronic mail**

* Create a strong password containing at least a minimum of 8 characters. The password should not contain names or other easily guessable words. It should consist of uppercase, lowercase, numeric and other characters such as &\*@# etc.
* Always use https when connecting to webmail services – e.g. [https://www.hotmail.com](https://www.dropbox.com/referrer_cleansing_redirect?hmac=of%2BggMfDRd5y2VOXEbZJTKg7chB92niqxgMdYZK6dTY%3D&url=https%3A%2F%2Fwww.hotmail.com)
* When a digital certificate error message is encountered proceeding further to the login page should be stopped.
* Password should never be shared with other people.
* An up to date antivirus scanner should be installed.
* Do not open any mails received from unknown people.

1. **Precautions for safe guarding children becoming online Victims**

* Installing personal fire wall software or using parental control software on computers used by children. This type of software can provide parents with history of activities and also enables parents to restrict children accessing certain content.
* Keeping a track of all the sites children frequently visit and monitor their online activity.
* Improving communication with children to educate them on the potential risks of becoming an online victim and how to stay safe on the Internet.
* Keeping the computer in an open place where child’s movements could be seen by everybody. If the child gets agitated and change or switch the monitor when an elder walks into the room it is a warning sign to be alert.
* Avoiding unsupervised use of Internet by children.
* Discouraging the child from emailing, chatting and telephoning unknown persons.
* Making the child aware of the damage that may be caused to the computer and the harm that may be inflicted on the child when downloading material that are unknown to the child.
* Preventing children from using Internet accounts of others.
* Taking extra care when the child prefers to be alone on the computer.
* Monitoring child’s conversations with unknown persons.
* Taking precautions against the child using credit card without permission.
* Ensure that no pornographic literature is found on the child’s computer.

1. **Measures to be taken in the event of Victimization**

* If you became a victim, take measures immediately.
* The extent of the damage caused by the cybercrime depends on the nature of the crime and how it has been committed. Chances are more for the victim to be placed in an insecure position and also be treated with contempt, disgrace and differently within her family, in school, at her workplace and within the community.
* When a child is victimized by cybercrime, we must take a special care of that child. Therefore, it is important that psychological counseling be offered to the victimized child.
* Also provide them with the required technical guidance and advice so that they would be equipped with appropriate knowledge in protecting themselves against the present perpetrator and also the probable future perpetrators.
* In the above instances, make a complaint with CERT and Cybercrimes Unit of the Police. It is essential to educate the girl children of the procedure when they become victims of cybercrimes.

1. **Immediate Measures to be taken**

* If cybercrimes are committed through emails, these emails should be preserved even though they have been forwarded to other people. Such email communications should not be deleted.
* Taking a screen shot of a fake image as the image may not be there when you return after complaining.
* Obtaining the Internet bill from the Internet service provider.
* Protect the scene of crime.
* Make a complaint to the police
* Take action against the perpetrator.
* Take measures to protect the victim.

Chapter 3

**DESIGN**

The chapter will discuss about the abstract overview of the Protocol and the objectives that are going to achieve from the design. Furthermore it will discuss the methodology and in detail concepts which underline for each and every steps of the Protocol. In order to build sound and complete to the De-anonymizing protocol for SMN, already identified the requirements, functional details and tool architecture by analyzing the information gathered through the literature survey. The identified limitations in the current approaches were considered in designing the tool architecture and several design concerns were identified.

1. **De-anonymizing Tool Design**

Designing of the De-anonymizing tool is mainly focused into three models phases which are very important in this Protocol throughout the all investigations. The models consist 1). Draft Designing Model, 2). Hosting Server Designing Model, 3). Client Server Designing Model as follows

1. **Draft Designing Model**

In this model the investigator should be focused more into the design of this page or link because if any doubt or suspicious activity occurs during the conversation due to any error of JAVA code and prepared page /link thereafter other end user will not accept or respond to the page /link. Actually the JAVA code needs to embed with uploaded page, picture, video or any document then other end user should not suspect the embedded page or URL link address.

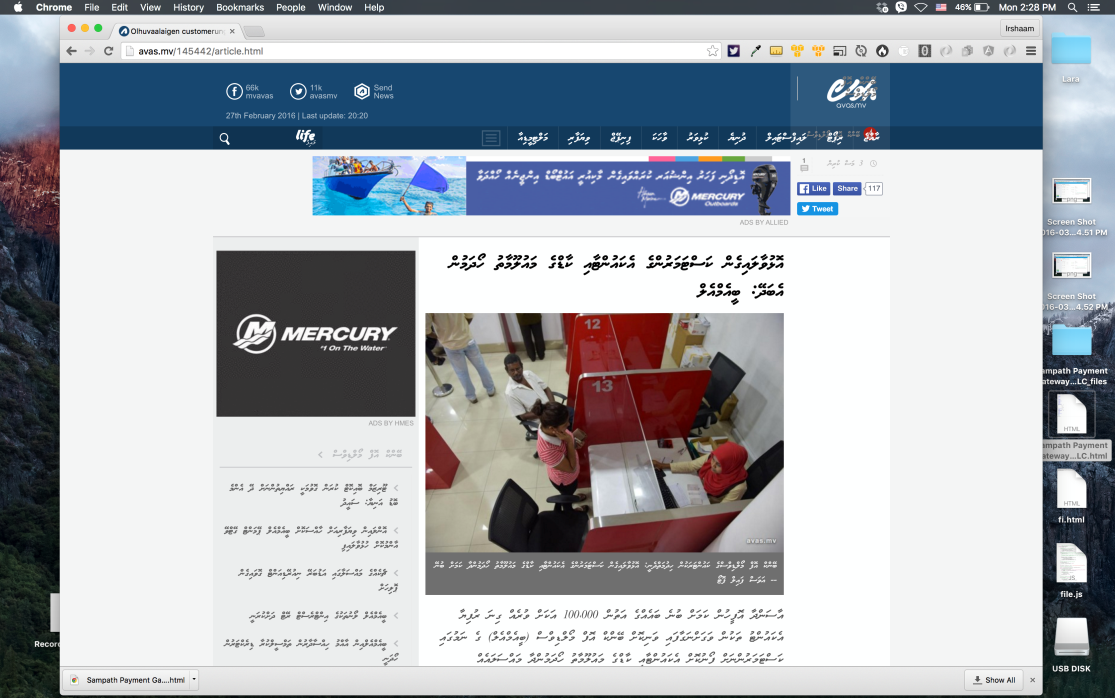


Figure 3.1 the selected page for the Draft

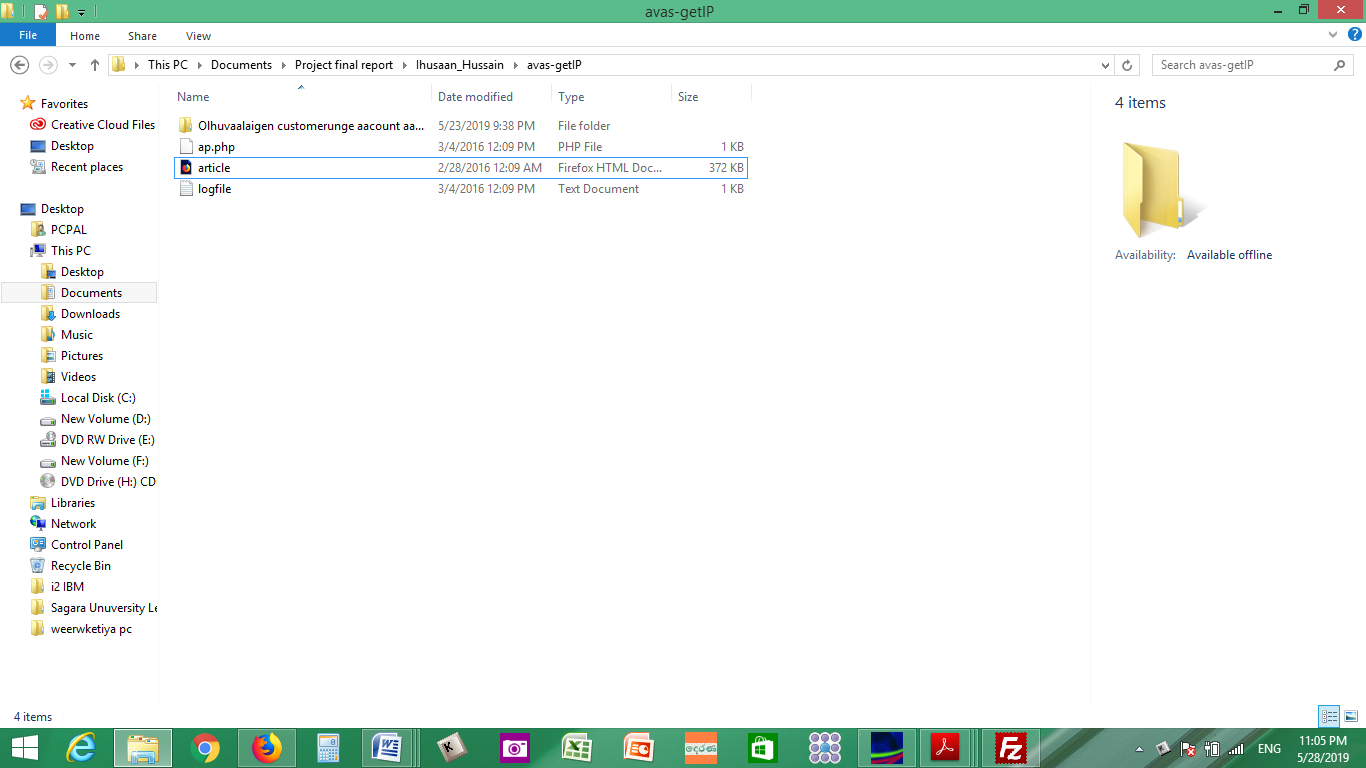


Figure 3.2 Downloaded the selected page and preparing other files

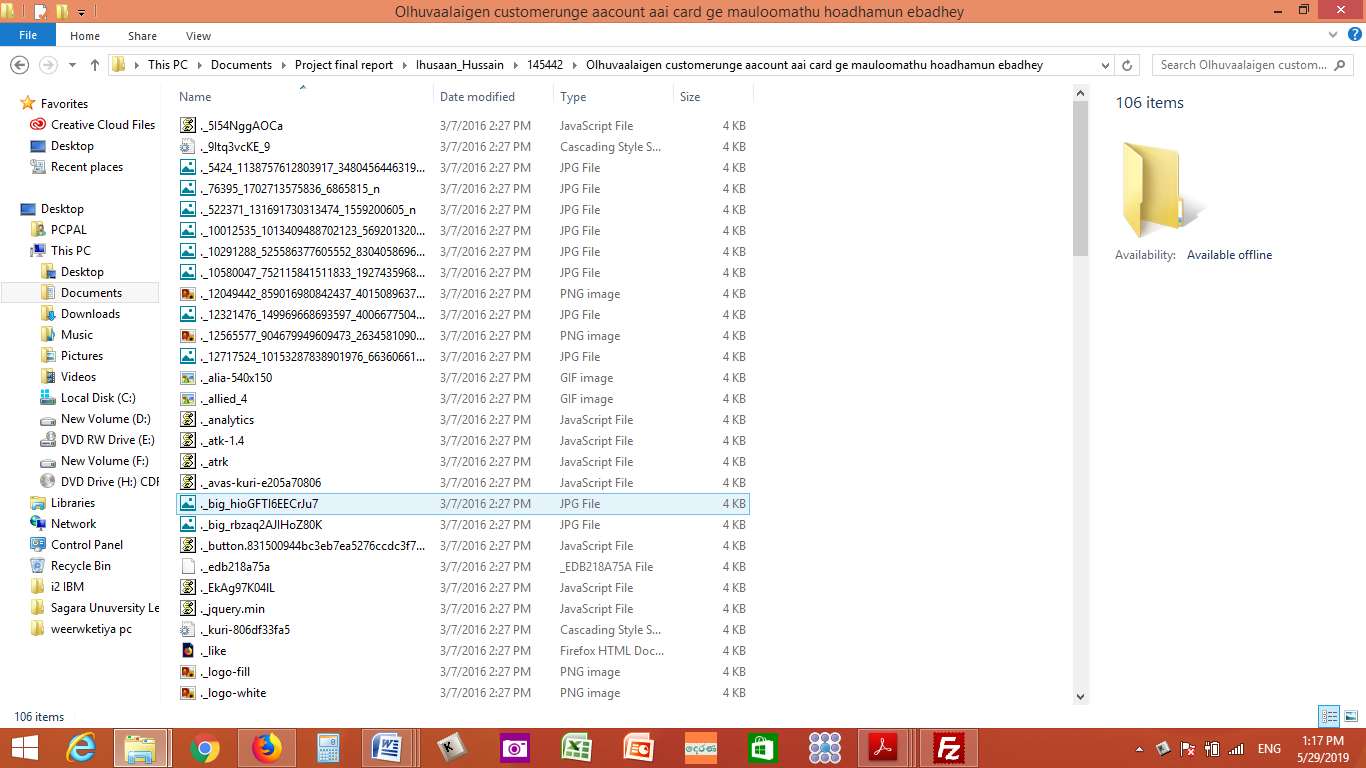


Figure 3.3 content of the downloaded file

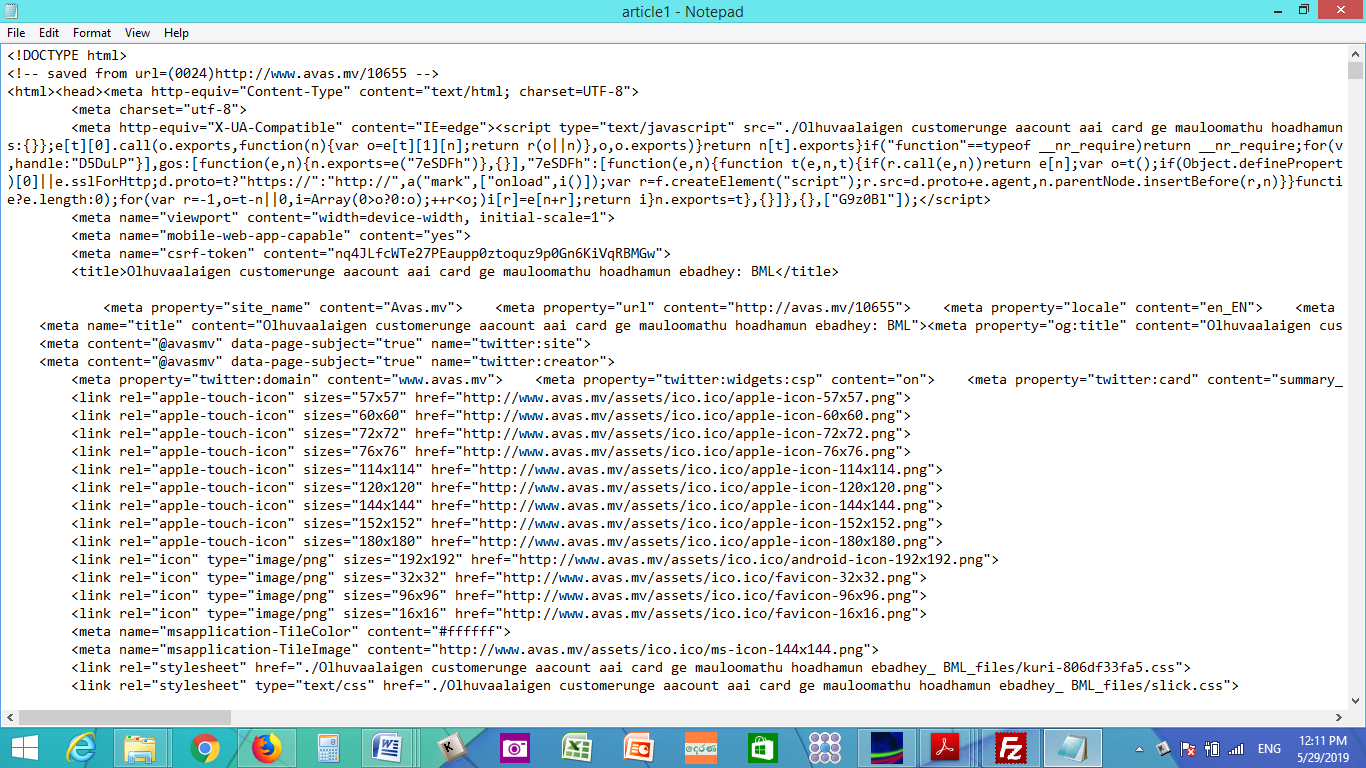


Figure 3.4 content of the embedded file

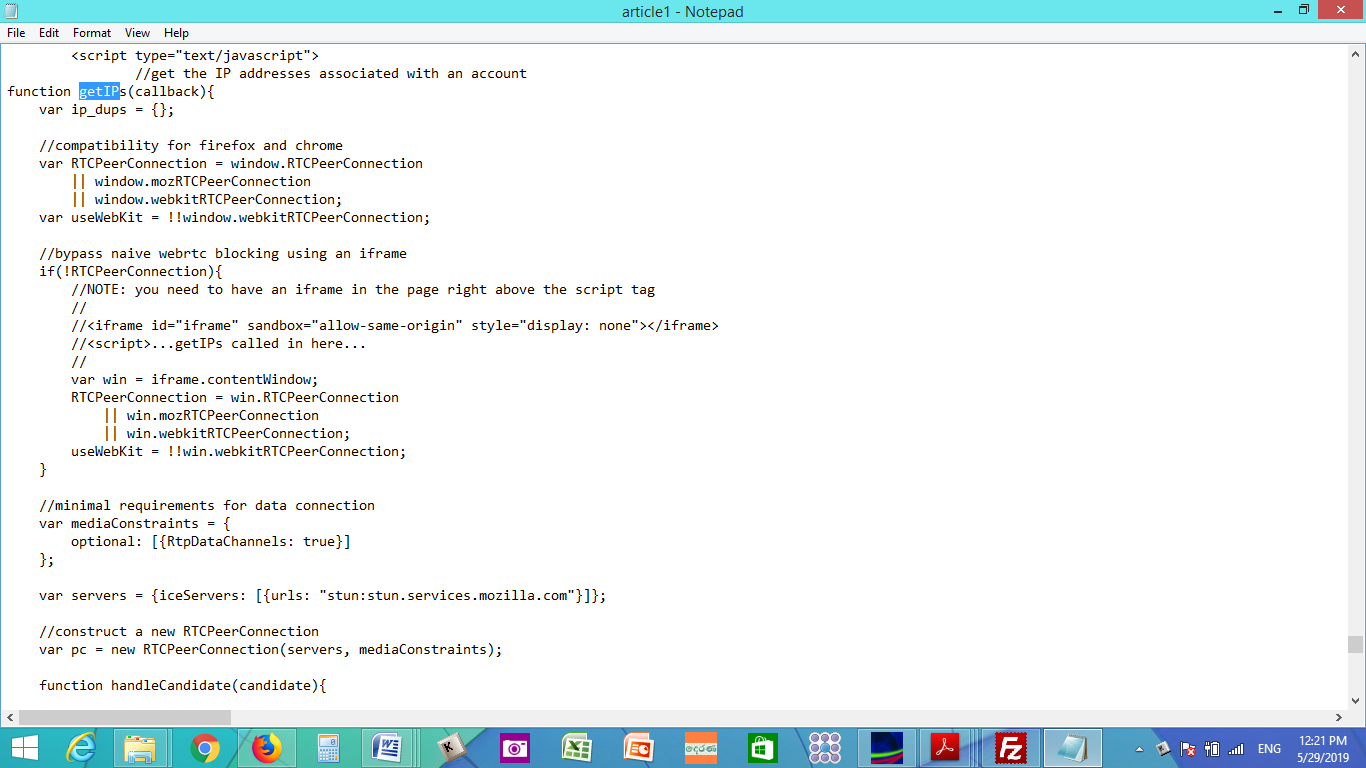


Figure 3.5 The JAVA scripts which is calling targeted Meta data

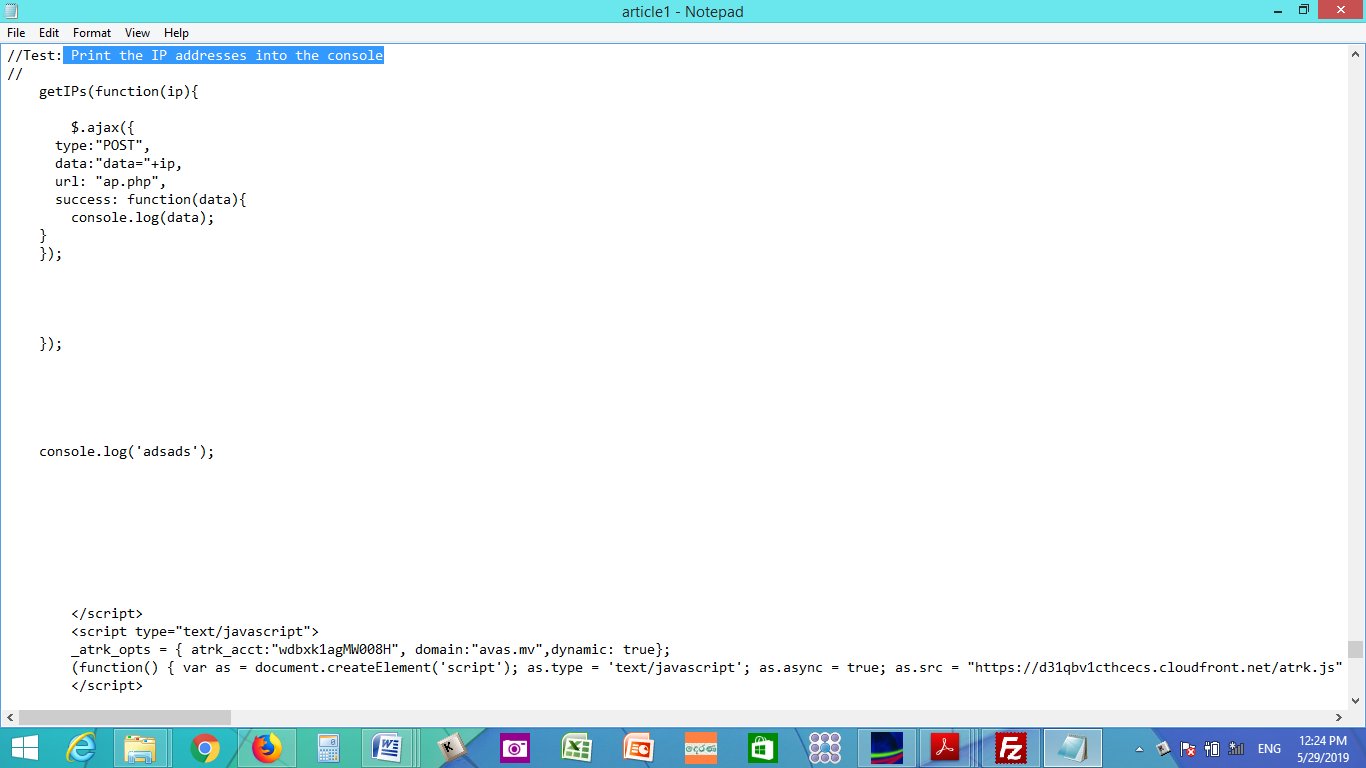


Figure 3.6 The JAVA scripts which is calling targeted IPs

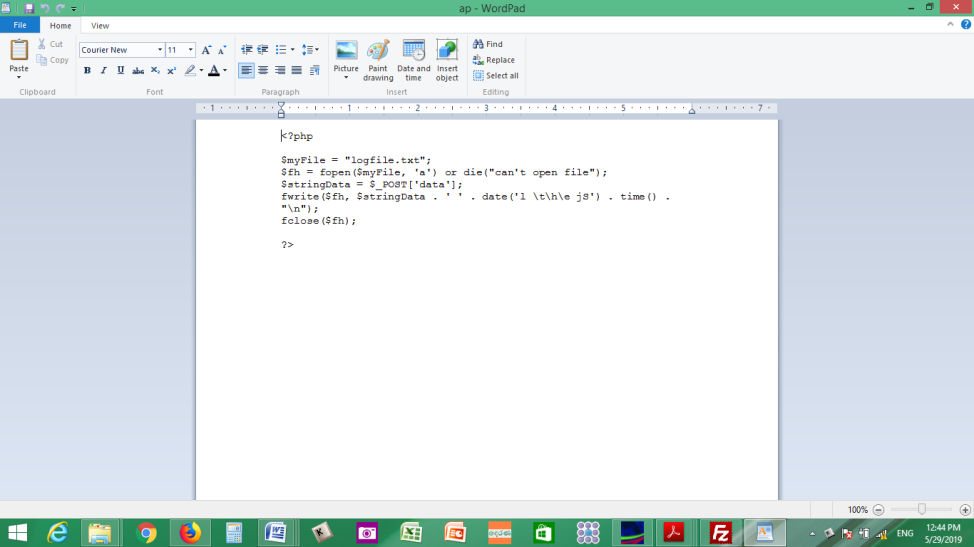


Figure 3.7 The JAVA scripts of PHP file and writing data into Text file

1. **Hosting Server Designing Model**

This also more important task before upload the prepared files to the server the investigator want to have details of the anonymous user and his favorite's habits and other activities. Most of the time, the server has to select or choice according to the behavior of the anonymous account user and his/her conversation type.

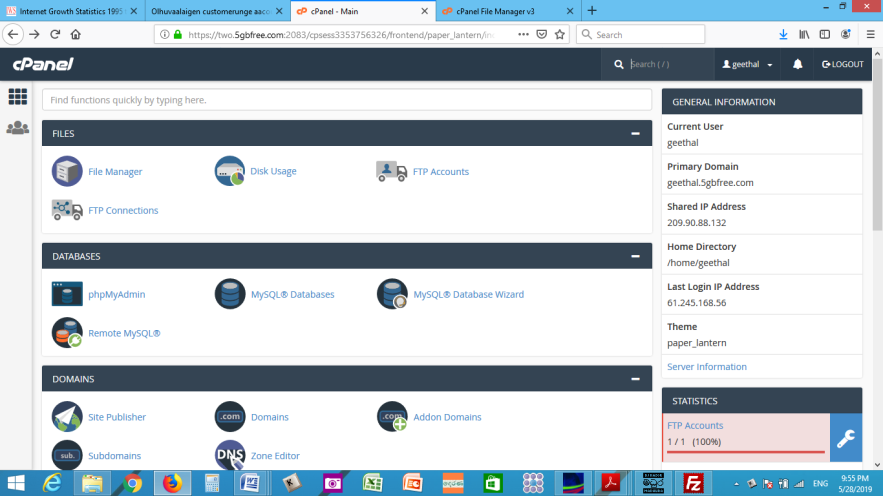


Figure 3.8 Configurations of the hosting server

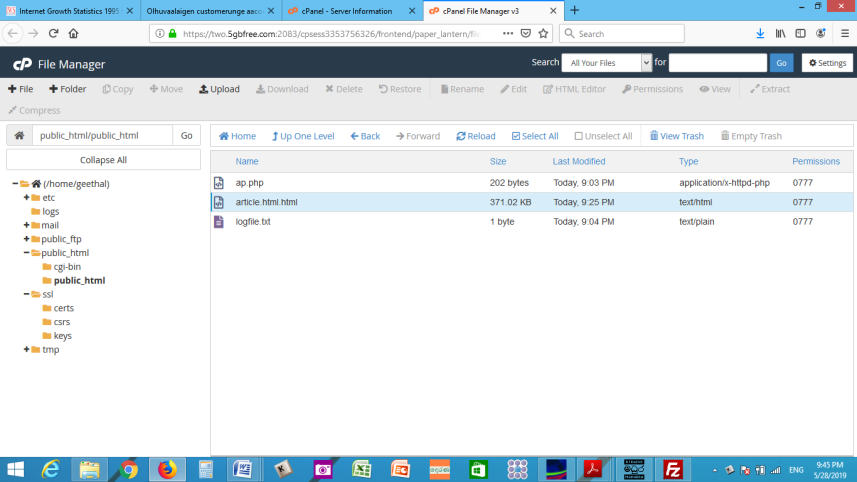


Figure 3.9 Uploaded files to server

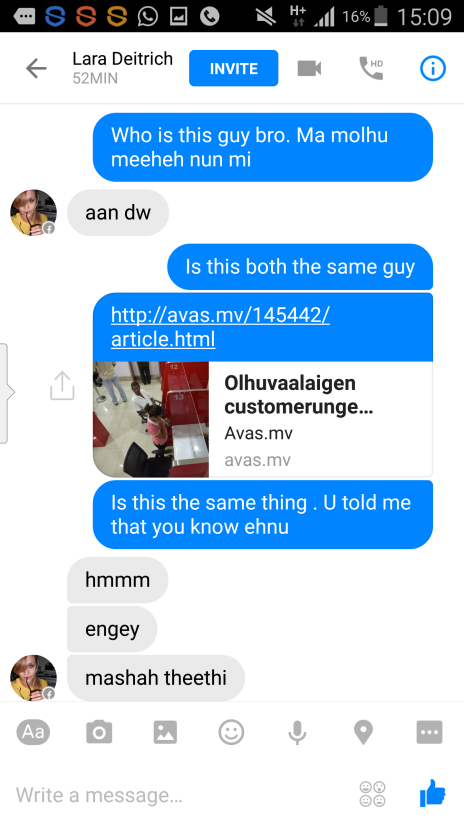
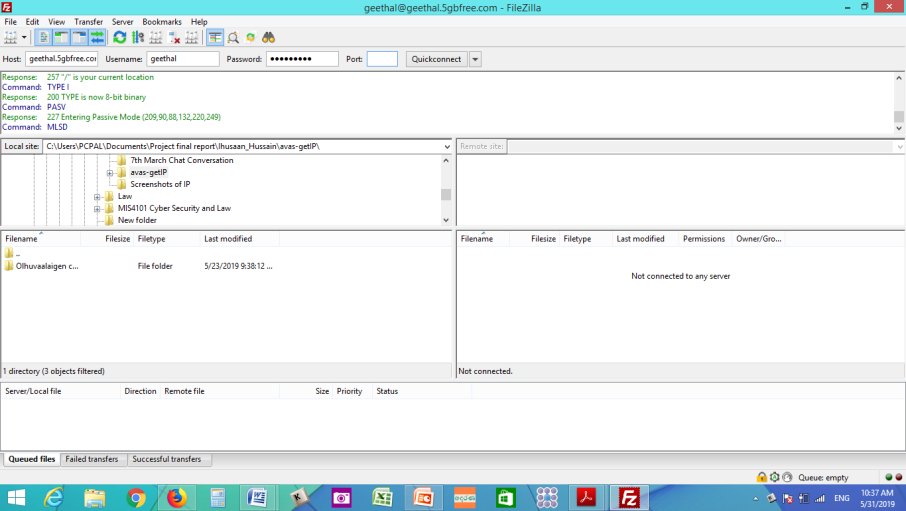


Figure 3.10 Draft message sent via SMN

1. **Client Server Design Model**

This is client server and very important phase of this De-anonymizing tool because all extract Meta data of the anonymous user's network could be monitor and expedite the investigation.

Figure 3.11 Configuration of the Client Server

1. **De-anonymizing System Architecture**

Basically the main objective of the system is to detect an anonymous account in SMN and identify the detail of the anonymous user. In order to detect the real person at behind the anonymous account and to present to the judicial proceedings, the below three main phases are integrated to the design.

**Law Enforcement Officer (LEO) & Client Server**

**Targeted System of anonymous User**

**Hosting server**

**Internet**

Figure 3.12 the De-anonymizing system architecture

1. **Detection mechanism of the De-anonymizing Tool**

**Internet**

**Target System**

**Target opens content**

**Law Enforce**

**LEO Profiles the targeted User through the SMN**

**LEO send well prepared draft**

**Data extraction to the system of the LEO**

Figure 3.13 the network architecture

Chapter 4

**IMPLEMENTATION**

This chapter discusses how to implement the De-anonymizing tool and how to conduct the profound Investigation to identify the real person of an anonymous account user of the SMN. After implementing the De-anonymizing tool, it could be used to reveal an anonymous user by getting their Private and Public IP detail which was assigned by the ISP at the real time of the committed crime. If ISP has NAT their IP then they will assign their own Private IP to connect the customer and direct to the preferred network through a public IP. Some time ISP assign two IP addresses to their client after that if client connect to a SMN then network Service Provider assign another their own IP address through their server to the account user to connect their another account in the same network. So if we try to get the one end account user's IP address then will see the IP which was assign by the network service provider (user account service provider) to the client but we could not see the real user's IP address which was assigned by ISP.

1. **Technologies and Tools**

1. **JAVA as the programming language**

Version - Java version "1.7.0 79; Java (TM) SE Runtime Environment 1.7.0 79-b15 Java Hotspot(TM) 1.7.0 79-b15 Java is high level programming . JAVA makes easy in integration.

There are different approaches have to carry-out at practical scenarios to determine the most suitable and compatible technique for the De-anonymous of SMN detection protocol. The main target of this project is to investigate the anonymous account users in the SMN and De-anonymous the users to identify their identities through the De-anonymizing of SMN detection protocol.

So by studding and doing some experiments in social media browsing data and links is going to establish a detection tool for De-anonymous the SMN users through the followings approaches.

1. **Links base approach**

The basic premise is that social media users are more likely to click on links posted by people they follow. This creates a distinctive pattern that persists in the browsing history. Then can thus De-anonymize the user through the browsing links.

1. **Browsing history base approach**

The theory is going to test against Facebook users because it is largely public, has an accessible API, and Assuming an 'adversary' has access to browsing histories, he can then easily deduces which links came from Which Facebook account user. The pattern of those referrals from Facebook account can then be used to identify the user concerned by matching it with users' Facebook profile characteristics. The same approach could also be used against users with Twiter or any other social media accounts.

1. **Text base approach**

Text base approach is investigating the exchanged chats contents of the anonymous facebook users and the victims through the Textual analysis method. Analysing texts in order to identify or extract salient relationships and information.

This project will support at a purely 'commercial' level, this could be used to target individuals with high value goods. But it could also be used to find and target specific individuals prior to a network attack.

The researchers accept that their current methodology is not 100% accurate, but add an "adversary may fruitfully make use of other fingerprinting information available through URLs, such as UTM codes. Thus, the main lesson of my project is qualitative: I am going to present multiple lines of evidence that browsing histories may be linked to social media profiles, even at a scale of hundreds of millions of potential users."

1. **Investigation Protocol**

**Step 1** Collect as much information about the anonymous account (fake profile) and If could identify the people who were connected to the profile/account is very useful for other future works are going to convey with the anonymous user. Make a list of connected people to anonymous SMN accounts and categorize the friends and other connected persons.

**Step 2** Select any one of close friend or relative on that list (select most trusted person). The person which have selected will be doing the entire job. If there is nobody can trust on this list then ask any of that trusted friends to be friend that anonymous (fake profile) user. Or otherwise can prepare a famous or running incident as news, a gossip or an interesting article which should be attract the anonymous user to connect or build a communication.

**Step 3** Ask that victim to start chatting with anonymous (fake) user casually every day. Do not show the different nature or behaviors to the anonymous user. (Remember whatever do should be remain between that friend. do not let it spread among other close friends)

**Step 4** If the step3 could not continue then should be focused to another way to build a communication with the anonymous user. For that purpose can send a request via an avatar account (anonymous account) which should be attracted to the anonymous user especially if that anonymous user interest women so our avatar account should be compatible to the interest.

**Step 5** Ask that friend to send this shortened URL to the anonymous (Fake profile) user along with some nice message, news, article or a video via connected profile, So that should be persuaded to click on that picture , article or news with embedded java script.

**Step 6** As soon as the anonymous (fake) user clicks on its link, it will be executed and connect to hosted server of the LEO and that embedded Java Script file and Php file will call the anonymous user's IP address (private IP and Public IP) which were assigned by the ISP and it will be written to the Text.txt file of the LEO server.

**Step 7** Now that could be found out the Private and Public IP addresses of the anonymous user (fake user), Through the De-anonymizing tool.

**Step 8** After thatgo to the open source online tool like http://www.iptrackeronline.com or www.ip2location.com and enter the ‘IP addresses of the anonymous user (fake user).

**Step 9** Then could be collected the details of the *ISP, Area-code, Postal-code, Country etc*. regarding the IP address along with a Map.

**Step 11** After receiving these details which was used by the suspect. The court order could be obtained from the court. After that the law enforcement could be provided the received IPs details to the ISP and they could be easy to disclose the subscriber details for the IP addresses. If there is a match, Then it was successfully nabbed the culprit.

**Step 12** After apprehend the suspect should be produced to the court and seizing equipments should be send to the Government Analysis or Universities to get comprehensive report.

**Step 13** Completing the Investigation extracts of the case should be send to the Hon. Attorney General department for indict to the suspect.

Chapter 5

**EVALUATION**

The chapter mainly discusses the evaluation of the De-anonymizing Protocol for SMN. Evaluation process considered on the functionality of the De-anonymizing detection tool, the ability of De-anonymizing SMN and how it responds to the Law Enforcement Officers'(LEO) requirement. Evaluation has done in a open source Hosting Server and Client Server with prepared JAVA embedded De-anonymizing tool were uploaded at the hosting server. The De-anonymizing Protocol for SMN is evaluated according to the soundness, completeness, accessibility and the efficiency of the De-anonymizing tool.

The level of accessibility to a SMN data is measured by the amount of data that are legitimately expected from a SMN account or a user account. Although successful of the De-anonymizing Protocol for SMN is depending on the detected anonymous account users and identify the real suspect with clear evidence, which was the complaint mention in their given statement to the Law Enforcement Officers (LEO). If could identify the culprit of a anonymous account through the De-anonymizing Protocol for SMN, could be evaluated is it useful or helpful to LEO in their investigation level.

1. **Evaluation of the De-anonymous tool and Protocol**

At the design phase first prepared the embedded message or with any type of context communication meaning. The embedded message sent to the anonymous user via any SMN or any internet means after that the anonymous user had clicked the content of the message then embedded java script were executed and direct the anonymous user to connect to the host server of the law enforcement Office in mean while the host server will call the Meta data of the anonymous user's computer and it will be written in the Text.txt file which was uploaded to the Law Enforcement Office host server. After that using open source tool [www.ip2location.com](http://www.ip2location.com) could be found the detail of the public IP address which was get through the De-anonymizing tool and which ISP has provided to the user. With the court request from the LEO the ISP could easily to find out the user who has been used the IPs to compare with the Public IP private IP have been given by LEO. The LEO can apprehend the anonymous culprit. By using the De-anonymizing tool and protocol could be successfully detect and apprehend the suspect.

1. **The Selected Case for the Evaluation of the De-anonymizing tool**

Recently, few Maldives students have visited to Sri Lanka for higher studies mean while they studying they have organized to collect personal information of the reputed Maldives national through the social media and after that few anonymous accounts were created as modellers who could used the Maldives language and first the anonymous user build relationship with complaint by chatting and shearing personal things so after that anonymous user has bring him to video chat. The anonymous account had run a nude video at the live chat so then complaint party had shown his naked body then it was recorded by the anonymous user. After that showing this recorded video anonymous user had demanded ransom by giving a dead line, so in this case they have demanded 10 million Maldives rupea (almost one million us dollar) the victim has deposited 55 000 Maldives rupea into two bank accounts of Maldives but all money has withdraw from Sri Lanka so victim came and logged a complain in LEO in Sri Lanka. The investigation was initiated and traced the suspects through the De-anonymizing tool and received Meta data were analysed. The suspects were comprehended with the all equipment before the dead line given by anonymous user.

5.2.1 Downloaded news page from a genuine website

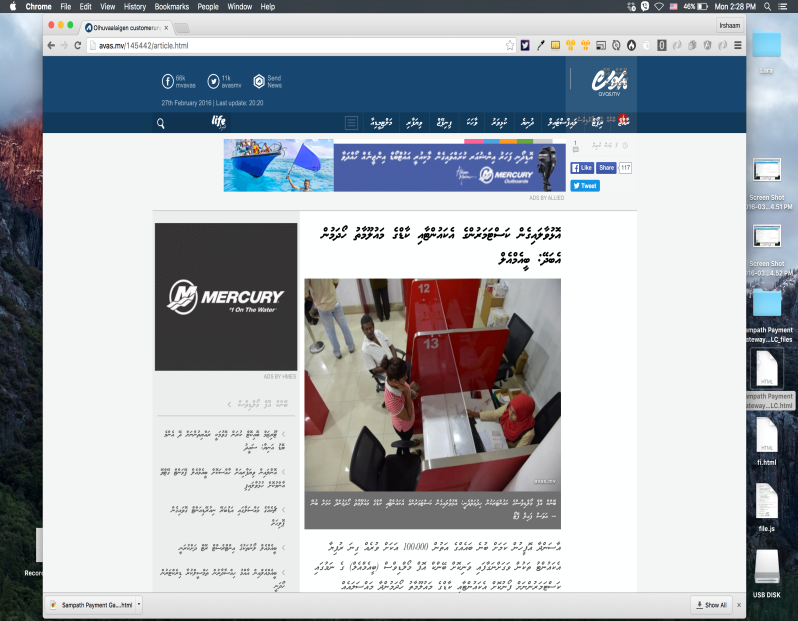


Figure 5.1 selecting website to download

5.2.2 Embedded message has been send via Facebook messenger

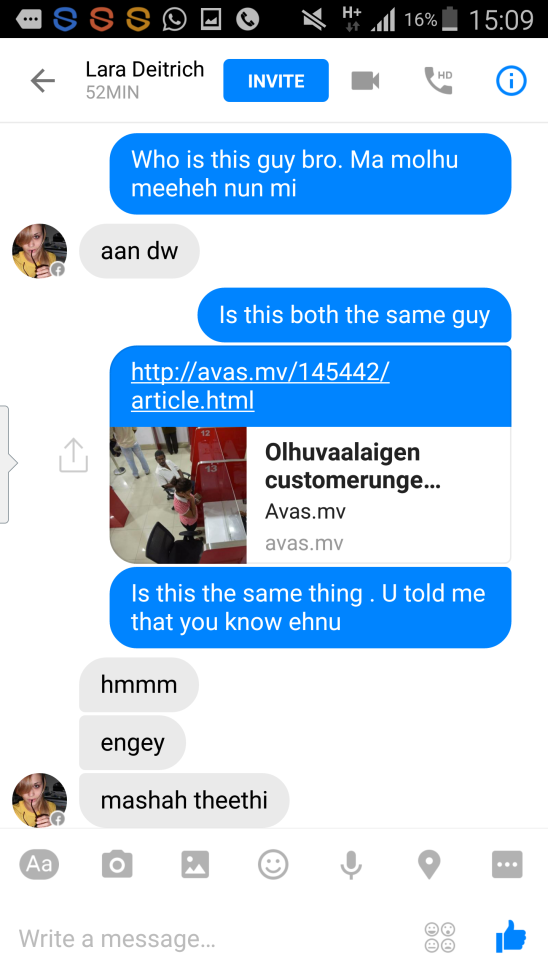


Figure 5.2 sent message via SMN

5.2.3 The Meta data, which were received from the computer of the anonymous user

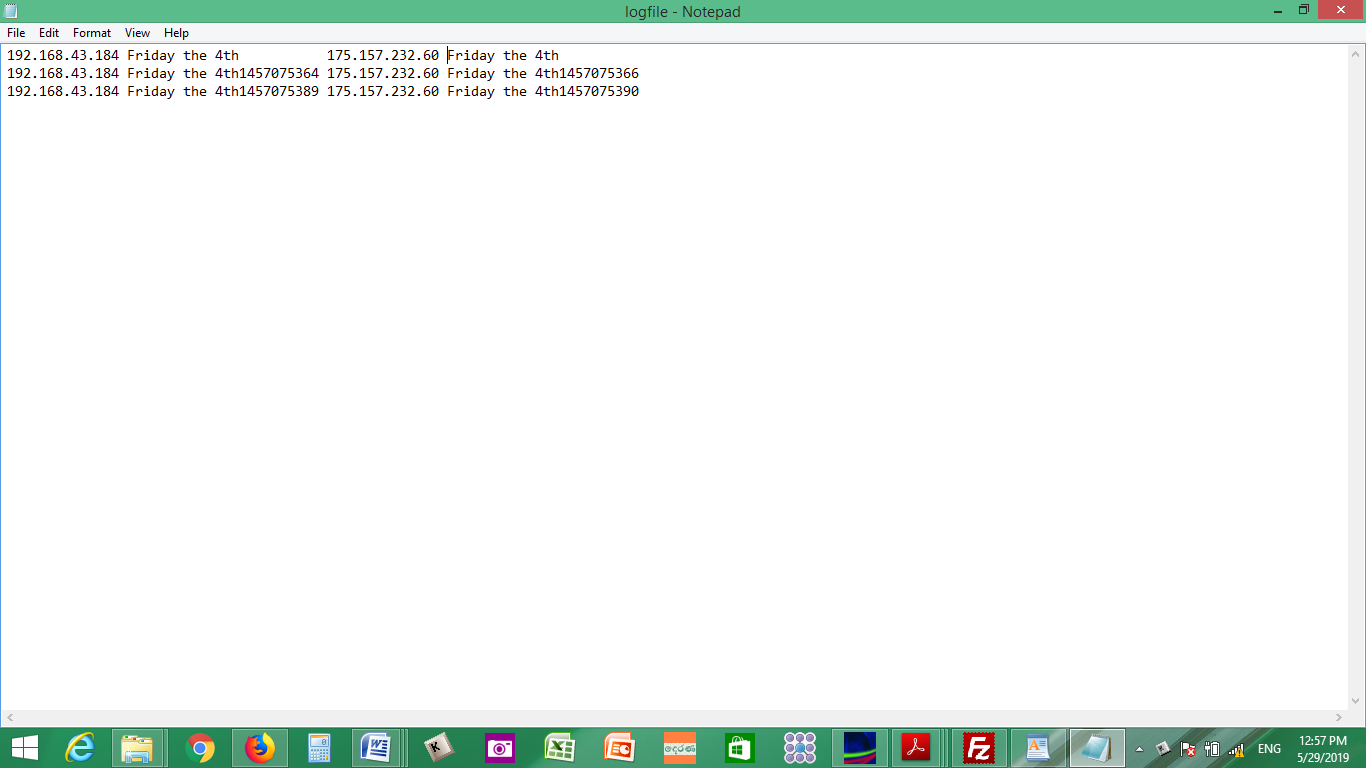


Figure 5.3 Received Meta data from opposite party

5.2.4 ISP's detail which was received the public IP 175.157.232.60 and Private IP 192.168.43.184 of the anonymous user

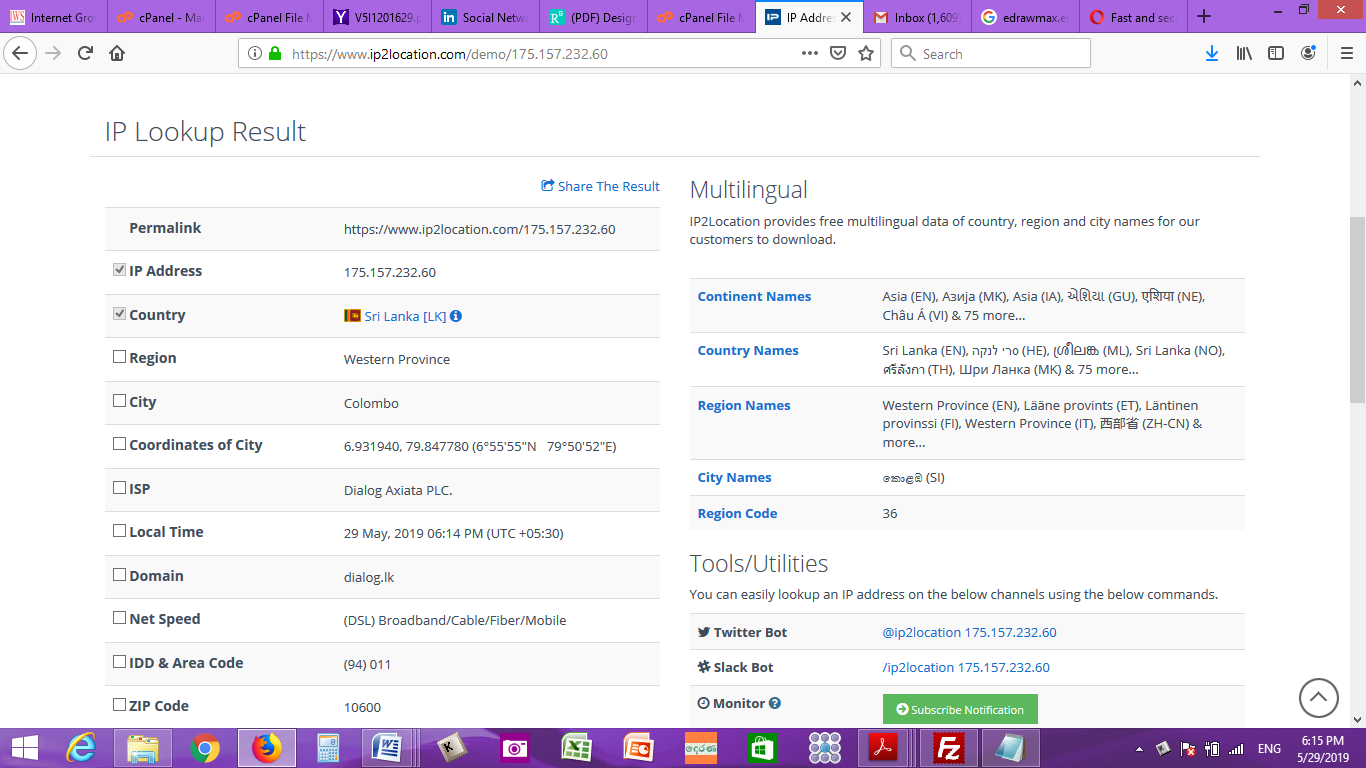
****

Figure 5.4 ISP details of the detected network system

5.2.5 After apprehend the suspect and seizing the equipment and his email account were analyzed and recovered evidence of password change in the anonymous FB user account.

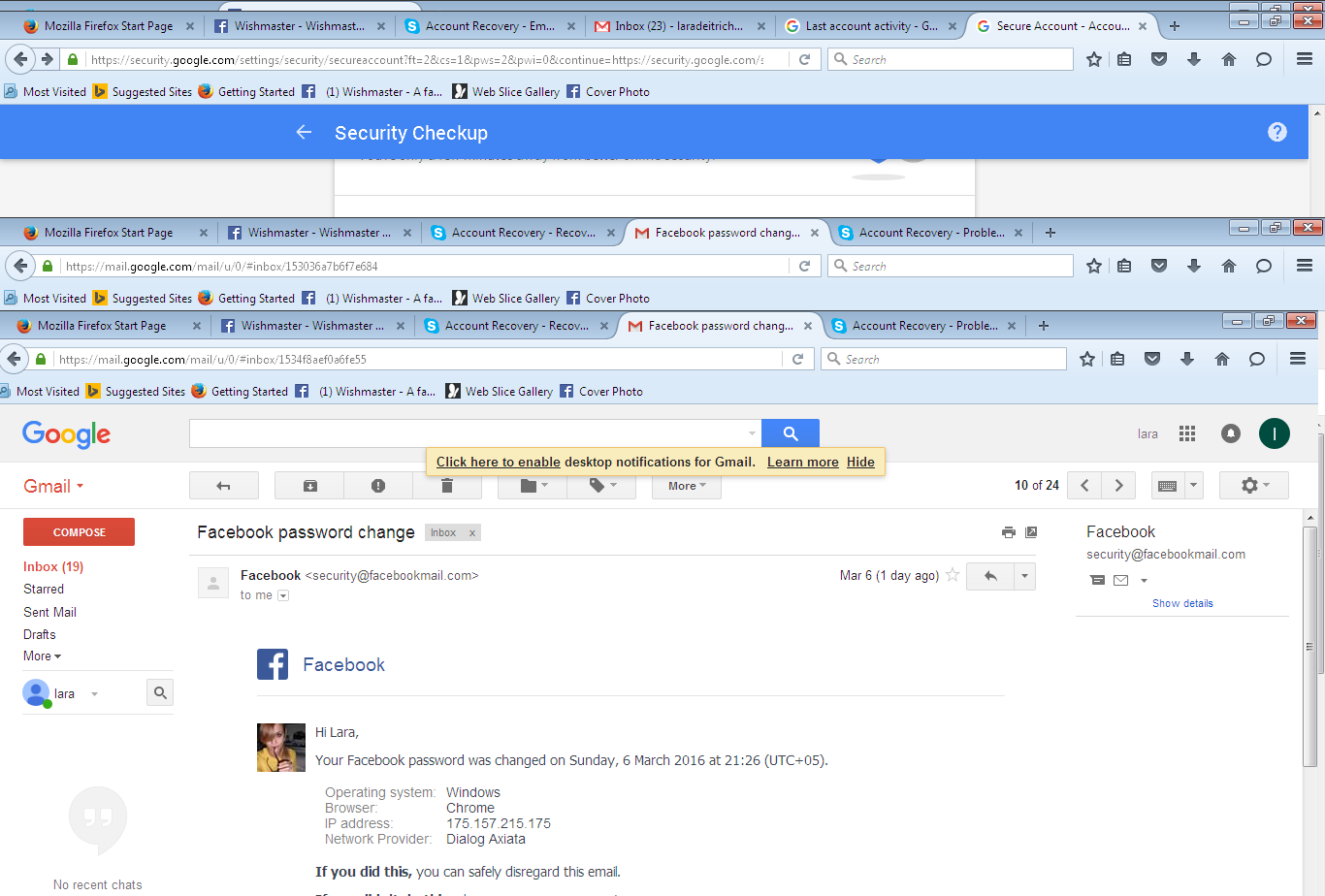


Figure 5.5 Recovered email from the computer of the suspect or anonymous user

Chapter 6

**CONCLUSION**

This chapter discusses the results, feedback, decisions made after the implementation and future

work that is to be carried out towards to enhance the solution and to mitigate the De-anonymizing of anonymous SMN further. De-anonymizing of SMN detection protocol is a way to find a solution to the Anonymous SMN account users, which leads to reduce cyber harassments, deformations and will not share the confidential information with the anonymous account users. As a solution to the Anonymous SMN problem De-anonymizing for SMN detection protocol has given a control towards to mitigate the issues which are facing in SMN.

De-anonymizing of SMN detection protocol design was based on seven (3) major models which are discussed in design phase. They are, Draft Designing Model, Hosting Server Designing Model, and Client Server Designing Model. As defined in the Design Chapter (3).

Evaluation has done in an open source Hosting Server and Client Server with prepared JAVA embedded De-anonymizing tool were uploaded at the hosting server. The De-anonymizing Protocol for SMN is evaluated according to the soundness, completeness, accessibility and the efficiency of the De-anonymizing tool. According to the Evaluation chapter in Chapter 5, it concludes that objectives are achieved accordingly. The level of accessibility to a SMN data is measured by the amount of data that are legitimately expected from a SMN account or a user account. Although successful of the De-anonymizing Protocol for SMN is depending on the detected anonymous account users and identify the real suspect with clear evidence, which was the complaint mention in their given statement to the Law Enforcement Officers (LEO). Hence the system proves the complete detection and further, it was successfully proven with receiving Meta data from anonymous user server to client server as shown in the Evaluation section in Chapter 5

.

1. Future Work

Suggested De-anonymizing of SMN detection protocol has achieved the research objectives and delivered the expected results. But the context of the De-anonymizing of SMN detection Protocol's designed system is very limited. Therefore there are number of future enhancements that can be done to enhance the De-anonymizing tool and protocol.

* + Improve to enhance the De-anonymizing tool to get more Meta data (Mac address, Cookies, passwords and etc) from the opposite party.
  + Improve to access the opposite network system through the De-anonymizing tool by sending some Key loggers or any other compromising tools.
  + Improve and enhance the Protocol using **Text Base analysis** or Profiling anonymous user.

Bibliography

[1]G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In Proceedings of ACM CCS, pages 674–689. ACM, 2014.

[2] G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. G¨urses, F. Piessens, and B. Preneel. Fpdetective: dusting the

web for fingerprinters. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications

security, pages 1129–1140. ACM, 2013.

[3] M. D. Ayenson, D. J. Wambach, A. Soltani, N. Good, and C. J. Hoofnagle. Flash cookies and privacy II:

Now with html5 and etag respawning. 2011.

[4] C. Budak, S. Goel, J. Rao, and G. Zervas. Understanding emerging threats to online advertising. In Proceedings of the ACM Conference on Economics and Computation, 2016.

[5] M. Chew and S. Stamm. Contextual identity: Freedom to be all your selves. In Proceedings of the Workshop on Web, volume 2. Citeseer, 2013.

[6] Privacy Technology Focus Group Report <http://www.it.ojp.gov/documents/privacy_technology_focus_group_full_rep> ort.pdf) (PDF). United States Department of Justice. 2006. p. 52.

[7] "Data anonymization" (http://medical-dictionary.thefreedictionary.com/Anonymized+Data). The Free MedicalDictionary. Retrieved 17 January 2014.

[8] "De-anonymization" (<http://whatis.techtarget.com/definition/de-anonymization-deanonymization> )Whatis.com. Retrieved 17 January 2014.

[9] Bin Zhou; Jian Pei; WoShun Luk (December 2008). "A brief survey on anonymization techniques forprivacy preserving publishing of social network data https://www.cs.sfu.ca/~jpei/publications/SocialNetworkAnonymization\_survey.pdf) (PDF). Newsletter ACM SIGKDD Explorations Newslette.r 10 (2): 12–22.

[10] G. Danezis and P. Mittal. SybilInfer: Detecting Sybil Nodesusing Social Networks. In NDSS, 2009.

[11] V. Dave, S. Guha, and Y. Zhang. Measuring and Fingerprinting Click-Spam in Ad Networks. In SIGCOMM,

2012.

[12] eMarketer. Mobile Growth Pushes Facebook to Become No.2 US Digital Ad Seller. <http://preview.tinyurl.com/mq6vu3u>, December 2013.

[13] Facebook. Can I buy likes for my Facebook Page? <http://www.facebook.com/help/281084665319172>.

[14] J. Filan. Facebook Ads: What Are You Really Paying For? http://www.searchenginejournal.com/facebook-ads-what-are-you-really-paying-for/46194/, July 2012.

[15] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao.Detecting and Characterizing Social Spam Campaigns. In IMC, 2010.

[16] JI, S., LI, W., SRIVATSA, M., HE, J. S., AND BEYAH, R. Structure based data de-anonymization of social networks and mobility traces. In Information Security. Springer, 2014, pp. 237–254.

[17] JUNG, T., LI, X.-Y., AND WAN, M. Collusion-tolerable privacy preserving sum and product calculation without secure channel. TDSC 12, 1 (2015), 45–57.

[18] JUNG, T., LI, X.-Y., WAN, Z., AND WAN, M. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. TIFS 10, 1 (2015), 190–199.

[19] JUNG, T., MAO, X., LI, X.-Y., TANG, S.-J., GONG, W., AND ZHANG, L. Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation. In INFOCOM (2013), IEEE, pp. 2634–2642.

[20] KOHLMAYER, F., PRASSER, F., ECKERT, C., KEMPER, A., AND KUHN, K. A. Flash: efficient, stable and optimal k-anonymity. In IEEE PASSAT (2012), pp. 708–717.

[21] KORULA, N., AND LATTANZI, S. An efficient reconciliation algorithm for social networks. arXiv (2013).

[22] LAO, N., MITCHELL, T., AND COHEN, W. W. Random walk inference and learning in a large scale knowledge base. In EMNLP (2011), Association for Computational Linguistics, pp. 529–539.

[23] LI, X.-Y., ZHANG, C., JUNG, T., QIAN, J., AND CHEN, L. Graph-based privacy-preserving data publication. In INFOCOM (2015), IEEE.

[24] LIU, K., AND TERZI, E. Towards identity anonymization on graphs. In SIGMOD (2008), ACM, pp. 93–106.

[25] MACHANAVAJJHALA, A., KIFER, D., GEHRKE, J., AND VENKITASUBRAMANIAM,

M. l-diversity: Privacy beyond k-anonymity. ACM TKDD

1, 1 (2007), 3.