Developing an Automated Online Notice System for Internet Crimes to Report Law Enforcement

Ibrahim OZDEMIR

A minor thesis submitted in part fulfilment of the degree of M.Sc. in Forensic Computing and Cyber Crime Investigation with the supervision of Dr. Anca Delia Jurcut.

School of Computer Science and Informatics

University College Dublin

09 August 2018

Acknowledgements

I would like to express my special gratitude to **Dr. Anca Delia JURCUT**. She has contributed this dissertation a lot with her deep knowledge. She has always helped me all the way through. I appreciate all the contribution she has done.

I would also like to thank **my parents and my brothers** with all my heart. I've always felt their support and affection with me. I couldn't finish this study without their support.

The other special person to whom I owe a lot is **Captain Onur CERAN**. He has always encouraged and supported me. I do appreciate all the things he has done for this study.

And finally, I would like to extend my appreciation to **my colleagues and the participants** who have attended the experimentation session.

Amor Patriæ Nostra Lex

Abstract

While providing endless benefits to the communities, internet also comes with the downsides. Nowadays, crimes on the internet are a growing problem in the world. The criminals are gradually moving from the physical world to the virtual one. Internet provides an ideal chance to criminals to disguise themselves easily. Law enforcement authorities must keep pace with this change. It is not always that smooth to detect criminals on the internet. Complaints of people play an important role wile combatting the crimes on the internet. An effective internet crimes reporting mechanism is needed. In this dissertation, a new internet crimes reporting system is provided. The main purpose of the study is to show why and how the current methods of reporting system should be changed and to introduce the proposed reporting mechanism. The current methods of reporting cybercrime in various countries are examined and then followed by criticisms. The proposed system is explained in detail after the problems are put forth. Two new software are created for the proposed system: one for desktop browser and for Android smartphones, respectively. Further, the experimentation phase is implemented with a comprehensive group of participants and the results obtained are analysed and compared using the current system and our proposed system. This analysis shows the benefits of our proposed system. The proposed system proves that it is more effective in terms of capturing the information required by the law enforcement authorities. Comparison of the results also shows that the proposed system make it convenient to review and examine the complaints for law enforcement. Availability through mobile platform is another benefit and easiness offered by the proposed system. Furthermore, sub-units of the software and how they work are included and explained.

List of Figures

List of Tables

Table of Contents

1 Introduction

The information and communication technologies have evolved dramatically during the last decades. The daily life of people has significantly been affected by the fast and robust alteration. Individuals are now able to take care of their daily lives even in their homes only with a computer connected to the internet. Banking, shopping, socializing, studying and getting in touch with somebody on the planet are easier than before with the online world. While the developments have pros, the cons shouldn't be underestimated as well. It is worth to bear in mind that this evolution is misused by criminals as well. The conventional ways to commit a crime such as robbing a bank with guns, stealing somebody's purse, buying illegal goods on the street are becoming less common these days. The evolving technologies are also being used by the criminals. People tend to commit crime on the internet by disguising themselves with the help of blessings derived from information technologies. In the meantime, risk factors are trying to be eliminated as much as possible. This situation directly affects the rapidity of the crime to be committed. Nowadays, millions of dollars may be stolen even with clicking a button without leaving any clues to identify the criminal. If the crime on the internet is committed that fast, the investigations must be conducted effectively against the criminals.

It is also important to emphasize the significance of the reporting mechanisms in order to let law enforcement authorities know about the crimes committed on the internet in a timely manner. Different types of law enforcement online notice systems are used in different countries. The way receiving reports from complainants must be effective and rapid as the time after the crime committed works unfavorably of law enforcement. An ineffective reporting mechanism can cause duplication of efforts, which finally cause wasting manpower, time and energy. This can merely be achieved by an effective, fast and functional reporting mechanism.

1.1 Problem Statement

Firstly, as a major problem, instead of filling long notice forms with full of required information such as name, last name, e-mail, phone number etc. people tend to take the screenshot of the problem encountered on the internet and send it to law enforcement's

e-mail address. These notices are just screenshots and mostly lack of necessities like URL of the page. Sometimes, after a crime shown on the internet, the perpetrators tend to delete the content after a period of time. This problem is one of the major problems for law enforcement authorities to deal with as there may be no evidences by the time the notice is received by the law enforcement. This may cause the failure of an investigation before it is started. When the sensitiveness of people against crime is taken into consideration, individuals are understandably reluctant to submit their reports to solely a cybercrime office which finally causes duplication of efforts for law enforcement agencies. For instance, Turkish National Police received approximately 400k reports via e-mail since July 2016. All of 81 Cybercrime Offices in Turkey have different e-mail addresses. Or, they just simply ignore a crime in order not to go through tiring and long process.

Secondly, it can be observed that individuals even mention law enforcement's social media pages and report the problem on social media even though it is sometimes clearly stated by law enforcement that they are not able to accept any kind of notices on social media platforms.

1.2 Research Purpose

Crimes against individuals such as fraud, terrorist propaganda and child sexual abuse on the internet must be strictly fought. Thus, reporting mechanism must be an instrument helping law enforcement officials' heavy workload rather than being a problem at the very early stage of the investigation which in fact starts generally with a complaint. A totally new system consisting of sub-modules is used to solve commonly encountered problems. It is user-friendly and help both sides of the problem. Indeed, it is vital to adapt it for both desktop and mobile devices. It captures the required information automatically for the law enforcement authorities. This information includes URL, screenshots of the page, date and time information and the most suitable type of crime. This can be widened by the requirements of law enforcement authorities.

It is believed that the research helps not only people to report a crime on the internet more easily and effectively but also helps law enforcement to receive a report with no missing required parts in order to start an investigation. This also encourage people not to ignore a crime they see on the internet.

1.3 Research Questions

The following questions are used to identify the best way of reporting an online crime by comparing it with the current ones:

- How should online reporting systems be to notify law enforcement authorities?

Sub-questions

- How do online reporting systems work in other countries?
- Which sub-units should be used for online reporting system?

1.4 Original Contribution of This Work

This study offers an original contribution to the current online crime notifications systems. By the time this study is being conducted, no law enforcement authority is using the proposed system components as a part of ongoing reporting mechanisms. In this context, the proposed system brings an innovation to the present crime notification systems.

1.5 Methodology

A number of people are asked to report an internet crime by using the current reporting system (via e-mail). Then, they are asked to report the crimes through the system to be developed. The results (time, the info received etc.) are firstly analyzed and then compared to measure the effectiveness and success rate.

2 Literature Survey

This chapter provides a discussion of the reasons for people to report a crime and of the reasons why they do not report a crime. It continues with different definitions of cybercrime according to public and private institutions. Then it is followed by how cybercrime is divided into two categories and what they are.

This chapter also covers how cybercrime is reported in various countries. These countries are the USA, the UK and Turkey, respectively. The current systems of cybercrime reporting mechanisms are examined in detail. The law enforcement authorities and institutions responsible for cybercrime reports in these countries are studied separately.

The chapter also explains the current reporting mechanisms step by step. The necessities to complete a form and limitations in the forms are included, as well.

2.1 Why to Report a Crime?

Reporting a crime is usually perceived as a wish to report a crime to the relevant authorities [1] and these reports are considered as the main information source of police forces [2]. According to State of Victoria, Australia and Ministry of Justice, New Zealand it is significant to report a crime for the following reasons:

- Individual safety should be protected,
- To let the law enforcement agencies act proactively and prevent a possible crime committed by the suspect,
- Insurance for personal damaged properties,
- To let police forces to identify crime trends in a specific area [3], [4].

In addition, Pennsylvania Office of Victim Services advise people to report a crime to arrest the suspect and to hinder a crime to happen against another individual [5]. It is also emphasized by Edmonton Police Service that reporting a crime is very important because if a crime is not reported, the number of crimes will increase accordingly [6]. Moreover, if the law enforcement forces are informed about the committed crimes and

they fight thoroughly, the crime rate has nothing but to decrease [7]. Finally, if the law enforcement authorities are let to know about the crime, it is unlikely for an individual to be a victim again[8].

2.2 Why Do Individuals Hesitate to Report a Crime?

The main reason why police is not informed about a crime is that the crime is considered as trivial or private. In addition to that, the relationship between people also has effect on reporting process. Several suggested hypotheses tried to find the effect of the relationship and gender on reporting a crime to the police:

- To prevent prospective crime,
- The fear of being attacked for reporting the crime,
- The crime is not considered serious enough to report,
- Fear of being known by the people around the victim,
- To protect strong relationship between the victim and suspect,
- Police's attempts to fix the issue between the victim and suspect, especially for domestic violence cases [9].

One of the reasons why most people hesitate reporting a crime is police's behaviour against the individuals. The crime may not be seen important to investigate. Furthermore, the way police behaves people is one of the other reasons for people not to report a crime again in the future [10]. It is also worth to bear in mind that Wesley G. Skogan suggested that the most important factor for reporting or not reporting a crime is the crime seriousness [11]. In the other hand, it is observed that the main factor can vary in some communities. In Greece, migrants are more likely to be reported to the police rather than the Greek criminals. In this situation, the ethnic origin is considered as the main subject of the reporting process [12].

When it comes to the reported/unreported crime rates, National Crime Victimization Survey states that while the rate of reported violent crime percent is %51, the rate of property crime remains only at %39.3 in the United States of America in 2010 [13]. If the

crimes committed in the USA from 2006 to 2010 are examined, it is very clear the major concern for not reporting a crime is that people handle the matter by themselves or another way (%34). It is respectively followed by; other reasons or not the most important reason (%18), not important enough to victim to report (%18), police would not or could not help (%16) and fear of reprisal or getting offender in trouble (%13) [14].

2.3 Internet Crimes (Cybercrime)

European Commission defines cybercrime as “criminal acts that are committed online by using electronic communications networks and information systems” [15]. One of the biggest anti-virus companies, Norton Security, defines cybercrime as “any crime committed with a computer, or targets a computer or a network, is known as cybercrime” [16].

Interpol has divided cybercrime into 2 categories: pure cybercrime and cyber-enabled crime. If the main aim for a criminal is to gain unauthorized access to a device or deny access to a legitimate user, then this falls under the first category, pure-cybercrime. However, if the conventional crimes are committed by means of computers, they become cyber-enabled crimes [17]. Similarly, Home Office of United Kingdom defines the cyber-dependent (pure cybercrime) crimes as crimes which can be committed only by using computers, computer networks or other form of information communications technology. And the cyber enabled crime is defined as the traditional crime that can be committed through computers, computer networks and other forms of ICT [18].

2.4 How Cybercrime is reported in Various Countries

2.4.1 United States of America

The primary federal law enforcement agencies that investigate domestic crime on the internet include: the Federal Bureau of Investigation (FBI), the United States Secret Service, The United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF) [19].

2.4.1.1 Federal Bureau of Investigation (FBI)

FBI is the biggest law enforcement organization within the United States of America. In order to report the internet-facilitated fraud crimes, Internet Fraud Complaint Center was established in 2000. However, its capacity was expanded in 2003 and renamed as Internet Crime Complain Center (IC3) and become an important reporting center for internet fraud incidents overlapping with different kinds of cybercrimes [20].

As shown on Appendix 1, when clicked on “File a Complaint”, 3 categories of reporting mechanism is shown on the webpage.

If the complainant proceeds with the submitting an internet crime complaint, a new webpage is opened and a short briefing about the complaint is shown. In addition, the complainant is supposed to accept several pre-conditions. Please see Appendix 2.

It is observed that in order to report a cybercrime incident (apparently it is mainly dedicated to cybercrime involving fraud), one has to submit his/her name, address, city, country, zip code/route, phone number and e-mail address as shown in Figure 1.

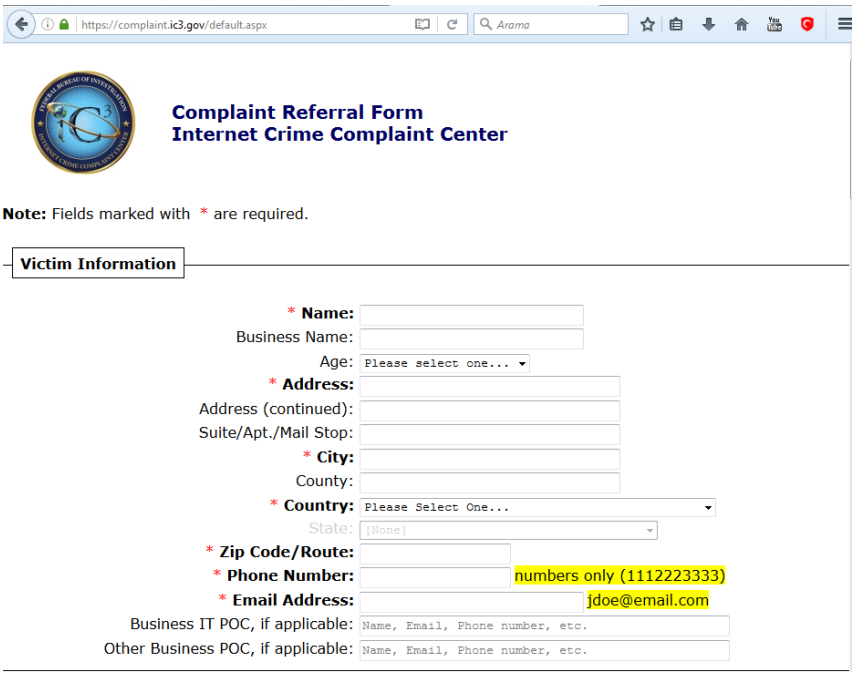


Figure 1 IC3 Reporting Page

Figure 2 shows the list of required information from the victim to include in the complaint.

Figure 2 IC3's List of Required Information from Complainants

Indeed, this means that submitting a report without the mandatory fields is impossible. People must provide their personal details.

When it comes to reporting Child Sexual Abuse on the Internet, IC3 directs the complainants to National Center for Missing and Exploited Children's (NCMEC) webpage.

Report Threats and Crime through Online Tips and Public Leads form is dedicated to submit any threat and crime regardless of online or not. When analysed, it is observed that one is not required to provide any personal information. It is totally up to the complainant to provide any details about him/her. It is clear that if somebody is intended to report any incident on the form, filling the "information" field which is restricted to 3000 character is the key point. Please see Figure 3.

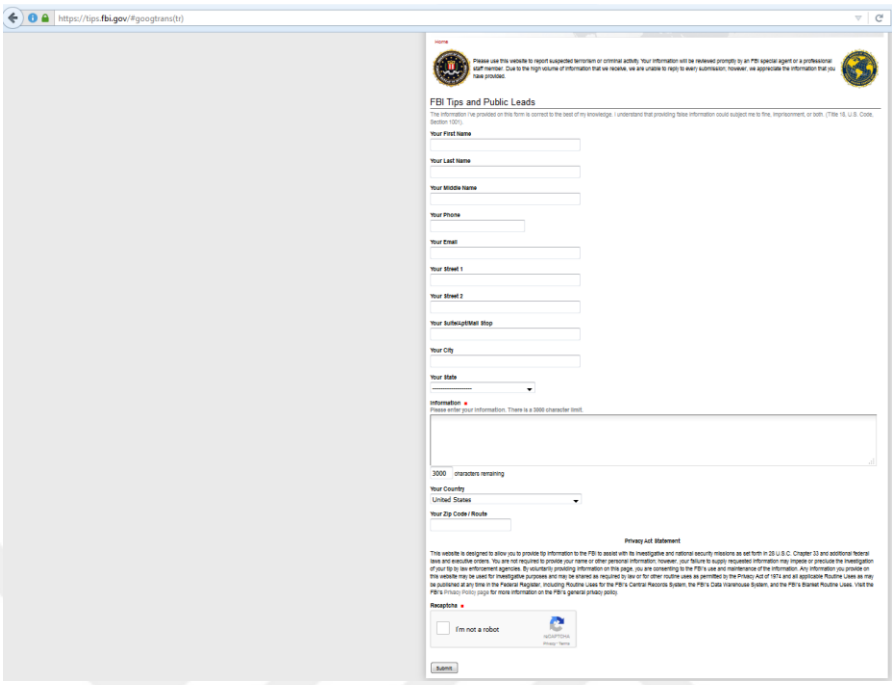


Figure 3 Report Threats and Crime through Online Tips and Public Leads Form

2.4.1.2 US Secret Service

US Secret Service is a federal law enforcement agency which operates under Department of Homeland Security. One of its authorities is to protect USA's financial infrastructure from cyber and financial criminals [21].

An individual can report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information to United States Secret Service [22].

It is observed that Secret Service has no online reporting mechanism for cybercrimes and other types of crime. Instead, they encourage people to go report a crime physically.

2.4.1.3 The United States Immigration and Customs Enforcement (ICE)

U.S. Immigration and Customs Enforcement (ICE) enforces federal laws governing border control, customs, trade and immigration to promote homeland security and public safety. ICE was created in 2003 through a merger of the investigative and interior enforcement elements of the former U.S. Customs Service and the Immigration and Naturalization Service. One of the three operational directorates, Homeland Security

Investigations, has online “HIS Tip Form”. When examined, it is observed that the form is not dedicated only to cybercrime but also other 400 violations that ICE deals with [23].

One does not has to provide his/her personal information such as first name, last name, e-mail address and phone number while filling the form. On the other hand, the complainant is supposed to provide one of the boxes which fits with the complaint in the fields of the location, crime type, state, previously reported or not. It is interesting that somebody is not able to report more than one crime into solely into a form.

2.4.1.4 The United States Postal Inspection Service

The United States Postal Inspection Service (USPIS) is the law enforcement arm of the United States Postal Service [24].

Even though this is listed as one of the investigative branches for internet crimes, one can submit a report through online reporting for Mail Fraud, Mail Theft, Identity Theft and Unsolicited Sexually Oriented Advertising. However, it is observed that all of the reporting types are dedicated to complain about something that has relation with physical mail delivery.

2.4.1.5 The Bureau of Alcohol, Tobacco and Firearms

ATF is a law enforcement agency in the United States’ Department of Justice that protects our communities from violent criminals, criminal organizations, the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism, and the illegal diversion of alcohol and tobacco products [25].

Generally reports are covering any violation about alcohol, tobacco and firearms. People can report these issues over the phone or through e-mail and anonymously via “ReportIt” application on mobile devices.

2.4.2 United Kingdom

2.4.2.1 National Fraud & Cyber Crime Reporting Centre

In United Kingdom, cybercrime reporting is gathered under a single roof. Either National Crime Agency’s webpage, UK National Cyber Security Centre’s webpage or Europol’s webpage which allows EU citizens to report a cybercrime to proper places direct the

complainants to the same reporting webpage which is https://www.actionfraud.police.uk/. This reporting tool is dedicated only to Fraud, Cybercrime and Phising Attempts.

ActionFraud is the UK's national fraud and cybercrime reporting centre. It is defined as the easiest way to report fraud or cybercrime [26].

When directed to the reporting page, one has 2 options which are Fraud and Cybercrime and a Phising Attempt, as shown on Appendix 3. The main difference between them is if an individual is a victim of phising attempt and lost money or exposed his/her personal details, he/she has to fill the Fraud and Cybercrime report. Please refer to Appendix 4.

During the reporting process a fraud or cybercrime incident, firstly, one has to choose the best of the options related to the incident which helps law enforcement to know about the type. The following steps are information about the victim, about the suspect, money, fraud details, fraud impact and support, respectively. After the type of the incident is provided, it is mandatory to provide personal details of the victim like name, last name and address.

2.4.2.2 Metropolitan Police

Metropolitan Police also has an online reporting system for different kinds of crime including online crimes. Before filling a form, one has to choose the best one amongst the given options. However, the crime must have happened within the Metropolitan Police's jurisdiction. Otherwise one is not allowed to complete a report afterwards.

2.4.3 Turkey

2.4.3.1 Turkish National Police (TNP)

Turkish National Police (TNP) is the biggest law enforcement authority in Turkey. It is structured as a General Directorship under Ministry of Interior. TNP consists of Central Organization, Provincial Organization and Abroad Organization. Central Organization, which consists of 37 Departments, is responsible for coordination, training and logistics of Provincial Organization which is established each 81 cities as City Police Departments in Turkey.

TNP has no police reporting system specifically for cybercrime. There is a central crime reporting hotline which can be reached by sending a letter, via phone or sending an

online form. Crime can also be reported to a local police station or, in some cases, directly to specialized units.

The online form is quite simple and out of date. All of the crime types whether online or physical are supposed to be submitted in the same form format. Firstly, one has to choose the place first which includes only the Provincial Organization Units. This means that individuals are not allowed to report a crime directly to Central Organization Units such as Cybercrime Department. Secondly, it is not mandatory to provide personal details such as name, last name, phone number and e-mail address. But, if the complainant would like to receive feedback, e-mail address or phone number must be provided, as well. However, the title, place and explanation fields are deemed necessary to provide. Please refer to figure 4.

Furthermore, each Department within TNP has institutional e-mail addresses to be used for any purposes including reporting a crime. For instance, Cybercrime Department has 3 e-mail addresses as mentioned. The e-mail addresses have been shared on publicly available platforms like news, newspapers, and social media platforms in order to raise awareness amongst people to report crimes especially after terrorist use of internet has increased. The amount of e-mail notices is increasing day by day.

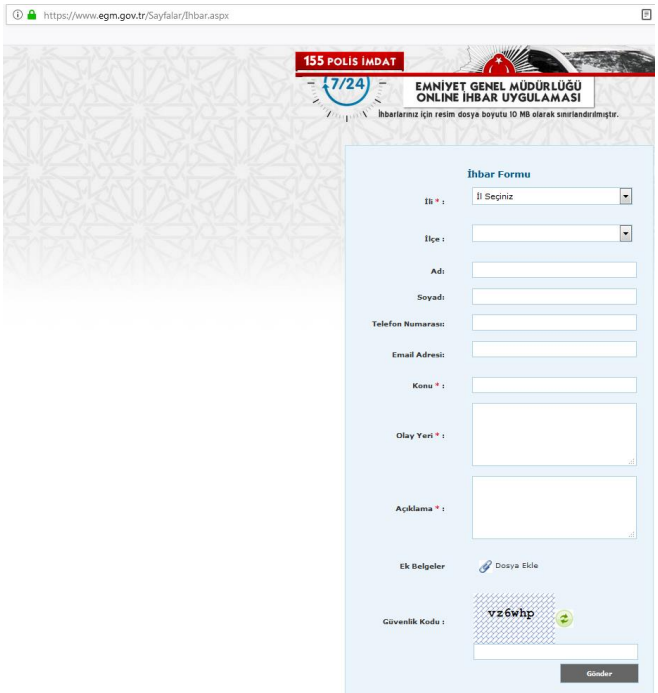


Figure 4 TNP's Crime Reporting Form

The notice system automatically sends the report to the stated City Police Department's central notice unit. Then, it is directed to the most relevant unit in order to be investigated.

2.4.3.2 Gendarmerie General Command

Gendarmerie General Command is one of 2 law enforcement authorities in Turkey. It is responsible of safety in rural areas such as villages, mountains etc.

Gendarmerie has also an online notice system. However, it is not dedicated only a type of a specific crime. Any complaints about a crime whether it is theft, murder or cybercrime must be submitted through this form. When examined, one has to provide the place and a brief description of the crime. However, providing personal details like name, last name, ID number etc. is not compulsory for submitting a crime.

3 Problem Statement

An individual or a group of people must have violated a law in order for police forces to start a criminal prosecution. Law Enforcement Authorities begin an investigation upon receiving a complaint or by themselves in case of detecting a crime or having suspicion of crime. However, the criminal prosecution is not a fast process. It depends on the criminal justice system of each individual country.

If the members of a community do not report a crime which they come across, police may have not any chance to know about it. The reasons why people do not report a crime are stated in Section 2. This makes the reports, which are submitted by the complainants, one of the main sources of law enforcement to begin an investigation. Accessing to the correct reporting mechanisms is significant because people must be aware of what to do in case of a crime.

An individual can report a crime through FBI's IC3 reporting mechanism for internet crime, terrorism and threat and child exploitation or child abuse. Anybody can reach the website easily by googling "reporting a cybercrime in USA". The webpage is simple. In that regard, there is not any complicated field that may cause misunderstanding. The system is advantageously detailed for fraud report submissions. People are allowed to provide as much information as they can. This helps FBI officials to deepen their knowledge about each individual crime. However, no other types of cybercrime are allowed to be submitted through this form. With that regard, the webpage is not comprehensive enough to cover other types of cybercrime such as malware, hacking, phishing, DDoS, identity theft etc. Furthermore, people are obliged to provide their personal details like name, address, phone number etc. which may cause hesitation for them to submit a report. On the other hand, FBI Tips and Public Leads form does not oblige people to provide any kind of personal details which is in benefit of complainants. It is simpler than IC3 form. It is accessible through IC3's main page. The only required field is information section on which people are expected to provide the compliant details. This may cause providing missing information by the complainants as they may not remember a detail by the time they are filling the form. The other disadvantage is this section is restricted to maximum 3000 characters which may be insufficient for some terrorism complaints.

US Secret Service is listed as one of the institutions dealing with cybercrimes. However, it has no online reporting mechanism. Instead, individuals are encouraged to submit a report physically. Thus, this may make the process difficult, not easily accessible. On the other hand, receiving the complaints physically lets Secret Service to acquire all of the details of a crime thoroughly. This is evaluated as the biggest advantage. However, it is not possible to stay anonymous.

In the UK, online cybercrime reports are assembled under one roof, National Fraud & Cyber Crime Reporting Centre. However, the online tool is mostly dedicated only to fraud cases. In this context, lack of other types of cybercrime is a big disadvantage of the system. For fraud cases, one has to go through a form which lets somebody choose one of the options that suit best. The options are very detailed. The form has no missing parts in terms of covering fraud complaints utterly. The system obtains all necessities of a fraud case.

Turkish National Police's online crime reporting tool is easily accessible through TNP's webpage. One does not have to provide any kind of personal details. The option of staying anonymous is an advantage of the system. Attachments are available which can help law enforcement to received proper information. It is not dedicated merely to a specific crime. Instead, all crime complaints including physical crimes such as theft, robbery or cybercrimes such as malware, online fraud etc. can be submitted through the form. For cybercrime, TNP Cybercrime Department has various e-mail addresses which are being used for cybercrime complaints. It has been disseminated through news, newspapers and internet. Especially since July 2016, the number of e-mail complaints has increased to 400k. They are handled by cybercrime investigators, respectively.

In the USA, the UK and Turkey, individuals are advised to go through a series of procedures to place a report for a crime. None of them are meeting the needs of the proposed ideal cybercrime reporting mechanism. They are mostly limited with online fraud which is one of the main challenges in cyber world. However, importance of other types of cybercrime should also be brought to the community's attention such as online harassment, cyber bullying, and terrorism on the internet. Online child exploitation reports can be submitted to NCMEC in the USA, and to CEOP in the UK. Turkey has no specific notifying system for online child exploitation. General procedures must be followed.

As a result, if the above-mentioned assessment about several countries and cybercrime reporting mechanisms are taken into consideration, an ideal reporting mechanism should at least have the following criteria:

- The system should be easily accessible and simple.
- Police should acquire all necessary details of a crime, after complaints are submitted.
- Reporting should not be a long process.
- The mechanism should cover as many crimes as possible in various sub-mechanisms to some extent.
- Complainants should have right to stay anonymous.

In Turkey, general trend to report a crime encountered on the internet is taking a photo or screenshot of the content and sending it via e-mail complaint system instead of going to the prosecutor office or nearest police station and follow slow procedures for a crime. This is one of the explanations of growing number of e-mail complaints since July 2016. It can be understood that people choose the easiest way for reporting a crime. However, the current systems are making a reporting process harder for people. Furthermore, if the more reporting mechanisms become easier in terms of speed, the more people concern about the crimes and report it. And as emphasized in Section 2, if the police deal with the crimes thoroughly, crime rates have to decrease. The main problems with e-mail complaints are people are unaware of what to include in an e-mail complaint. In other words, some people just think that only the content is important for police and do not include any identifiers of the webpage or social media profile. This makes investigation process very challenging. Police then get in touch with the complainant and request the precise information. Indeed, this situation cause waste of time if police luckily have any chance to reach the complainant as in some cases complainants use throw away e-mail addresses to stay anonymous. If not, police is unable to launch an investigation. This may cause serious crimes not to be investigated, especially if it is an emergency.

4 Adopted Approach

This chapter provides comprehensive information about how an ideal online reporting system for cybercrimes should be and what components it should include. The proposed system offers a very rapid and effective cybercrime notification process to the police. Instead of filling long forms or going through series of options, complainants are supposed to do all of the requirements with no more than several clicks only.

The proposed system consists of 3 main components. The main component is the user interface which is the process running on the user's computer and mobile device. The second one is the central processor which stores the pushed information from user interface and forms purposeful information for the investigators. And the final one is the investigator interface which displays the data received from central processor in a form that makes the investigators reach all required information on a single interface. The general illustration of the components is shown in Figure 5.

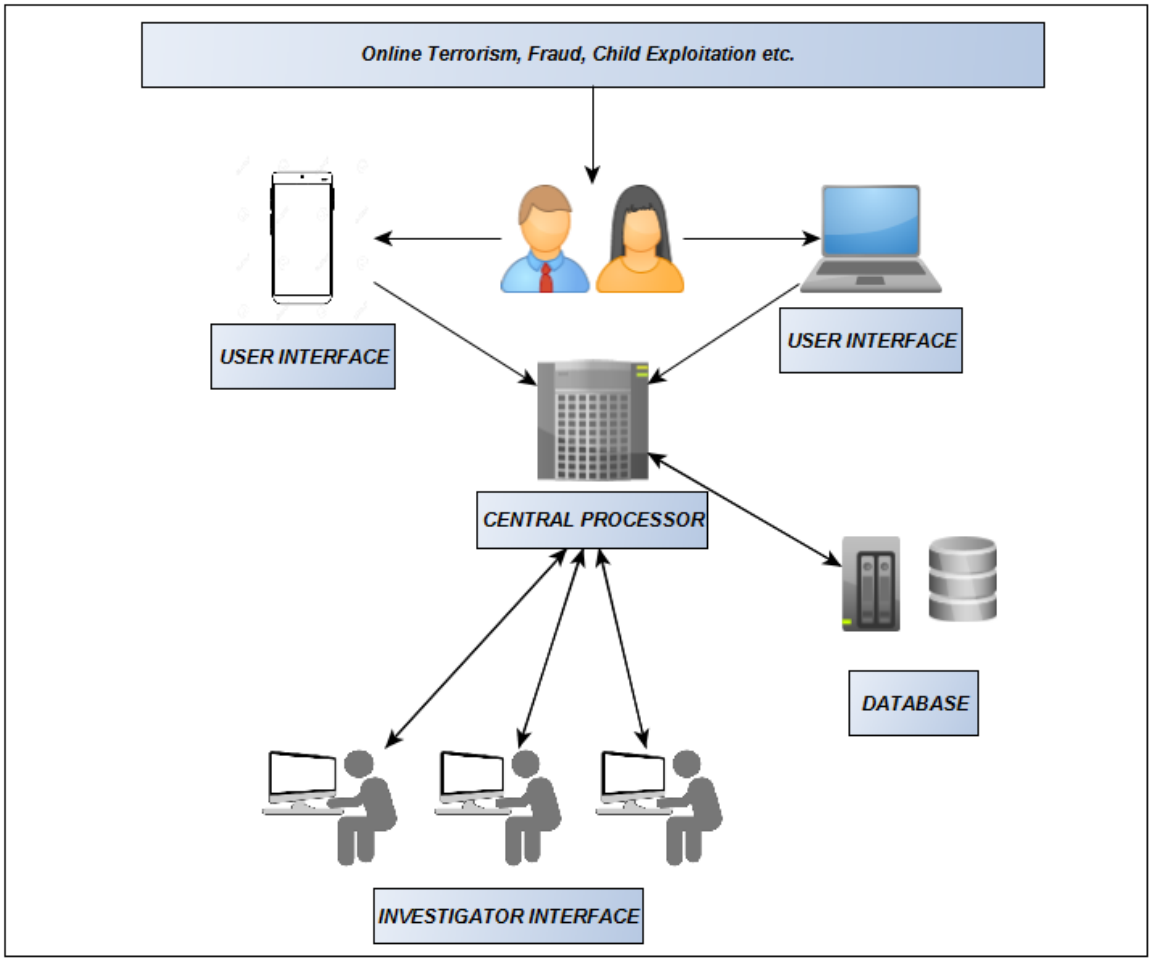


Figure 5 Components of Proposed System

4.1 Components of Adopted Approach

The main components consist of sub-units. These are shown in Figure 6 and then explained in the next sections.

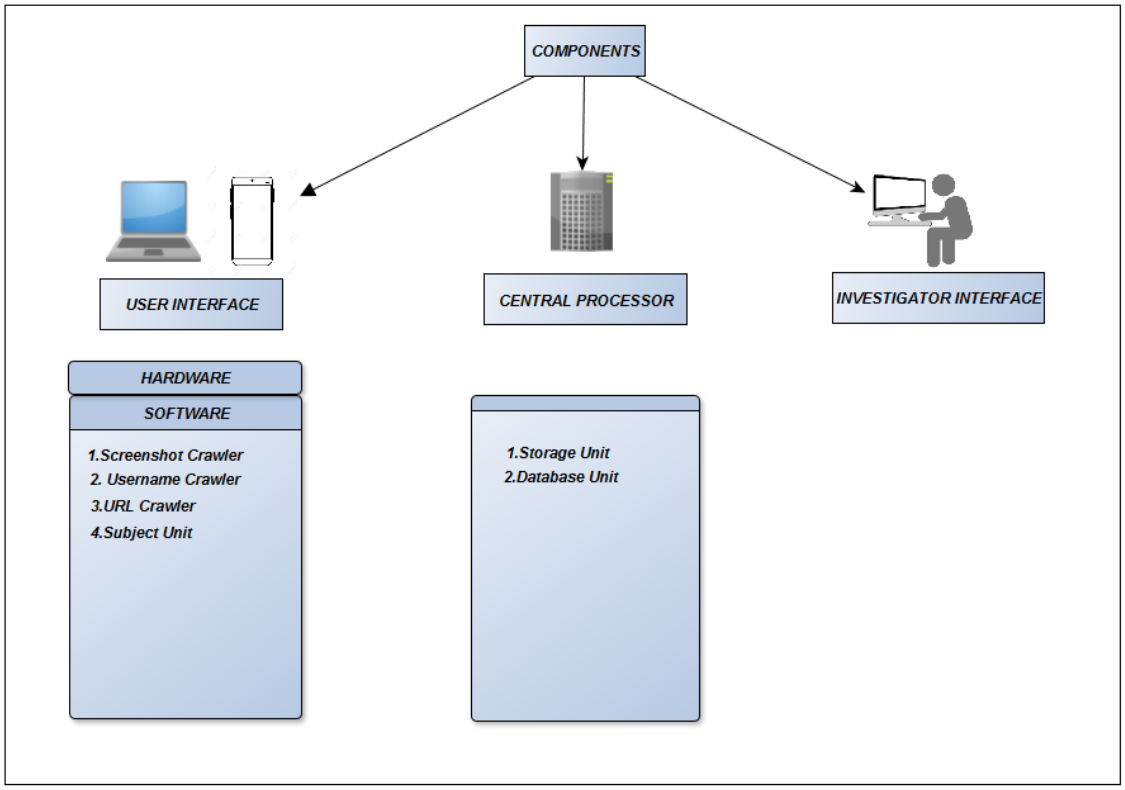


Figure 6 Sub-Units of Components

4.1.1 User Interface

Online notifying system is based on computers and Android based smartphones in order to notify police for a crime on the internet. Computers are settled in the core of daily life nowadays. It is quite normal for a person to check e-mails, read newspapers, watch movies, check social media etc. regularly in daily life. While doing so, it is not astounding to come across with a crime especially on social media or web blogs. User interface's main interest is pulling the raw data from a web source. The system is developed for PCs and Android based smartphones. Both PC and Android based smartphone must have an internet connection to push information to central processor. And also, Google Chrome must be installed in PCs. User Interface consists of 2 sub-units.

4.1.1.1 Hardware

When an individual surfs on the internet, he/she may come across a crime anytime. The adopted approach requires an Android smartphone which has at least Android 5.0 version. This necessity arises from the requirements to upload the Mobile Application to the Google Play Market. Moreover, one has to install Google Chrome Browser to use the Add-on which is explained in next parts.

4.1.1.2 Software

A browser Add-on and Mobile Application manage the major missions of the user interface. The developed system uses Google Chrome extension and Android Mobile Application to notify police for a crime on the internet. The reason why the system is developed for Google Chrome is Google Chrome is by far the most used desktop web browser in the world from June 2017 to June 2018[27]. In addition, Android is by far the most used mobile operating system in the world from June 2017 to June 2018[28].

4.1.1.2.1 Screenshot Crawler

This unit allows Google Chrome Extension and Android Mobile Application take a screenshot of the webpage which allegedly contains a criminal element. If the webpage or social media account is private or police officers are not legally allowed to contact with the suspect with a fake profile or username, this unit lets police officers to have the screenshot of the post as evidence.

4.1.1.2.2 Username Crawler

Usernames, especially on social media platforms, on a specific date are unique identifiers as only one user is assigned with a specific username. The extension and mobile application are designed to capture the username of the suspect if it is assigned by the social media company. This is very useful in terms of acquiring one of the suspect’s unique identifiers.

4.1.1.2.3 URL Crawler

URL of the webpage in question has vital importance for investigations. In case of a demand to verify the content, police should have access to the page by using the URL. Thus, URL Crawler captures the URL of a webpage.

4.1.1.2.4 Subject Unit

The complainant is expected to choose the most suitable crime type. It helps police to classify the crimes and gather statistics. This also helps to send the notification to the proper unit(s) automatically. An “Other” section is provided in case the complainants have no idea about what the crime is.

4.1.2 Central Processor

After the raw data is acquired by the user interface with Google Chrome extension and mobile app, it should be go through a server which has high processing capability. The server must have the central processor in order to produce a meaningful information source for the police. The Central processor’s sub-units are explained next.

4.1.2.1 Storage Unit

Storage unit is responsible for storing the data acquired by user interface unit. This information must be stored to produce information for investigator interface. RAID (Redundant Array of Independent Disks) is used for performance improvement. And also, backup disks are used for an unexpected failure.

4.1.2.2 Database Unit

Database Unit can be thought as the list holder of the relevant information within the server. It distinguishes all the information and put together the relevant information to produce information for investigator interface. MySQL database management system is used in this unit. MySQL in the server can only be accessed by system admin. It is not shared with the other users.

4.1.3 Investigator Interface

Investigator Interface is the component which visualizes all the information acquired by user interface and stored and interpreted by central processor. The interface is divided into sub-sections for each complaint, respectively. It is designed to illustrate everything that an investigator may need for the investigation. This is also related to the capacity of the Add-on and Mobile App and their ability to capture as much information as possible.

Investigator Interface has a big importance as the investigators should know where to find required information to check, verify or start an investigation.

4.2 Web Browser Add-on

Web browsers play an important role for web surfing. Web browsers retrieve content and display from remote web servers using a stateless and anonymous protocol called HyperText Transfer Protocol (HTTP)[29]. However, web browsers may not fully be able to display the content of a web page. They may need additional functions to work properly. Web browser add-ons do this. A web browser add-on is a software that provides an extra functionality to the web browsers and make them act properly. For instance, to view a different kind of document (ex. Excel sheet) in a web browser, an appropriate web browser add-on must be installed.

4.2.1 “IHBAR 1.0” Add-On

IHBAR 1.0 plugin is a web browser add-on which is created for Google Chrome Browser. It is written with HTML, CSS and JavaScript. This plugin is able to offer people an effective internet crime reporting capability.

As shown in Figure 7, IHBAR 1.0 plugin consists of 5 sub-modules which are Title, Crime Type, I Know the Suspect, E-mail and Phone.

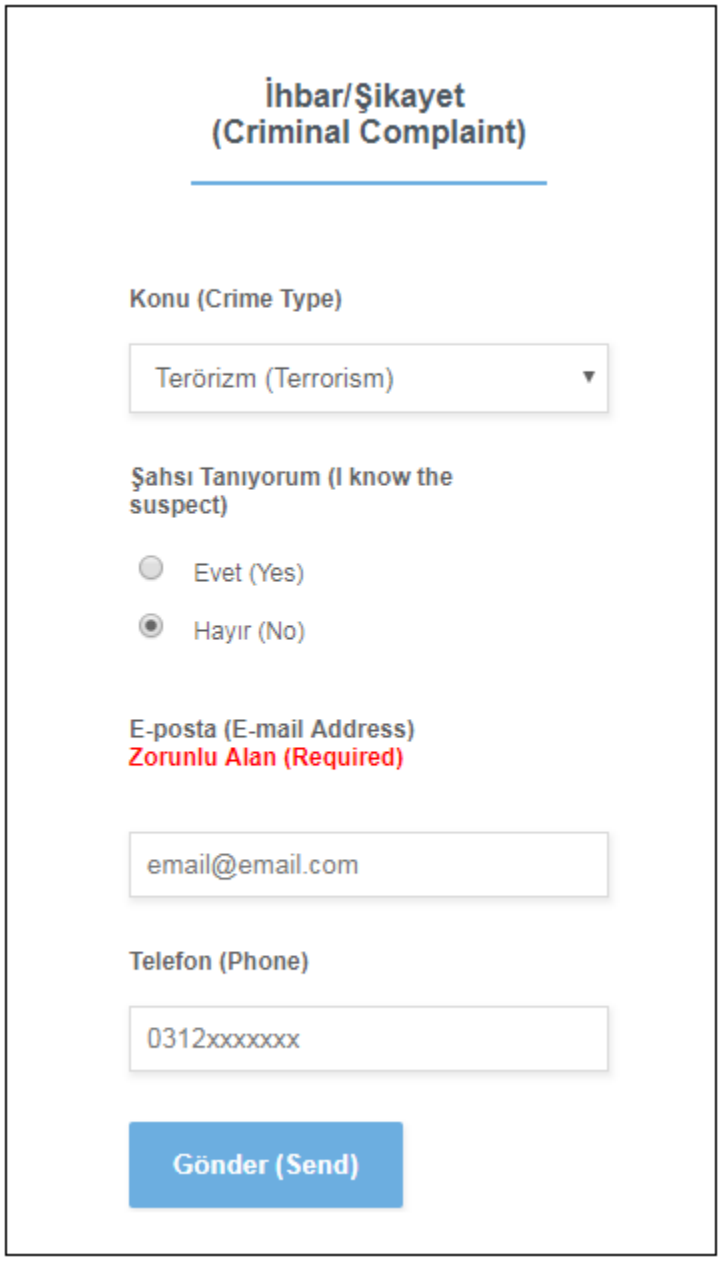


Figure 7 Main Screen of IHBAR 1.0

When the plugin is designed, the current forms are taken into consideration so that it is designed to acquire as less as information possible about the complainant. The number of fields can be reduced or increased depending on the law enforcement agency's requirements and present laws. The fields in Figure 7 are put for experimentation

purposes only. E-mail field is compulsory to have at least one unique identifier for the experimentation session participants.

As shown in Figure 8, the Crime Type field consists of 6 sub-fields which are Terrorism, Online Child Abuse/Exploitation, Credit Card/ Debit Card Fraud, Illegal Gambling, Dissemination of Classified Information/Document.

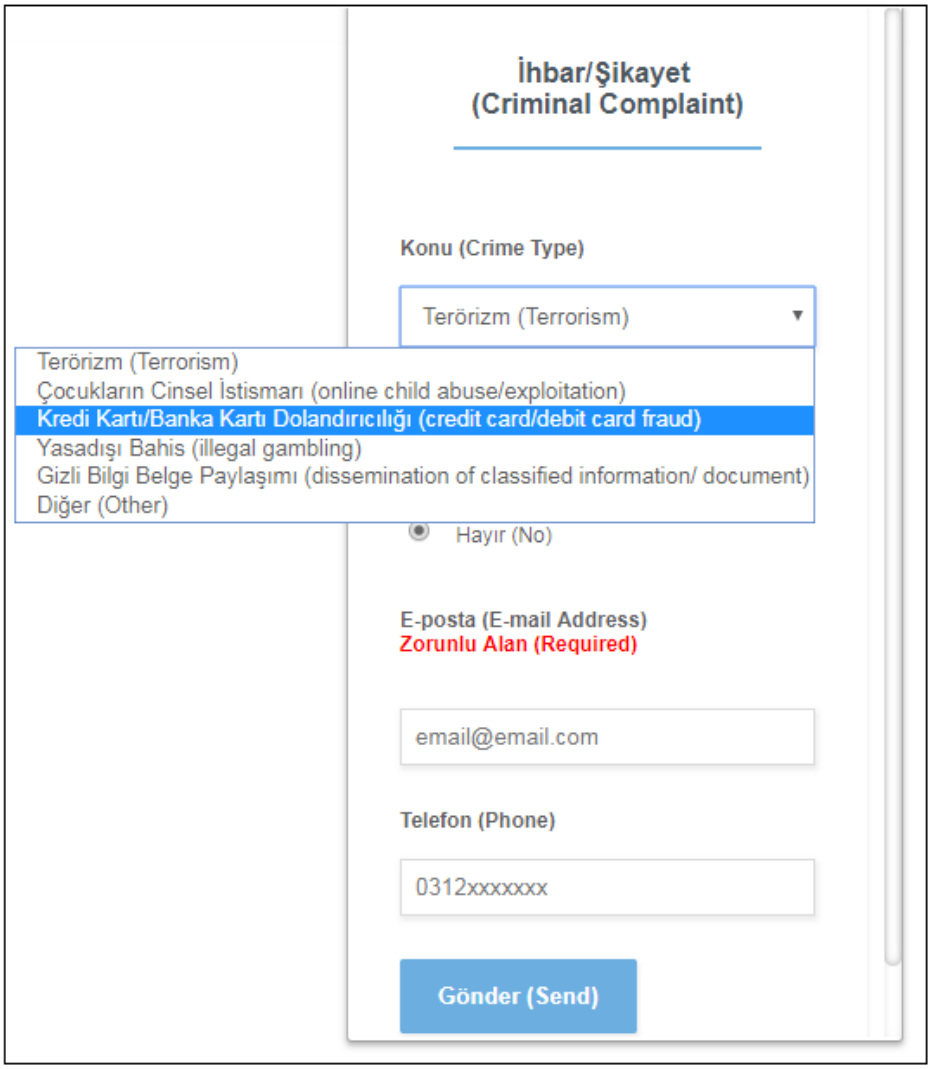


Figure 8 Crime Types Placed in IHBAR 1.0

During the complaint, the web page, which is suspected to pose a criminal threat must be the page, must be displayed on the home screen. Otherwise, the plugin takes the screenshot of an irrelevant page. When the “Send” button is clicked, the information

retrieved from the web page and complainant interacts with Storage and Database Units and then appears in the investigator interface with an ID number assigned by the database in a format as shown on Figure 9.

Figure 9 Investigator Interface of IHBAR 1.0

The elements gathered by the plugin are as follows (from leftmost to right):

ID : This is the unique queue number assigned by the system to list the complaints in a correct order.

Notification Date : This is the date and time information of the complaint.

URL : This is the URL of the web page which contains criminal element. The plugin automatically captures this information.

Crime Type : This is the crime type of the content. This is very useful if the law enforcement agency decides an automatic direction of the complaints to the most relevant units and/or departments.

Platform : This is the platform that criminal act or suspicious behavior takes place. The plugin automatically detects it for social media websites. This may be designed for more platforms including blogs, online newspapers etc.

Username : Username plays a vital role when it comes to websites that distinguish users with unique numbers or names like Facebook and Twitter. Even though the users can change it, the information belongs to a person between specific dates.

I know the suspect : This is the section to let law enforcement that the complainant knows the suspect. This information may be useful for further information.

Detailed Information : This section is not included in the plugin as a feature. However, the plugin may be designed and people may compulsorily or voluntarily be asked for detailed information.

E-mail address : This field is put only for experimentation purposes. It is used in every step of the experimentation to correlate each participant's inputs.

Phone : This field is for the complainants who wish to be contacted by the law enforcement officials.

Content : This section is not activated but aims to get more information from the complainant.

Screenshot : This is the screenshot of the page. The database saves the screenshot in base64 format as evidence.

The plugin may be designed to receive only one complaint of a specific URL even if more than a person complaints about it. This feature is beneficial in terms of preventing duplication of efforts. However, for experimentation purposes, this feature is not activated.

4.3 "Thesis Application" - The Android Application

Android is an open source operating system. Developed and supported by Google, it is free to cell phone and tablet developers to use in their technologies [30]. The total market share of Android is much bigger than closest competitor to itself, IOS. This

makes Android the most popular operating system for smartphones. Android Operating System has its own application market called Google Play. The number of applications on Google Play increased 110 times from December 2009 to June 2018 and is currently 3.3 million apps[31]. This result also shows how big market share is owned by Android Operating System.

Nowadays, smartphones are used more than desktop and PC for social media access[32]. This is the clearest reason to have an alternative in smartphones for people to report a crime on the internet. By taking this fact into consideration, “Thesis Application” is developed for Android phones. The application is for Android 5.0 and above. This is because during the experimentation session, the app is disseminated to the experimentation participants on Google Play. Google Play accepts apps only for Android 5.0 and above versions.

When the app runs in an Android smartphone, it basically opens an interface as shown in Figure 10.

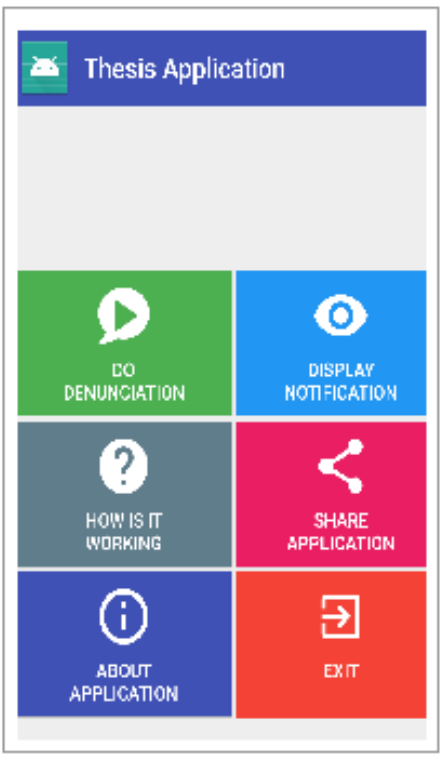


Figure 10 Main Screen of Thesis Application

The app offers a quite simple way of reporting a crime via Android based smartphones. Its interface consists of 6 sub-modules. Each of the sub-modules is explained below.

Display Notification : This field provides feedback from the unit in charge of the notification. For now, it is deactivated for experimentation purposes.

How It Is Working : This field shows how to report a crime with illustrations.

Share Application : This field aims to share the app to as many people as possible.

About Application : This field contains information about the app.

Exit : This field shuts the app down.

Do Denunciation : This field starts the reporting mechanism. After being clicked the app works in background and a head appears on the screen as shown in Figure 11.

Figure 11 Thesis Application Head on the Phone's Main Screen

Afterwards, the complainant has to go to the webpage or social media app and copy the link of the criminal content. If the URL is copied, one has to click on the head. The app working in the background takes a screenshot of the content and shows up on the screen as shown in Figure 12.

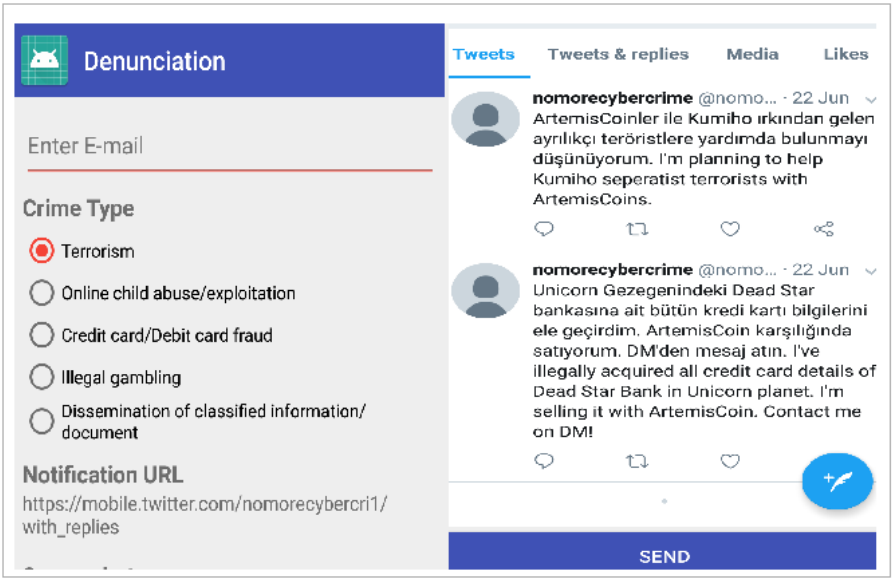


Figure 12 Thesis Application after the Captured Screenshot

E-mail address field is only for experimentation purposes. This may not be necessary for real use. Later, the complainant has to choose one of the crime types. The number of crime types may be increased depending on the country and present laws. At the very bottom of the page “Send” button must be clicked. The information retrieved from the web page and complainant interacts with Storage and Database Units and then appears in the investigator interface with an ID number assigned by the database in a format as shown in Figure 13.

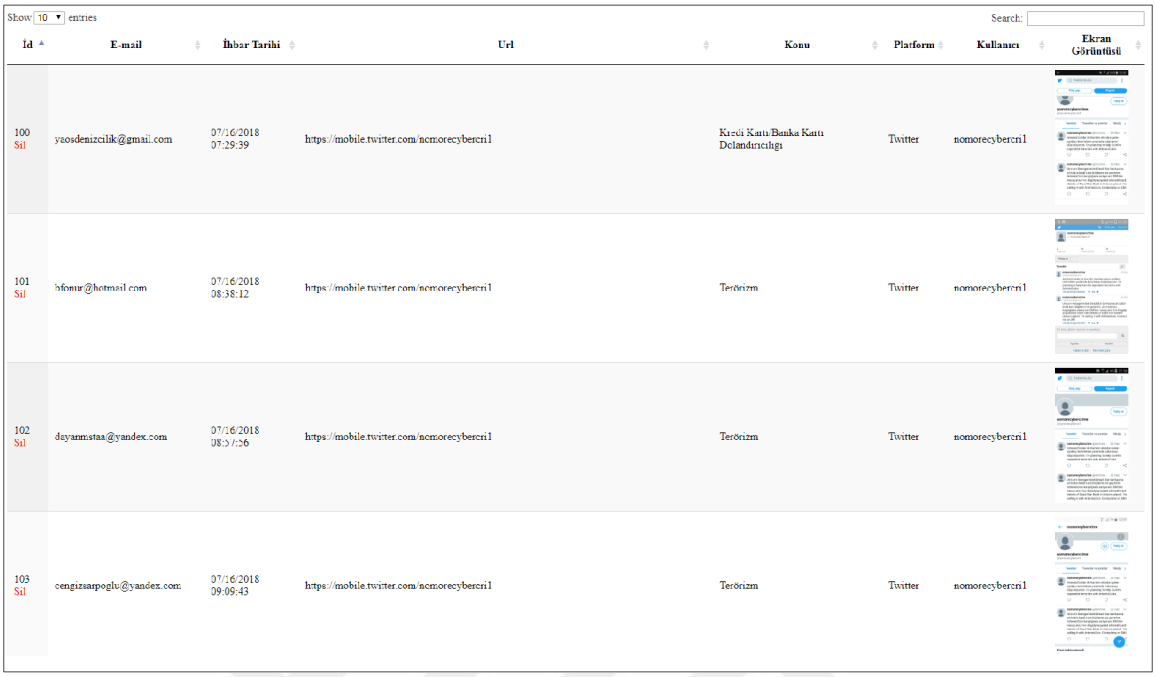


Figure 13 Investigator Interface of Thesis Application

The elements gathered by the Android App are described below (from leftmost to right):

ID : This is the unique queue number assigned by the system to list the complaints in a correct order.

E-mail address : This field is put only for experimentation purposes. It is used in every step of the experimentation to correlate each participant's inputs.

Notification Date : This is the date and time information of the complaint.

URL : This is the URL of the web page which contains criminal element. The plugin automatically captures this information.

Crime Type : This is the crime type of the content. This is very useful if the law enforcement agency decides an automatic direction of the complaints to the most relevant units and/or departments.

Platform : This is the platform that criminal act or suspicious behavior takes place. The plugin automatically detects it for social media websites. This may be designed for more platforms including blogs, online newspapers etc.

Username : Username plays a vital role when it comes to websites that distinguish users with unique numbers or names like Facebook and Twitter. Even though the users can change it, the information belongs to a person between specific dates.

Screenshot : This is the screenshot of the page. The database saves the screenshot in base64 format as evidence.

5 Description of Results

This chapter provides detailed information about how the experimentation phase is conducted and the outcomes. The experimentation phase consist of four steps. These are Pre-Condition; E-mail Complaint; IHBAR 1.0 Plugin Complaint and Thesis Application Complaint, respectively. Each step is conducted with a comprehensive group of voluntary participants. Each step and its elements are explained in the next sub-sections. All the steps are based on the same criminal content in order to compare the results.

The participation and success rates are provided. Further, the results of each step are illustrated in graphical forms. Finally, the effect of demographic variables is analysed and explained in the end.

5.1 Experimentation Phase

Experimentation phase consists of 1 pre-condition and 3 steps. The participants are asked to fill a form prepared on Google Forms. The first step of this phase is complaining about a crime using the current approach of reporting which is via e-mail. The second step is complaining about the same content via our proposed implemented plugin, IHBAR 1.0. The third and the last step is complaining with our proposed Android Application, “Thesis Application”. The pre-condition and all of the steps are explained and detail in the following sub-sections.

5.1.1 Pre-Condition

During the pre-condition step, participants are asked to fill the form including demographic information about them. In the study I conducted, 194 participants have attended the pre-condition session. Demographic information includes the number of years that internet has been actively used; if the participants have reported a crime before; operating system of their smartphones; age; gender; monthly income; education level and their job. Further, the participants are asked to provide their e-mail address for the next 3 steps. 176 of the participants have provided their e-mail address for the next step. The results are shown in Appendix 5, 6, 7, 8, 9, 10, 11 and 12.

5.1.2 The First Step - E-mail Complaint

The pre-condition participants are asked to make a complaint about a Twitter user who has posted criminal content on Twitter. There are 2 tweets. One of them is about credit card fraud and the other one is about terrorist financing. Tweets do not possess a criminal threat in real world. They are totally a fictitious world for this experiment in order to avoid any prosecution in the real world as shown in Figure 14.

Figure 14 Criminal Content for Experimentation Phase

An e-mail address which is dedicated only for e-mail complaint is shared with the participants in the form explanation, as well. The participants are asked to assume that it is the official e-mail address of the law enforcement in their countries. In order to make a thorough e-mail complaint, the complainants must basically provide a Crime Type, a URL and a Screenshot of the criminal content. They have not been informed about this fact.

Although 193 people have attended the pre-condition step (one of the participants has mistakenly filled the form 2 times. The second reply is ignored), 76 of them (%39.37) have voluntarily made e-mail complaint. 24 of 76 participants (%31.57) specify Crime Type in the e-mail, 33 of them (%43.42) specify criminal content's URL and 42 of them (%55.26) specify Screenshot of the web page. Figure 15 shows the statistical illustration of 3 pain pillars of a complete e-mail complaint.

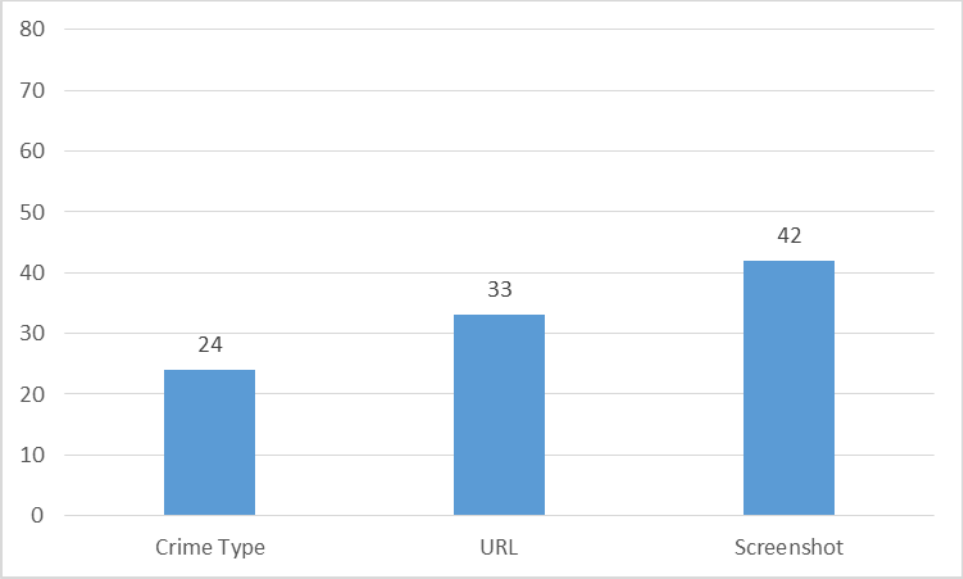


Figure 15 E-mail Complaint Results

As shown in Figure 15, people ignore to specify the Crime Type in an e-mail complaint. Only one participant has clearly specified the crime according to Turkish Penal Code. This explains that either people do not need to specify crime or people cannot decide if the content really possesses a criminal threat or not. Crime Type may be an important element if the law enforcement classifies the complaints according to the crime types.

URL is another important piece of information because it is a unique identifier for a specific webpage. By URL, everybody can display the correct webpage without any mistakes. 33 participants (%43.42) have given a place to URL. The other 43 participants have missed specifying either the entire URL or a part of it. This proves that URL doesn't have a big importance for most of the participants while reporting a crime. URL can help law enforcement to view the criminal content. And also it has great importance if the law

enforcement desires to pursue an International Mutual Legal Assistance (MLAT) through judicial process.

Screenshot becomes an important element if the criminal content is deleted or become invisible later. A screenshot may be documented and used for intelligence purposes for further steps.

In total, only 7 participants have made complaints without any defect as shown in Figure 16. This is an important point because only %9.21 of the participants' complaints can be investigated without any need for a missing element.

Total

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	incomplete	69	90,8	90,8	90,8
	complete	7	9,2	9,2	100,0
	Total	76	100,0	100,0	

Table 1 Complete and Incomplete E-mail Complaints

5.1.3 The Second Step – "IHBAR 1.0" Plugin

The second step is to ask people to report the same tweets, which were the subject of the first step, via the developed Google Chrome extension, IHBAR 1.0. The e-mail addresses gathered in the first step were used to disseminate the plugin. It was uploaded to Google Drive. Its link was shared with all the e-mail complainants. A guideline showing how to install a plugin manually was also uploaded to the drive.

71 of 76 (%93.42) of the e-mail complainants have voluntarily attended the second step. 6 participants (%8.45) have complained about each tweet separately by choosing different crime types. The rest 65 complainants (%91.54) have chosen one crime type for both of the tweets.

URL and screenshots were also automatically obtained as shown in Figure 16.

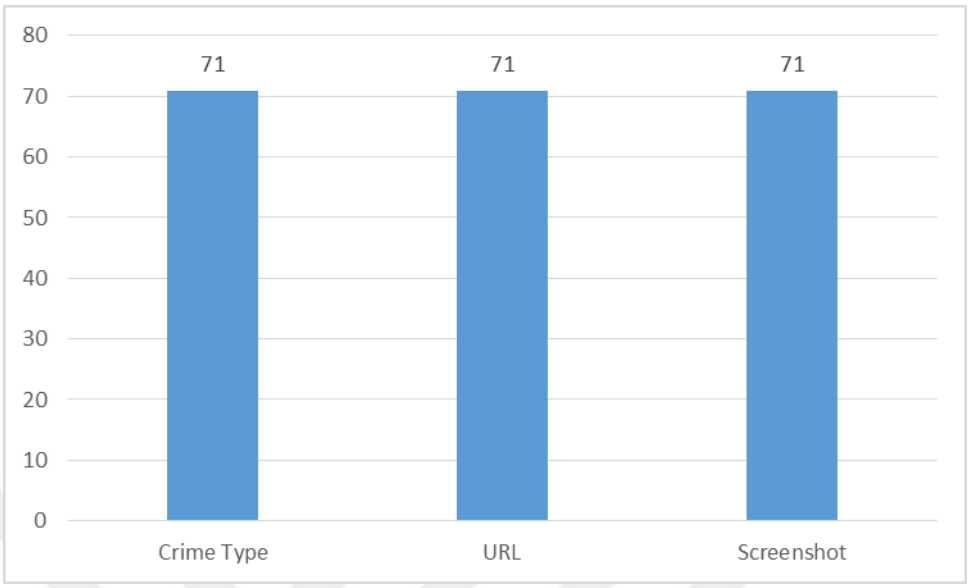


Figure 16 IHBAR 1.0 Complaint Results

All of the basic needs to start an investigation were successfully gathered by law enforcement without any mistakes.

5.1.4 The Third Step – "Thesis Application" Complaint

The third step is to ask people to report the same tweets, which were the subject of the first and second steps, via the developed Android application, Thesis Application. The e-mail addresses gathered in the second step were used to disseminate the application. It was uploaded to Google Play Market. Its link was shared with all the plugin complainants. Although some of the participants use IOS operating system in their smartphones, most of them used an Android smartphone to attend the third step.

69 of 71 (%97.18) of the "IHBAR 1.0" complaints have voluntarily attended the third step. Only 1 participant has complained about the tweets separately by choosing different crime types.

URL and screenshots were also automatically obtained as shown in Figure17.

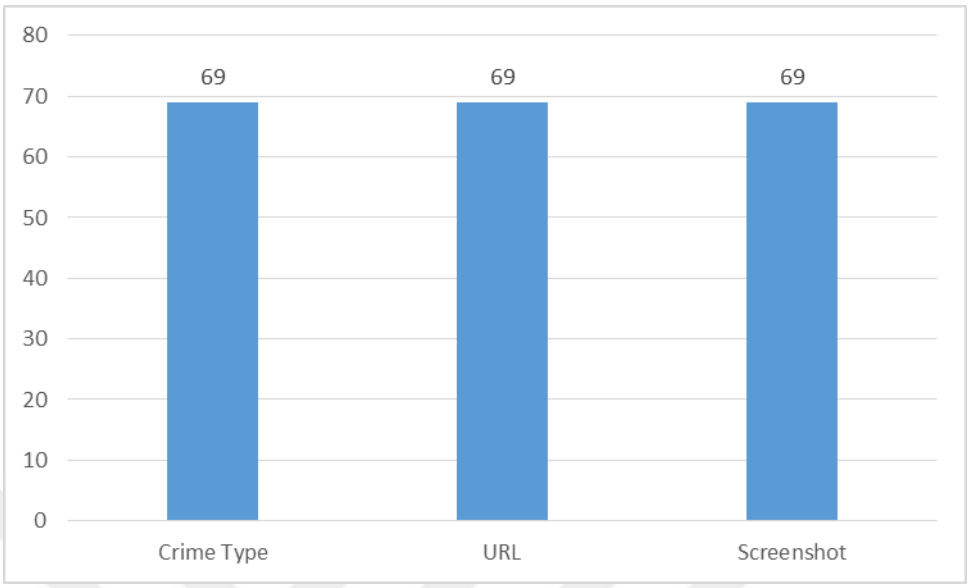


Figure 17 Thesis Application Complaint Results

All of the basic needs to start an investigation were successfully gathered by law enforcement without any mistakes.

5.2 Effect of Demographic Variables on E-mail Complaints

The experimentation shows that when the subjects make a complaint by themselves (without any options or orientations), they tend to miss one or more elements of the complaint as explained in the previous chapter. On the other hand, it is very clear that the proposed system do not miss any elements. The software captures all the required information. The correlation between demographic resources and e-mail complaint success is examined the sections below.

5.2.1 Have You Ever Reported a Crime

Group Statistics

	Haveyoueverreported acrimeyouhaveencou	N	Mean	Std. Deviation	Std. Error Mean
Total	No	39	,05	,223	,036
	Yes	37	,14	,347	,057

Table 2 Group Statistics of Those Who Have Reported or Have Not

According to our study, 37 of the participants have reported an internet crime in the past while the other 39 have not. When the effect of reporting or not reporting an internet crime on e-mail complaint success is evaluated, 2 hypotheses are created:

H_0 = There is no difference between those who have reported a crime in the past and those who have not in terms of success via e-mail complaint.

H_1 = There is difference between those who have reported a crime in the past and those who have not in terms of success via e-mail complaint.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Total	Equal variances assumed	6,828	,011	-1,260	74	,212	-,084	,067	-,216	,049
	Equal variances not assumed			-1,246	61,005	,217	-,084	,067	-,218	,051

Table 3 Independent Sample Test

According to Independent Sample Test in Table 3, since Sig. (2-tailed) 0.217>0.05, H_0 reflects the truth. It means that when it comes to the success rate, there is no difference between those who have reported a crime in the past and those who have not in terms of success via e-mail complaint.

5.2.2 Education Level

Descriptives

Total

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
High School	14	,00	,000	,000	,00	,00	0	0
Associate's Degree	11	,09	,302	,091	-,11	,29	0	1
Bachelor's Degree	42	,12	,328	,051	,02	,22	0	1
Master's Degree	8	,13	,354	,125	-,17	,42	0	1
PhD	1	,00	.	.	.	.	0	0
Total	76	,09	,291	,033	,03	,16	0	1

Table 4 Education Level Descriptive

Table 4 shows the descriptive of education level amongst the participants. For instance, there are 42 participants who have Bachelor's Degree. Standard Deviation of this category is 0,302 and standard error is 0,91.

When the effect of education level on e-mail complaint success is evaluated, 2 hypotheses are created:

H_0 = Education level does not affect the success of e-mail complaint.

H_1 = Education level affects the success of e-mail complaint.

ANOVA

Total

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	,166	4	,042	,477	,752
Within Groups	6,189	71	,087		
Total	6,355	75			

Table 5 One Way ANOVA Test for Education Level

According to the One Way ANOVA Test in Table 5, since Sig=0,752>0,05, , H_0 reflects the truth. It means that when it comes to the success rate, education level does not affect the success of e-mail complaint.

5.2.3 How Long Have You Been Using the Internet Actively

Descriptives

Total

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
0-5	7	,00	,000	,000	,00	,00	0	0
6-9	15	,00	,000	,000	,00	,00	0	0
10-13	22	,14	,351	,075	-,02	,29	0	1
14+	32	,13	,336	,059	,00	,25	0	1
Total	76	,09	,291	,033	,03	,16	0	1

Table 6 Internet Usage Year Descriptive

Table 6 shows the descriptive of the number of internet usage years amongst the participants. For instance, there are 32 participants who have been using the internet actively more than 14 years. Standard Deviation of this category is 0,336 and standard error is 0,59.

When the effect of education level on e-mail complaint success is evaluated, 2 hypothesis are created:

H_0 = There is no correlation between the years of internet usage and e-mail complaint success.

H_1 = There is correlation between the years of internet usage and e-mail complaint success.

ANOVA

Total

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	,264	3	,088	1,042	,379
Within Groups	6,091	72	,085		
Total	6,355	75			

Table 7 One Way ANOVA Test for Internet Usage Years

Since Sig=0.379>0,05, H_0 reflects the truth. It means that there is no correlation between the years of internet usage and e-mail complaint success.

6 Conclusion

The major contribution of this study is creating an original and unique reporting mechanism for internet crimes. This mechanism does not only reduce the efforts of the complainants and motivates them not to ignore an internet crime but also it facilitates the efforts of law enforcement officials if there is a problem with the complaint such as lack of a requirement in the complaint.

In this study, e-mail complaint, desktop browser plugin and mobile application are tested and analysed to compare the success rate. There is a big difference between the results. The results show that the individuals tend to miss or ignore a part of required information in the e-mail complaints. This may be because they are unaware of what to specify in an e-mail complaint or they only specify the most important elements according to themselves. However, the created software are able to capture all the requirements regardless of the complainant's priorities.

Moreover, the results show that reporting a crime via e-mail is independent from education level, reporting a crime in the past and number of internet usage years. This means that complainants from various parts of the community can make mistake during a reporting process. On the other hand, the proposed system works notwithstanding these kinds of variables by offering a simple reporting process.

Having such a mechanism is very fruitful for law enforcement, as well. This is because in case of anonymity, the complainant may not be reached again and this situation may fail prosecuting a threat. On the other hand with the offered system, this situation cannot be a matter of inadequacy. The proposed mechanism can also minimize the duplication of efforts. The software can be designed to illustrate only one complaint on the investigator interface even if thousands of people complain about the same content.

7 List of References

[1] G. n. Kimenju, “Determinants of Reporting or Failing to Report a Crime to Police: a Case Study of Githurai 45, Nairobi: University of Nairobi, 2015.

[2] H. Goudriaan, Reporting crime: Effects of social context on the decision of victims to notify the police. Veenendaal: Universal Press, 2006.

[3] S. of V. Australia, “Reasons to report a crime”, 25-Jul-2017. URL: https://www.victimsofcrime.vic.gov.au/the-crime/reasons-to-report-a-crime. Last Accessed on 03-Mar-2018.

[4] N. Z. G. Ministry of Justice, “Reporting a Crime”, 13-Jun-2016. URL: http://www.victimsinfo.govt.nz/police-involvement/reporting-a-crime/. Last Accessed on 03-Mar-2018.

[5] C. of P. Office of Victim Services, “THE IMPORTANCE OF REPORTING A CRIME”. URL: http://pcv.pccd.pa.gov/available-services/Pages/The-Importance-of-Reporting-a-Crime.aspx. Last Accessed on 04-Mar-2018.

[6] E. Police Service, “Why should you report a crime?”. URL: http://www.edmontonpolice.ca/ContactEPS/ReportACrime.aspx. Last Accessed on 04-Mar-2018.

[7] M. C. Scheider, D. L. Spence, and J. Mansourian, The relationship between economic conditions, policing, and crime trends. Washington, DC: US Department of Justice, 2012.

[8] S. I. Ranapurwala, M. T. Berg, and C. Casteel, “Reporting crime victimizations to the police and the incidence of future victimizations: a longitudinal study”, PloS One, 2016.

[9] R. B. Felson, S. F. Messner, A. W. Hoskin, and G. Deane, “Reasons for reporting and not reporting domestic violence to the police”, Criminology, 2002.

[10] B. David, “Reporting crime is a waste of time, says survey”, 24-Oct-2010 URL: www.telegraph.co.uk, Last Accessed on 21-Mar-2018

[11] H. Goudriaan, Reporting crime: Effects of social context on the decision of victims to notify the police. Veenendaal: Universal Press, 2006.

[12] G. A. Antonopoulos, “Public reporting of criminal activities to the police in Greece: is there a difference when the offender is migrant?”, Eur. J. Crime Crim. Law Crim. Justice, 2006.

[13] J. L. Truman, “National Crime Victimization Survey Criminal Victimization, 2010”. Washington D.C.: US Department of Justice, 2011.

[14] L. Langton, M. Berzofsky, C. P. Krebs, and H. Smiley-McDonald, Victimizations not reported to the police, 2006-2010. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2012.

[15] Migration and Home Affairs, “Cybercrime”, 20-Mar-2018 URL: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en. Last Accessed on 20-Mar-2018.

[16] Norton Security, “What is Cybercrime”. 20-Mar-2018. URL: https://www.nortonsecurityonline.com/security-center/cybercrime.html. Last Accessed on 20-Mar-2018.

[17] Interpol General Secretariat, “Global Cybercrime Strategy”. Lyon: Interpol, 2017.

[18] M. McGuire and S. Dowling, “Cyber crime: A review of the evidence”, Home Office, 2013.

[19] T. U. S. Department of Justice, “REPORTING COMPUTER, INTERNET-RELATED, OR INTELLECTUAL PROPERTY CRIME”, 03-Mar-2017. URL: https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. Last Accessed on 14-Mar-2018.

[20] US DOJ, FBI, “Internet Crime Complaint Center (IC3)”. URL: https://www.ic3.gov/about/default.aspx. Last Accessed on 17-Mar-2018.

[21] U. S. Secret Service, “The Investigative Mission”. URL: https://www.secretservice.gov/investigation/#cyber. Last Accessed on 19-Mar-2018.

[22] U. S. Department of Homeland Security, “Cyber Incident Reporting, A Unified Message for Reporting to the Federal Government”, Homeland Security, 2016.

[23] U. S. Immigration and Customs Enforcement, “Who We Are”, 01-Mar-2018. URL: https://www.ice.gov/about. Last Accessed on 19-Mar-2018.

[24] “United States Postal Inspection Service”, 20-Şub-2018. URL: https://en.wikipedia.org/wiki/United_States_Postal_Inspection_Service. Last Accessed on 20-Mar-2018.

[25] US DOJ, Bureau of Alcohol, Tobacco, Firearms and Explosives, “About the Bureau of Alcohol, Tobacco, Firearms and Explosives”. URL: https://www.atf.gov/. Last Accessed on 20-Mar-2018.

[26] National Fraud & Cyber Crime Reporting Centre. URL: https://www.actionfraud.police.uk/.Last Accessed on 25-Feb-2018.

[27] StatCounter Global Stats “Desktop Browser Market Share Worldwide”, URL: http://gs.statcounter.com/browser-market-share/desktop/worldwide. Last Accessed on 16-Jul-2018.

[28] StatCounter Global Stats “Mobile Operating System Market Share Worldwide”, URL: http://gs.statcounter.com/os-market-share/mobile/worldwide. Last Accessed on 16-Jul-2018].

[29] A. Grosskurth and M. W. Godfrey, “A Reference Architecture for Web Browsers”, Waterloo: School of Computer Science University of Waterloo, 2005.

[30] J. Higginbotham and S. Jacobs, “The Future of the Android Operating System for Augmentative and Alternative Communication”, SIG 12 Perspectives on Augmentative and Alternative Communication, 2011.

[31] Statista, “Number of Google Play Store apps 2018 | Statistic”, URL: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/. Last Accessed on 19-Jul-2018.

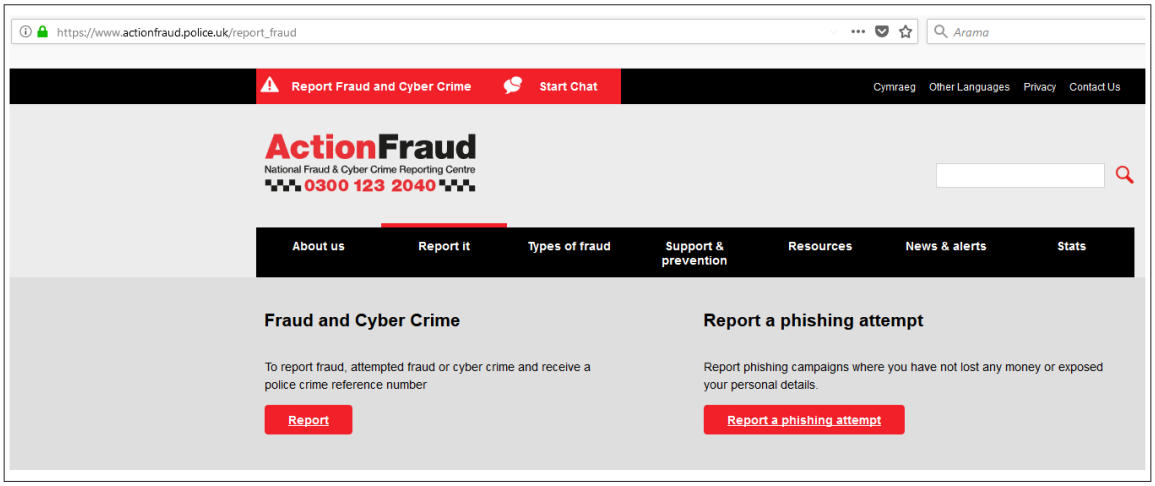
[32] G. Sterling, “Nearly 80 percent of social media time now spent on mobile devices - Marketing Land”, URL: https://marketingland.com/facebook-usage-accounts-1-5-minutes-spent-mobile-171561, 2016.

8 Appendices

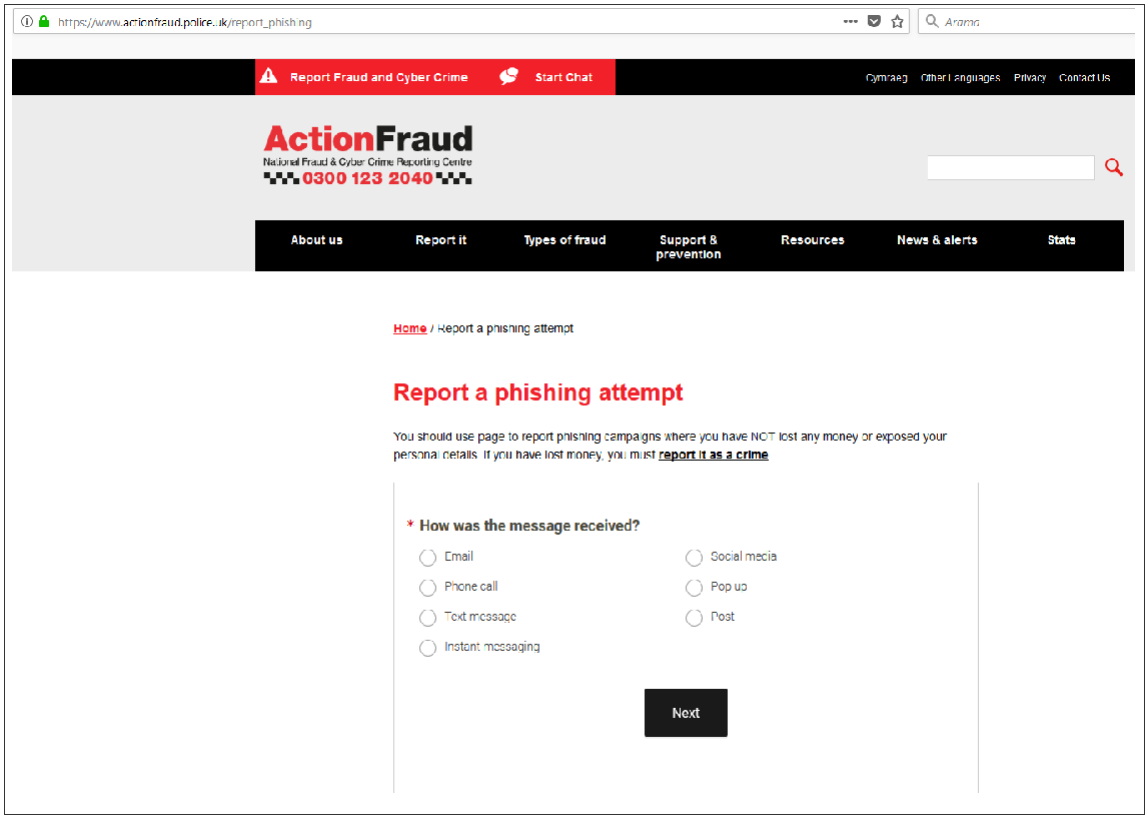
8.1 Appendix A – Law Enforcement Reporting Forms

Appendix 1 IC3's Crime Types to Report

Appendix 2 IC3's Pre-Conditions

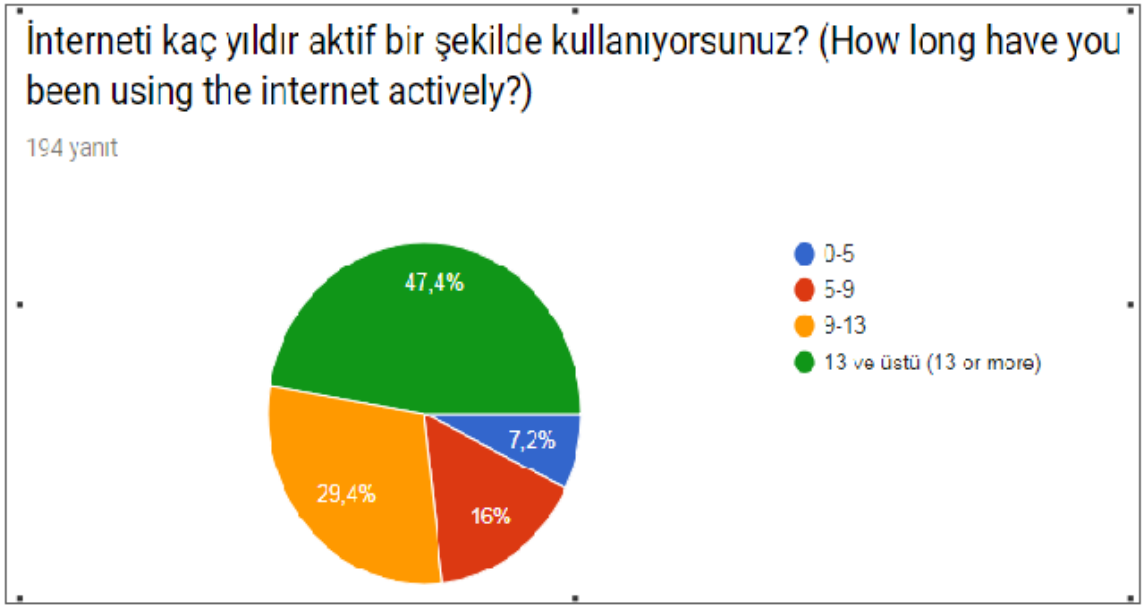


Appendix 3 ActionFraud's Crime Types to Report

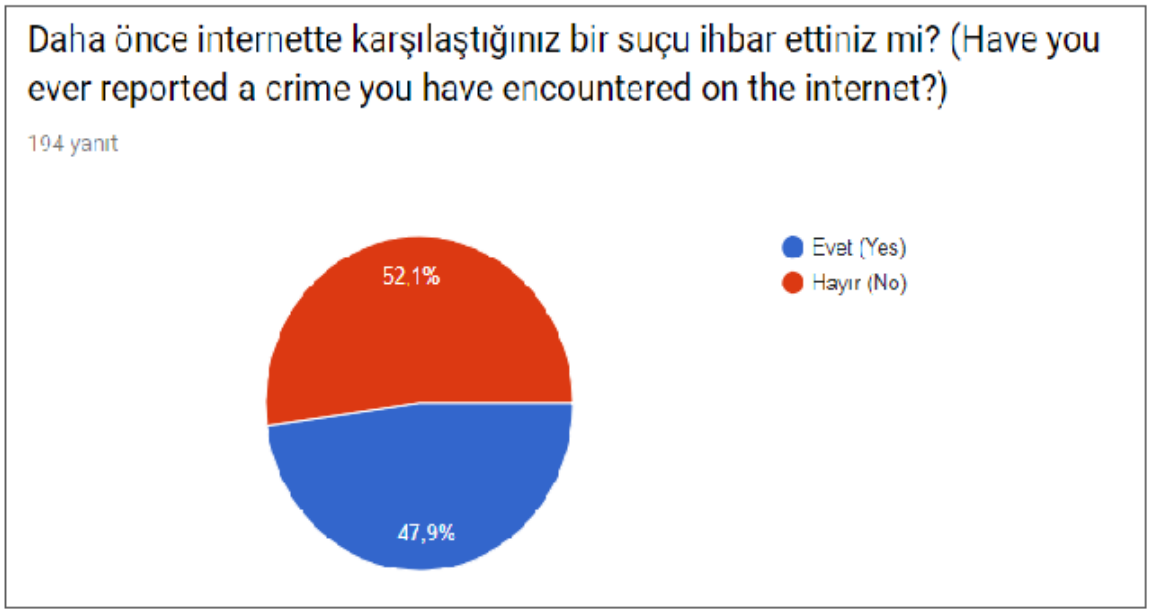


Appendix 4 ActionFraud's Phising Form

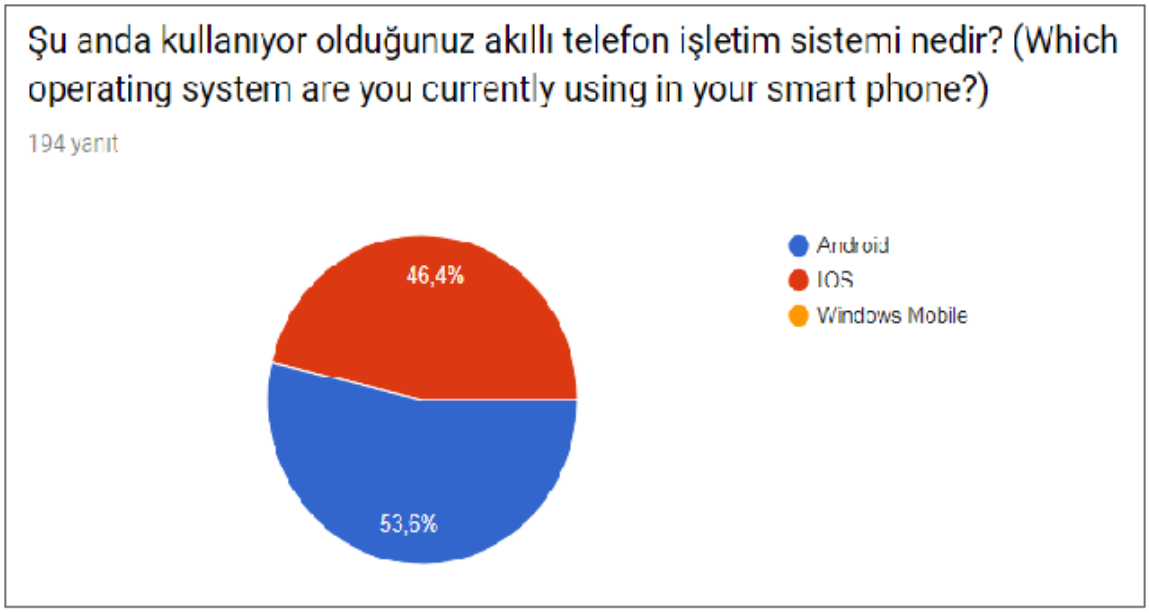
8.2 Appendix B – Demographic Backgrounds of the Participants



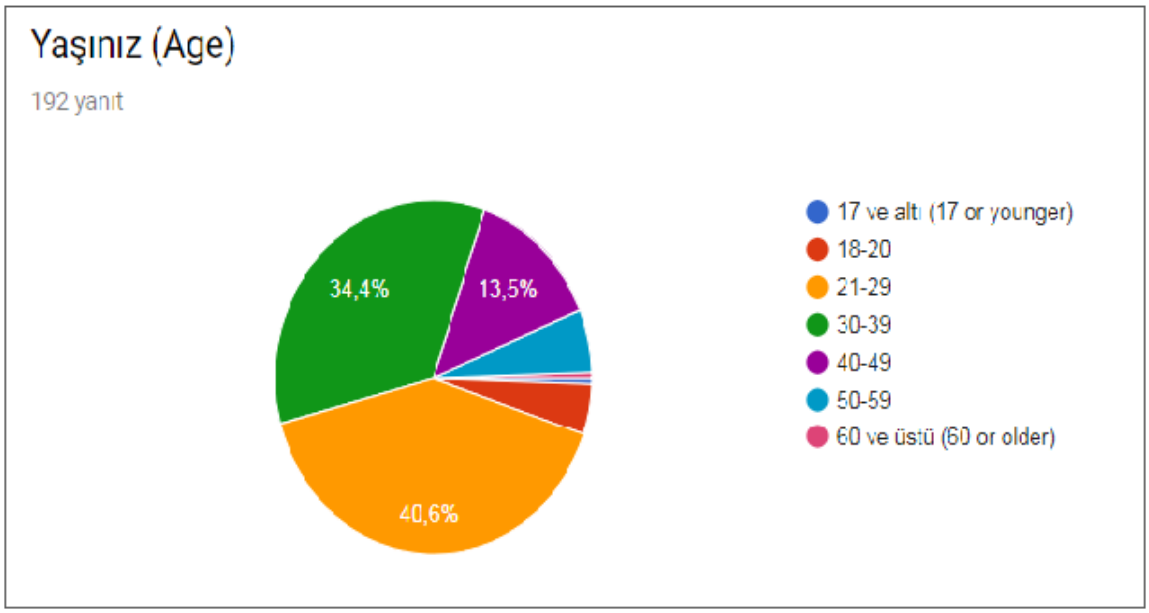
Appendix 5 Number of Internet Usage Years



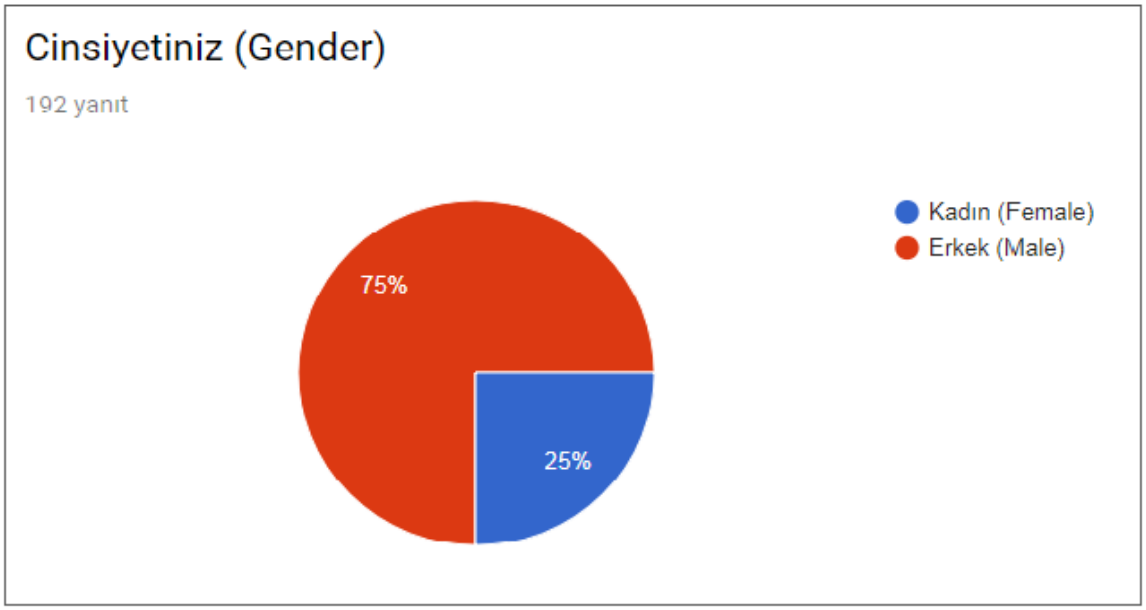
Appendix 6 Reporting Experience



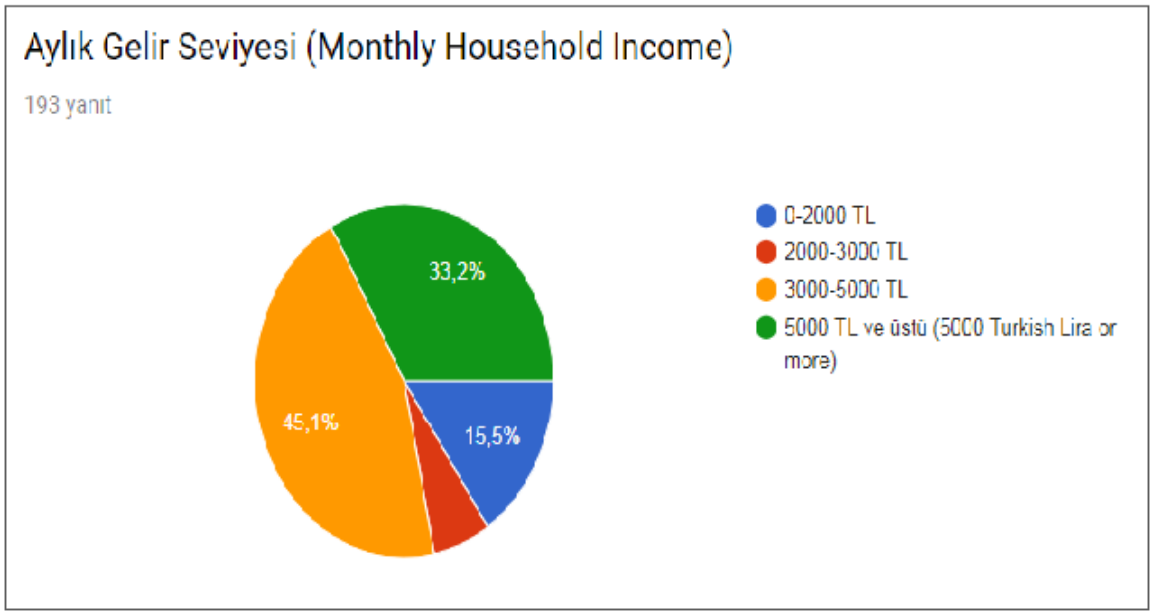
Appendix 7 Smartphone Operating System



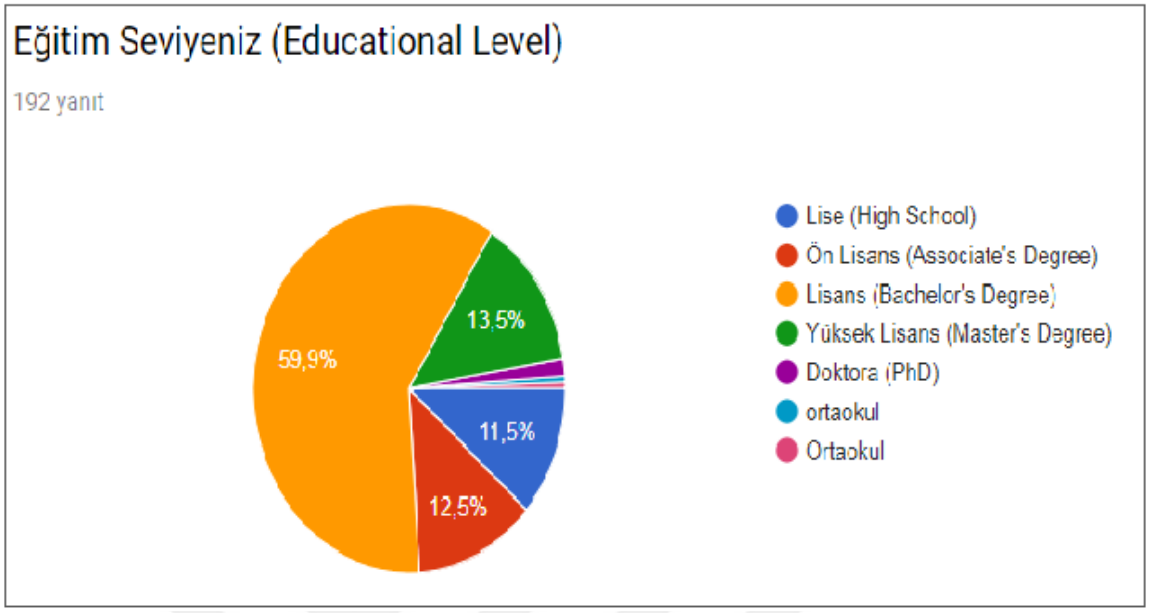
Appendix 8 Age



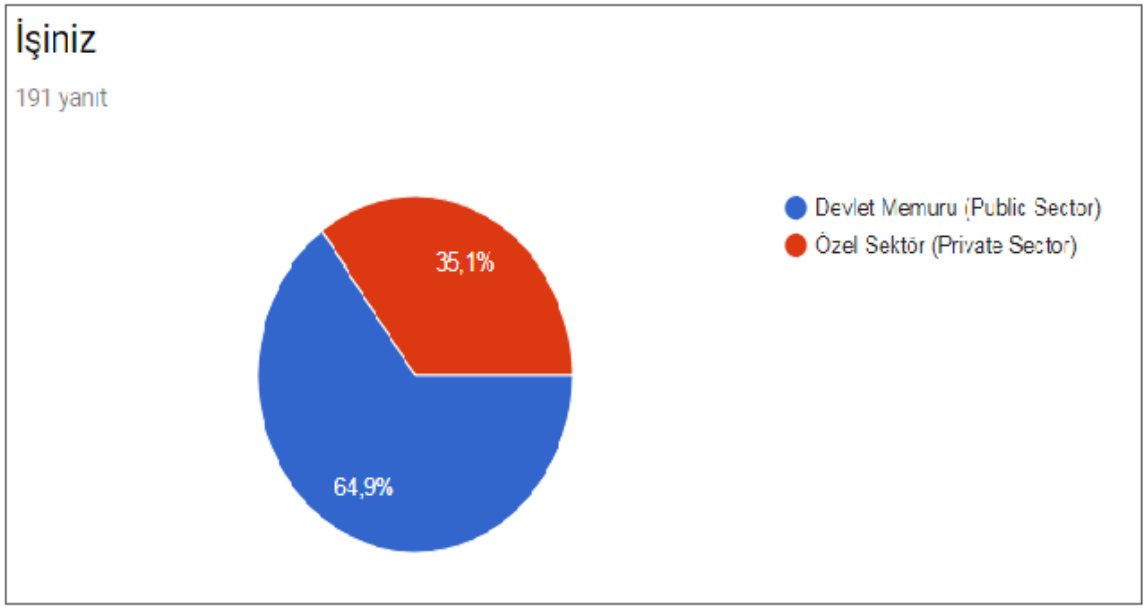
Appendix 9 Gender



Appendix 10 Monthly Income



Appendix 11 Education Level



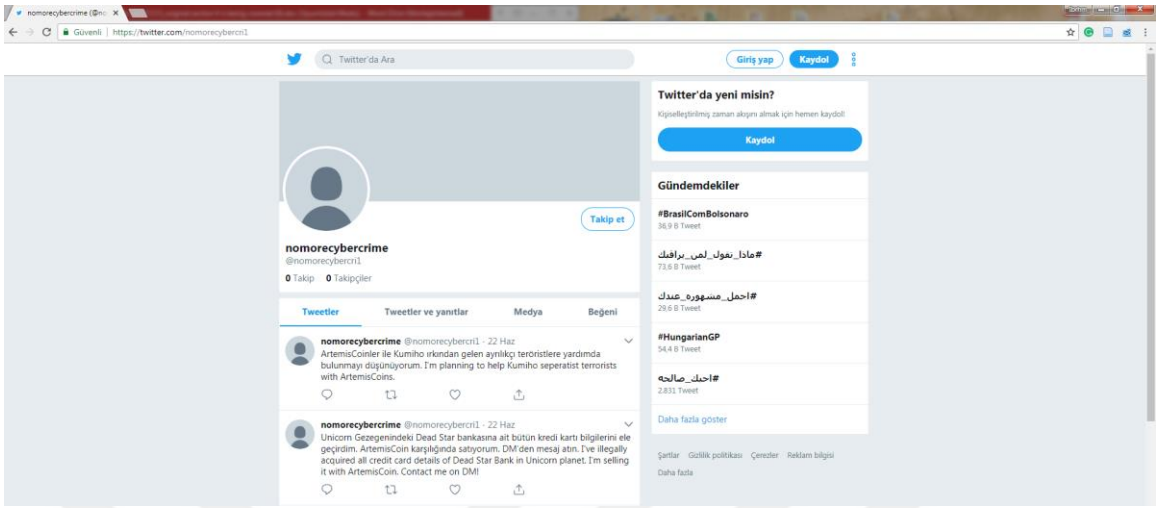
Appendix 12 Job

8.3 Appendix C – User Manual for IHBAR 1.0

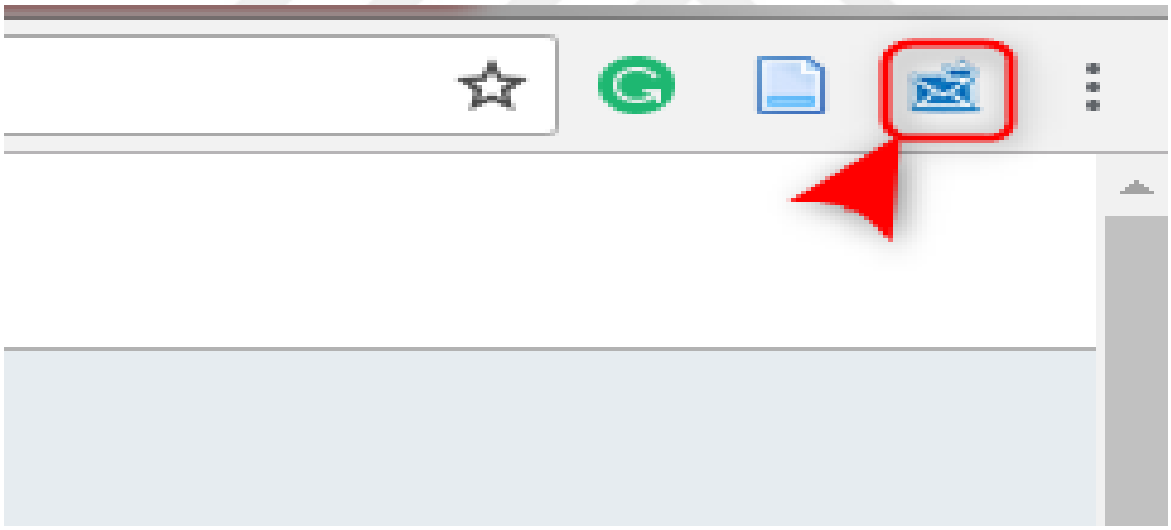
Chapter 8.3 explains how to install IHBAR 1.0 Plugin. Then, how to use and report a crime is explained step by step.

1. Öncelikle, size e-posta ile göndermiş olduğum link üzerinden **"chrext2"** isimli .rar uzantılı dosyayı indiriniz. Firstly, download the .rar file named **"chrext2"** via the link I've sent your e-mail address.
2. İndirdiğiniz dosyaya sağ tıklayarak **"Dosyaları Çıkart"** seçeneğine bastıktan sonra önünüze gelecek ekrandan istediğiniz konumu seçerek dosyayı çıkarınız. Press right click on the .rar file then press **"Exract files"**. Choose your destination then press "Ok".
3. Google Chrome'u açınız. Open Google Chrome.
4. Sağ üstte göreceğiniz alt alta sıralanmış 3 noktalı kısıma tıklayarak **"Diğer Araçlar"** ardından **"Uzantılar"**a tıklayınız. Find and click the bottom line ordered 3 points on the top right corner. Press **"Other Tools"** then press **"Extensions"**.
5. Açılan sayfada tarayıcınıza (eğer varsa) zaten yüklü olan uzantıları göreceksiniz. You'll see the extensions already installed on your browser (if there is any).
6. Sağ üstte göreceğiniz **"Geliştirici Modu"** sekmesinin açık olmasına lütfen dikkat ediniz. Aksi halde diğer adımları takip edemeyeceksiniz. Please note that **"Developer Mode"** tab on the top right corner must be on. Otherwise, you'll fail to follow the next steps.
7. Üstte göreceğiniz **"Paketlenmemiş Öğe Yükle"** sekmesine tıklayınız. Press **"Load Unpacked Item"** on the top.
8. Açılan ekrandan, **2. adımda seçtiğiniz konuma giderek** çıkardığınız dosyayı seçiniz. Find the file that you've extracted **in step 2** and pick it.
9. Ekranda **"İHBAR 1.0"** yazılı bir uzantı görüyorsanız uzantıyı başarıyla yüklediniz demektir. If you are able to see an extension named **"İHBAR 1.0"**, it means that you've successfully installed the extension.

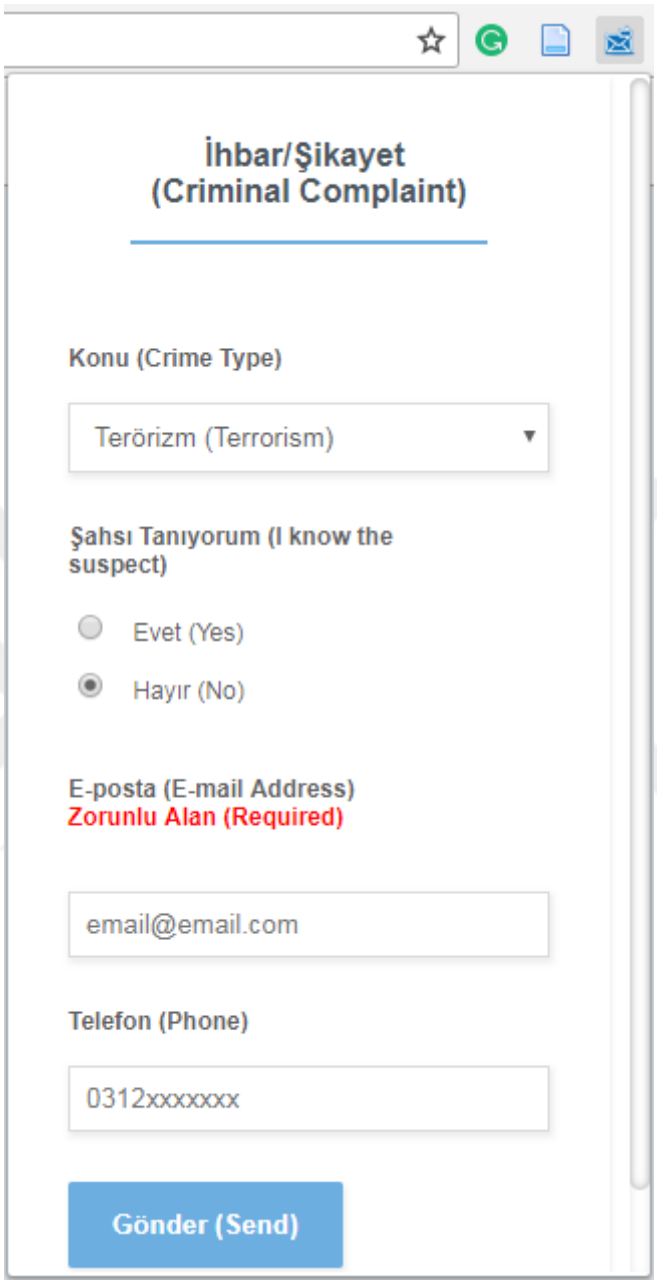
Appendix 13 How to Install IHBAR 1.0 Plugin



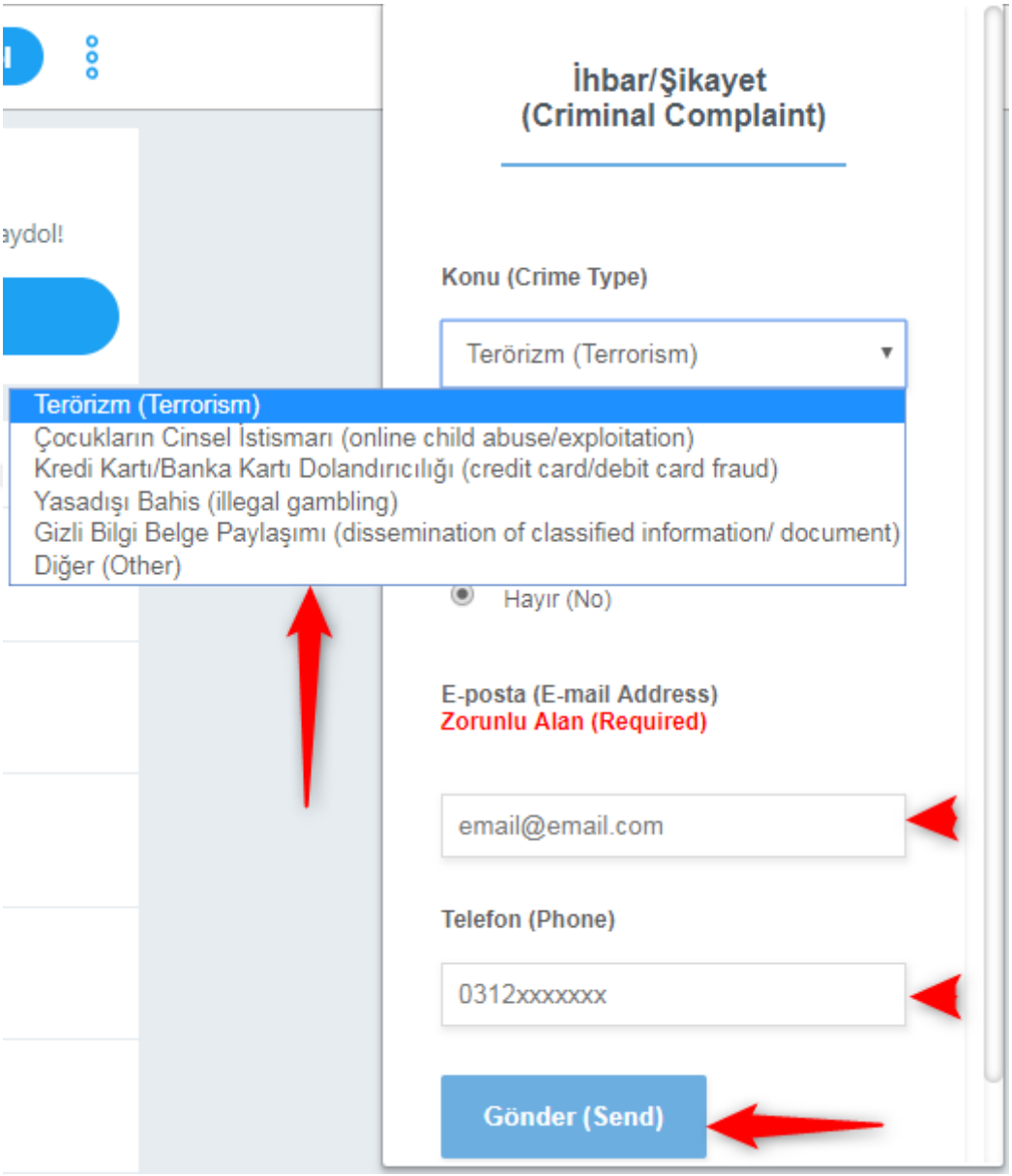
Appendix 14 Step 1



Appendix 15 Step 2



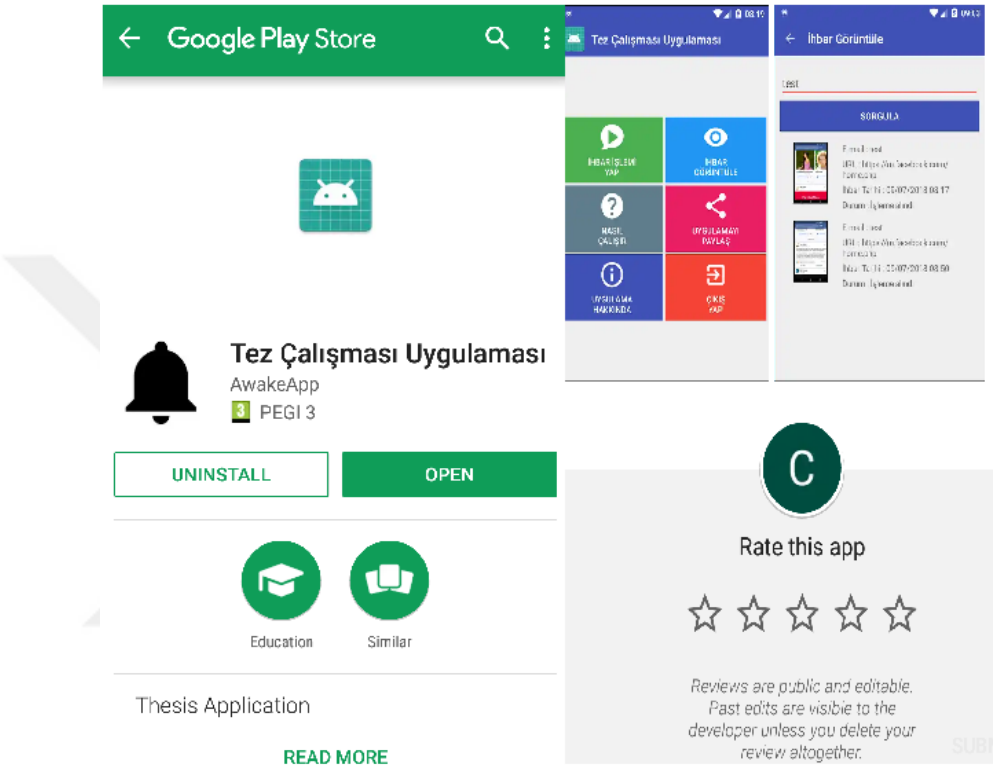
Appendix 16 Step 3



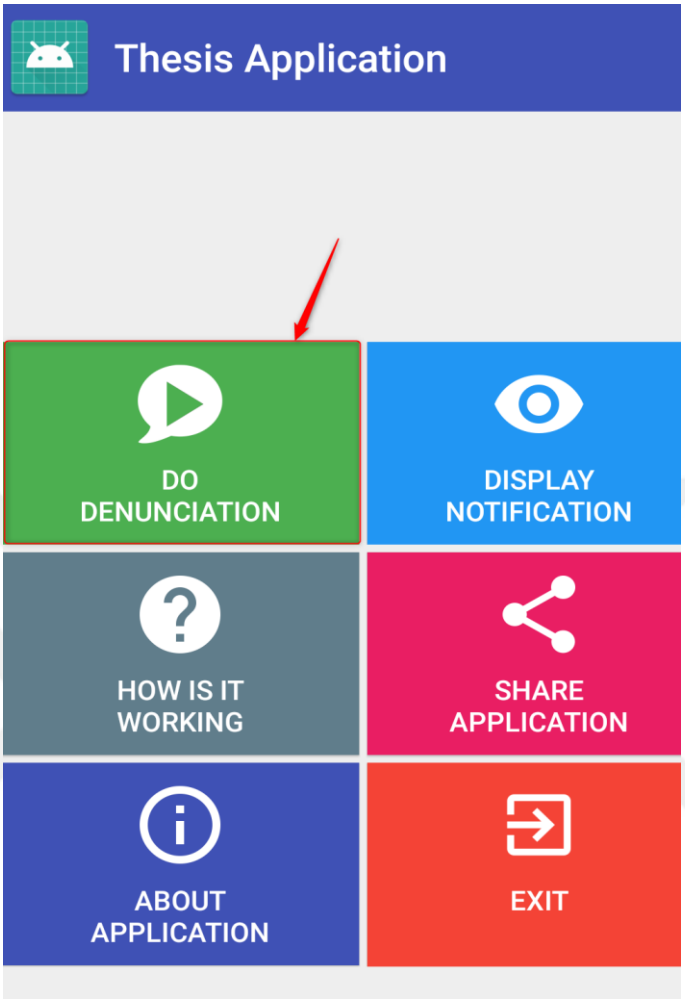
Appendix 17 Step 4

8.4 Appendix D - User Manual for Thesis Application

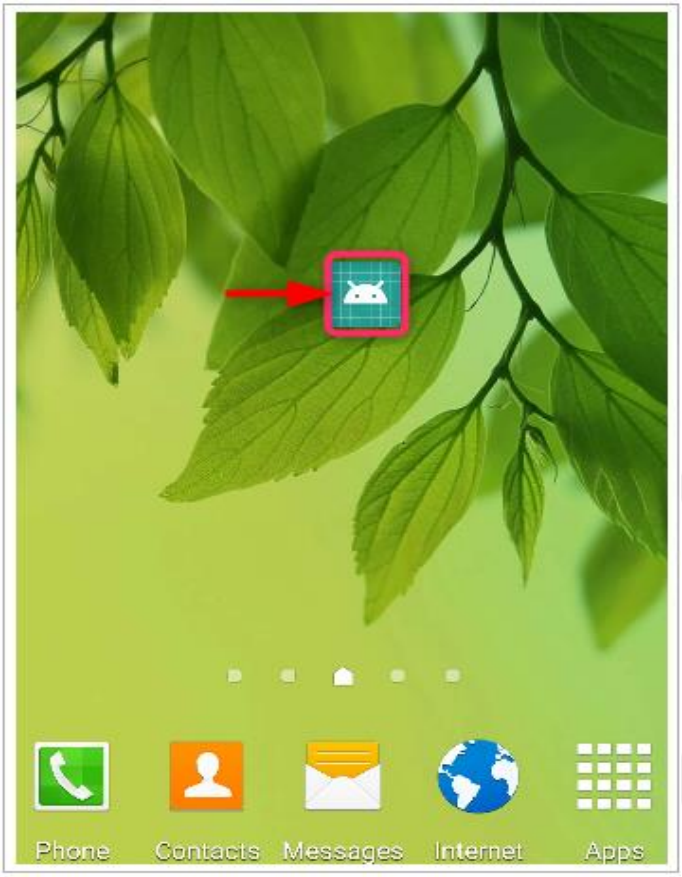
Chapter 8.4 explains how to install Thesis Application. Then, how to use and report a crime is explained step by step.



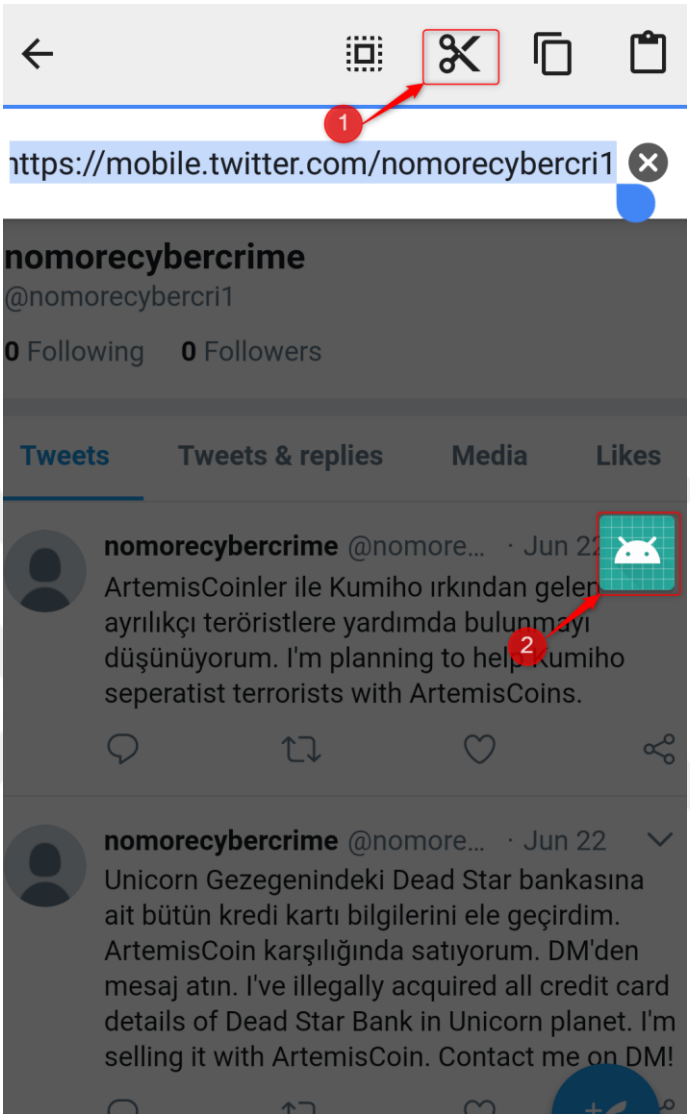
Appendix 18 Thesis Application on Google Play



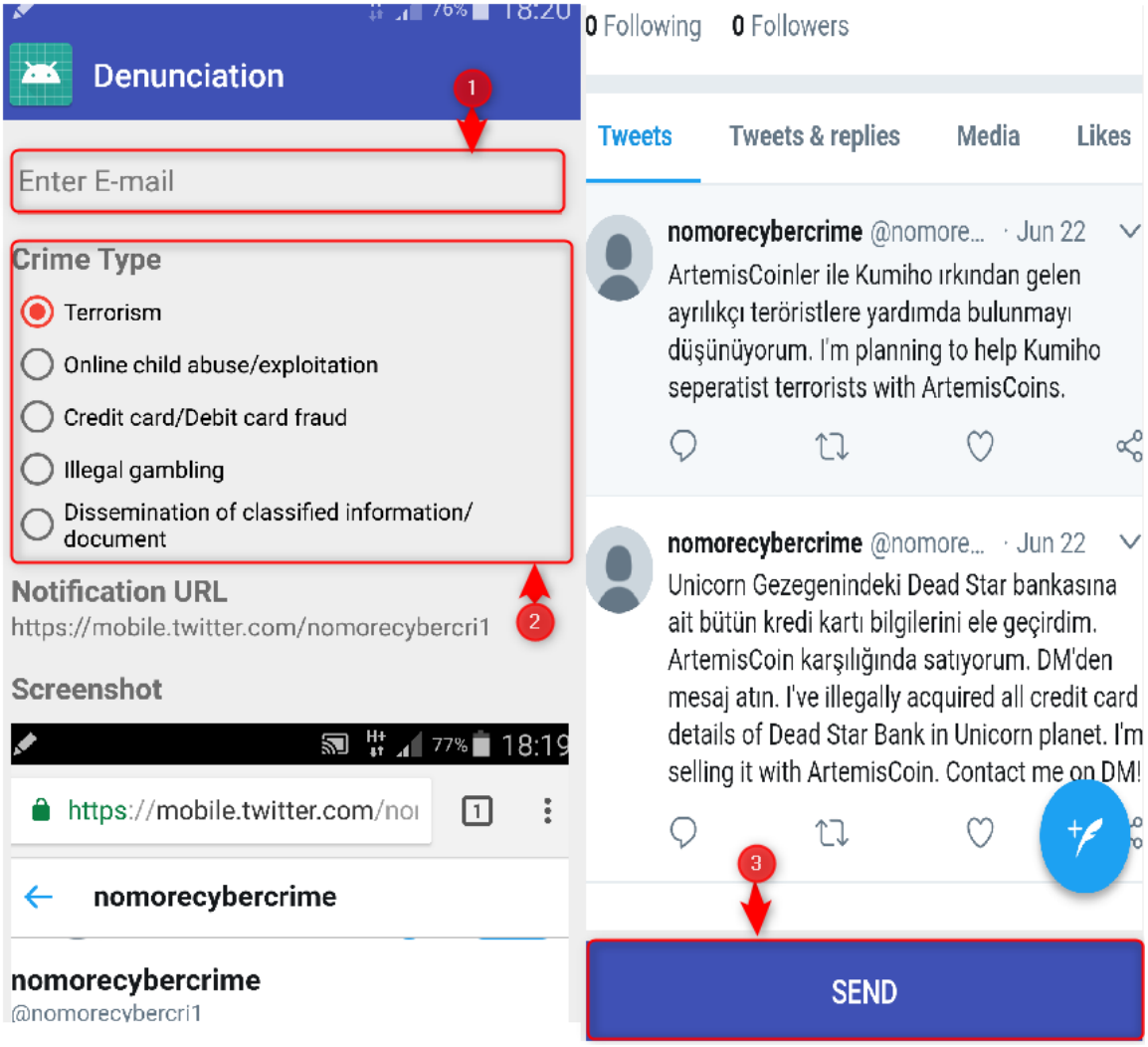
Appendix 19 Thesis Application Main Screen



Appendix 20 Thesis Application Head on the Phone's Main Screen



Appendix 21 URL Copying and Thesis Application Head Using



Appendix 22 Last Step of Reporting via Thesis Application

8.5 Appendix E – Important Source Code Functions of the "Thesis Application"

Function 1: Imported Class and Library Elements

```
import android.annotation.TargetApi;
import android.app.Dialog;
import android.content.ClipData;
import android.content.ClipboardManager;
import android.content.Context;
import android.content.Intent;
import android.graphics.Bitmap;
import android.graphics.PixelFormat;
import android.graphics.Point;
import android.hardware.display.DisplayManager;
import android.hardware.display.VirtualDisplay;
import android.media.Image;
import android.media.ImageReader;
import android.media.MediaPlayer;
import android.media.projection.MediaProjection;
import android.media.projection.MediaProjectionManager;
import android.os.Build;
import android.os.Bundle;
import android.os.Environment;
import android.os.Handler;
import android.os.Looper;
import android.provider.MediaStore;
import android.support.v4.app.FragmentManager;
```

```
import android.support.v4.app.FragmentTransaction;
import android.support.v7.app.AppCompatActivity;
import android.util.Base64;
import android.util.DisplayMetrics;
import android.util.Log;
import android.view.Display;
import android.view.KeyEvent;
import android.view.LayoutInflater;
import android.view.View;
import android.widget.Button;
import android.widget.ImageButton;
import android.widget.ImageView;
import android.widget.Toast;

import com.android.volley.AuthFailureError;
import com.android.volley.Request;
import com.android.volley.RequestQueue;
import com.android.volley.Response;
import com.android.volley.VolleyError;
import com.android.volley.toolbox.StringRequest;
import com.android.volley.toolbox.Volley;
import com.example.bubbles.BubbleLayout;
import com.example.bubbles.BubblesManager;
import com.example.bubbles.OnInitializedCallback;

import java.io.ByteArrayOutputStream;
```

```
import java.io.File;

import java.io.FileOutputStream;

import java.io.IOException;

import java.nio.ByteBuffer;

import java.util.HashMap;

import java.util.Map;
```

Function 2: Function that saves the screenshot to the phone's gallery from media projection

```
private class ImageAvailableListener implements
ImageReader.OnImageAvailableListener {

    @Override

    public void onImageAvailable(ImageReader reader) {

        Image image = null;

        FileOutputStream fos = null;

        bitmap = null;


        requestQueue = Volley.newRequestQueue(getApplicationContext());


        try {


            image = mImageReader.acquireLatestImage();


            if (image != null) {

                Image.Plane[] planes = new Image.Plane[0];

                planes = image.getPlanes();

                ByteBuffer buffer = null;
```

```
                buffer = planes[0].getBuffer();

                int pixelStride = 0;

                pixelStride = planes[0].getPixelStride();

                int rowStride = 0;

                rowStride = planes[0].getRowStride();


                int rowPadding = rowStride - pixelStride * mWidth;

                // create bitmap

                bitmap = Bitmap.createBitmap(mWidth + rowPadding / pixelStride, mHeight,
Bitmap.Config.ARGB_8888);

                bitmap.copyPixelsFromBuffer(buffer);

                // write bitmap to a file

                fos = new FileOutputStream(STORE_DIRECTORY + "/myscreen_" +
IMAGES_PRODUCED + ".jpg");

                bitmap.compress(Bitmap.CompressFormat.JPEG, 100, fos);


                if (screen_shot) {


                   if (sayac == 1) {

                       bmp_screenshoot = bitmap;

                       dbKaydet();


                       MediaStore.Images.Media.insertImage(getContentResolver(),
bmp_screenshoot, "Resimlerim", "screenshot");


                       sayac = 0;


                       onResume();
```

```
            }

            stopProjection();


        }
        IMAGES_PRODUCED++;
        Log.e(TAG, "captured image: " + IMAGES_PRODUCED);
    }

} catch (Exception e) {
    e.printStackTrace();
} finally {
    if (fos != null) {
        try {
            fos.close();
        } catch (IOException ioe) {
            ioe.printStackTrace();
        }
    }

    if (bitmap != null) {
        bitmap.recycle();
    }
```

```
            if (image != null) {
                image.close();
            }
        }
    }
}
```

Function 3: Function that creates virtual screen in media projection

```
@TargetApi(Build.VERSION_CODES.LOLLIPOP)
    private class MediaProjectionStopCallback extends MediaProjection.Callback {
        @Override
        public void onStop() {
            Log.e("ScreenCapture", "stopping projection.");
            mHandler.post(new Runnable() {
                @Override
                public void run() {
                    if (mVirtualDisplay != null) mVirtualDisplay.release();
                    if (mImageReader != null)
mImageReader.setOnImageAvailableListener(null, null);


                    sMediaProjection.unregisterCallback(MediaProjectionStopCallback.this);
                }
            });
        }
    }
```

Function 4: Function that encodes the screenshot to base64

```
public String getStringImage(Bitmap bmp) {
        ByteArrayOutputStream baos = new ByteArrayOutputStream();
        bmp.compress(Bitmap.CompressFormat.JPEG, 50, baos);
        byte[] imageBytes = baos.toByteArray();
        String encodedImage = Base64.encodeToString(imageBytes, Base64.DEFAULT);
        return encodedImage;
    }
```

Function 5: Function that sends the captured data to the database

```
public void dbKaydet() {
        final String image = getStringImage(bmp_screenshoot);
        String[] dizi = textUrl.split("/");
        ortam = dizi[2];

        StringRequest request = new StringRequest(Request.Method.POST, url_kaydet,
new Response.Listener<String>() {
            @Override
            public void onResponse(String response) {



            }
        }, new Response.ErrorListener() {
            @Override
            public void onErrorResponse(VolleyError error) {
```

```
        }
    }) {
        @Override
        protected Map<String, String> getParams() throws AuthFailureError {


            Map<String, String> params = new HashMap<String, String>();

            params.put("url", textUrl);

            params.put("ortam", ortam);

            params.put("resim", image);

            return params;


        }
    };

    requestQueue.add(request);

}
```

Function 6: Commands that listens the Thesis Application Head

```
imagbtn_ihbar_devam.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            if (bubbleView == null) {
                addNewBubble();
            }
            moveTaskToBack(true);
            onPause();
        }
    });


    imagbtn1.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            Toast.makeText(getApplicationContext(), "Tanıtım Sayfasını Açıp Kapatacak",
Toast.LENGTH_SHORT).show();
        }
    });


    imagbtn2.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            if (bubbleView == null) {
```

```
                addNewBubble();

            } else {

                Toast.makeText(getApplicationContext(), "Sol Üst Köşede İhbar Baloncuğu
Var", Toast.LENGTH_SHORT).show();

            }

        }

    });
```

Function 7: Command that listens the changes in the clipboard

```
initializeBubblesManager();




    clipboardManager = (ClipboardManager)
getSystemService(CLIPBOARD_SERVICE);

    clipboardManager.setText("");



    clipboardManager.addPrimaryClipChangedListener(new
ClipboardManager.OnPrimaryClipChangedListener() {

        @Override

        public void onPrimaryClipChanged() {

            cliptest = true;



        }

    });

  }
```

Function 8: Function that creates the virtual screen

```
@Override
    protected void onActivityResult(int requestCode, int resultCode, Intent data) {
        if (requestCode == REQUEST_CODE) {
            sMediaProjection = mProjectionManager.getMediaProjection(resultCode, data);
            try {
                Thread.sleep(1000);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
            if (sMediaProjection != null) {
                File externalFilesDir = getExternalFilesDir(null);
                if (externalFilesDir != null) {
                    STORE_DIRECTORY = Environment.getExternalStorageDirectory() + "/" +
Environment.DIRECTORY_DCIM + "/";
                    File storeDirectory = new File(STORE_DIRECTORY);
                    if (!storeDirectory.exists()) {
                        boolean success = storeDirectory.mkdirs();
                        if (!success) {
                            Log.e(TAG, "failed to create file storage directory.");
                            return;
                        }
                    }
                } else {
                    Log.e(TAG, "failed to create file storage directory, getExternalFilesDir is
null.");
                    return;
```

```
            }

            DisplayMetrics metrics = getResources().getDisplayMetrics();
            mDensity = metrics.densityDpi;
            mDisplay = getWindowManager().getDefaultDisplay();

            createVirtualDisplay();

            sMediaProjection.registerCallback(new MediaProjectionStopCallback(),
mHandler);

        }
    }
}
```

Function 9: Function that launches the virtual screen

```
private void startProjection() {

    startActivityForResult(mProjectionManager.createScreenCaptureIntent(),
REQUEST_CODE);
    bubblesManager.removeBubble(bubbleView);

}

private void stopProjection() {
    mHandler.post(new Runnable() {
```

```
        @Override
        public void run() {
            if (sMediaProjection != null) {
                sMediaProjection.stop();
            }
        }
    });
}

private void createVirtualDisplay() {
    // get width and height
    Point size = new Point();
    mDisplay.getSize(size);
    mWidth = size.x;
    mHeight = size.y;

    mImageReader = ImageReader.newInstance(mWidth, mHeight,
PixelFormat.RGBA_8888, 2);
    mVirtualDisplay = sMediaProjection.createVirtualDisplay(SCREENCAP_NAME,
mWidth, mHeight, mDensity, VIRTUAL_DISPLAY_FLAGS,
mImageReader.getSurface(), null, mHandler);
    mImageReader.setOnImageAvailableListener(new ImageAvailableListener(),
mHandler);

}
```