Chapter 67

Digital Evidence in Crime:
A Case Study on Text Shared in Social Media

Ersin Caglar
https://orcid.org/0000-0002-2175-5141
European University of Lefke, Turkey

Deniz Ersalıcı
European University of Lefke, Turkey

Luca Rivaldo Tonini
https://orcid.org/0000-0002-4333-281X
European University of Lefke, Turkey

ABSTRACT

This research was conducted to analyze the risk factors of online violent video games, relationship between these games and social media in terms of conducting crime, and techniques that might be used to prevent crime on social media text. The technique was tested with texts shared on Facebook posts. There are also some keywords used in most popular online violent video games. A sentence analyzer tool was developed in this research to test sentences taken from Facebook. The findings of the analysis were shared, and also the eligibility of the technique in term of preventing crime on social media was discussed.

1. INTRODUCTION

The Internet is at once a worldwide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers regardless of geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Beginning with the early research in packet switching, the government, industry, and academia have been partners in evolving and deploying this exciting new technology (Leaner et. al., 2009). With the development of the Internet, new terms like World Wide Web (WWW) and Uniform Resource Locator (URL) entered our life. World Wide Web (WWW) is a virtual environment that connects information with connections.

DOI: 10.4018/978-1-6684-7366-5.ch067

The development of the Internet also creates new opportunities for users like web pages that contain information they want, personal assistants giving every answer to them in a few seconds, and also Internet communities which mean social media and chat and instant messaging (Goodwill Community Foundation, 2013).

According to another research (Allam et. al., 2014), the Internet creates new envy- ornament for users different from the real world they are living in. This digital space gives opportunity to users to create their identity on the Internet. Popularity and population are increasing every day, and from 2000 to 2012, its population increased by 566.4%, and the average age of active user population is between the ages of 18-34. The use of the internet has both positive and negative impacts on users. Accessing library collections and books online, communicating with other users, business transactions, and conducting research become easier for users. They can find the information that they want with one click without spending hours, or they can communicate with their relatives in a digital environment easily. These are some of the positive effects of the internet on users. However, it has some serious effects on users as well. Excessive use of the Internet can cause Internet addiction, which is the problem when there is too much relationship between user and machine, and it can cause serious problems in the normal life of users. Internet addiction can cause psychological, emotional, physical, and social problems. Also, it can diminish the effectiveness of the work of users. Based on these problems, social media is the major application to make these kinds of effects.

Social media is the general name given to interaction can- treed media-sharing platforms (Manning, 2014). These new types of platforms have 2 bases. While one-way communication Chan- news, which is the first base of the development of social media, helps to share media with the use of tools such as television and radio, the second base of development of social media started with the improvement of interactivity. Nowadays, one person can see updates on others' life from one platform, send messages, communicate, and interact with their posts. This new media age makes people reach media types and information they want as many sources as possible. In the past, the only source for information was the ones around, but now, there are millions of sources with one click through an internet connection and technological device.

Another definition of social media is that it is a platform that is not about technology but sociology (Cheol 2012). According to this view, it is the place that gives people the opportunity to create their community. This community can include family only or a much wider community that creates an environment for users from all around the world. It is an independent area that allows its users to communicate with people with the same interests, habits, common interests, political actions, beliefs, profession, and location even if they don't know each other from the real world. Users can present their ideas with their networks while they can also see others' ideas, interact, communicate, and be connected with them. Social media makes the development of social networks as quick as it can be, and today, users can easily find new people and add them as a friend with one click.

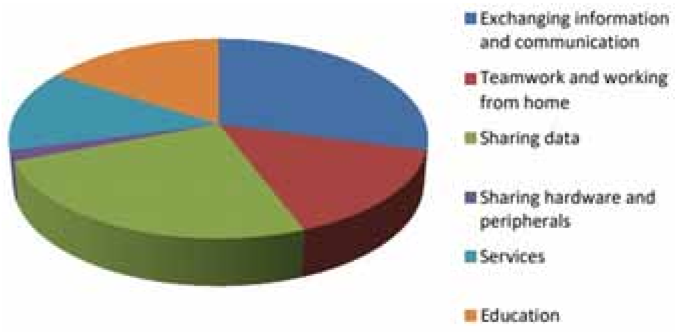
Common forms of social media are email, Facebook, Insta- gram, Messenger, and WhatsApp. Email is the most common among them and the availability of free platforms makes it more reachable. Another common form of media on social media is text. Instant messages and texts as posts are the most common forms shared on social media. Established in 2004, Facebook has the first place with 1,871 million users. Facebook Messenger and WhatsApp, established in 2009 with 1,000 million users come second. Also, Instagram, established in 2010, is the fifth with 600 million users (Wail, 2017).

The use of social media rated for adults is increasing fast. Ac- cording to the report of Suraj Sharma, the use of social networking was 7% from 2005 to 2015 and 65% of adults used social media sites frequently. Also, the report pointed out that, there is relation between social media use and age. The age group of 18-29 is using social networking sites most and nowadays, 90% of young adults are social media sites where the rate was 12% in 2005 (Sharma, 2016). Also, Bhola and Mamaku identified that the most commonly used social media site is Facebook for chatting, finding new friends, interacting with ones from the opposite sex, and people spend 3.6 hours of the day there (Bhola and Mamaku, 2014).

The growth of social media also brings negative things like crime. It is dangerous in terms of crime because everything about crime becomes easy in the world of social media. Criminals can find their victims easier than in the real world. They don't need to be in the same environment. Only having an internet connection, a technological device like a cellphone, tablet, laptop, or Personal Computer (PC), and having a connection from that kind of platform is enough to commit the crime. In that situation, it is easy to be persuaded by others, and it is not easy to stop crime on social media. This is the critical point we will research it.

A survey was done to analyze the advantages and disadvantages of the use of social media in the European Union (Datoog and Balco, 2017). Facebook with 89,20%, Instagram with 48,60%, and Google+ with 56,80% are the top 3 most popular social media platforms among the social media users when the survey was conducted. They use social media platforms mostly to contact their friends (83,30%), obtain information (80,60%), sell products (27,80%), online marketing (25%), monitor messages (22,20%), make new friends (16,70%) and other purposes (2,80%). Figure 1 below shows the advantages and Figure 2 below shows the disadvantages of the use of social media platforms.

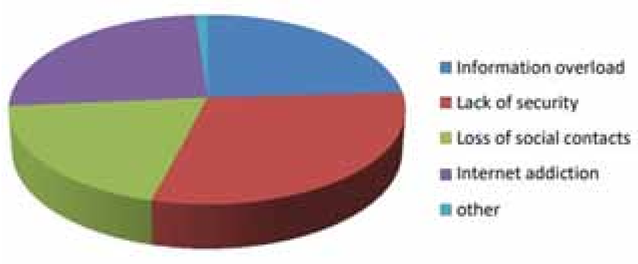
Figure 1. Advantages of Use of Social Media



As can be seen from Figure 1, the most import- tant advantage of the use of social media platforms is about exchanging information and communication with a percentage of 97.2. However, as was drawn in Figure 2, the most important disadvantage of the use of social media is the lack of security with a percentage of 72.2.

The development of society and mostly technology also caused ways of crimes to be applied. With the development of technology, a new type of crime which is "cybercrime" has emerged, which is the criminal activity committed by using computers and networks. It can be categorized as computer crime which intends to reach and destroy information stored inside the computer and network crime which is using devices with internet connection to reach users' information. They try to reach meaningful information about users to utilize (Krishnan, 2019). Social network sites are one of the most important tools to commit cybercrime. The efforts to conduct attacks are increasing every day because of the increase

Figure 2. Disadvantages of Use of Social Media



in the population of them. Criminals have different motivations to use social networking sites. These can be categorized as size, uncountable available data, difficulties in the identification of criminals, and dynamic nature. The size of social networking sites had a huge increase because of the information age (Burcher and Whelan, 2018). They continue to increase their capacity every day with higher rates and this makes criminal's life easier than before. Criminals can commit crimes and find as many as users they can find to commit crimes (Das and Patra, 2020).

While social media provides personal freedom, it also poses dangers to people in terms of both safety and health. While social media offers its users immense freedom, it also provides endless possibilities for crime. These possibilities are of such a size that they create life-threatening danger. One of the most important examples of this is the Blue Whale game developed by Russia. The blue whale game specifically orders people to commit suicide after 50 missions that find their victims on social media.

At this point, social media allows malicious people to access their victims. He states that around 130 child suicides were recorded between November 2015 and April 2016, and a significant portion of them may have "The Blue Whale" underneath. e It is possible to define "The Blue WhaleChallange" as an "interactive" platform that communicates with its "target" (victim) in such a way that it breaks down the virtual-realistic wall with other online-based communication applications (Whatsapp, Instagram, Facebook, etc.)(Candan, 2018).

2. LITERATURE REVIEW

Social media can be considered an interactive and internet-based Web 2.0 tool. It is also to be known as a social network or social tool. It is a web-based tool that makes interaction possible and easy between active users. However, this internet-based tool makes crime also become easier to conduct, and creates some new ways of crime which are named "cyber-crime." This section will give information about the development of social media and cybercrime and their associated relationship.

2.1 Development of Social Media

Social media is a new type of media that lets people interact with each other by using network conditions. Devil- open Social Media has 2 stages. The first stage is broadcast and the second one is interaction (Manning, 2014). In the first stage, there is only one-way communication. The most important examples of the broadcasting stage are radio, television, and newspaper. In that type of media transmission, information is only transferred from owner to user. There is no interaction between the user and the owner. The interaction between them is so rare and limited. After the development of digital and mobile technologies, every individual has a chance to have interaction with each other. The main part of this new type of media is interactivity. Many people can talk as a group or community. Social media sites like Facebook are now part of users', most of the young generation, everyday life (Chowdhury and Asha, 2015). Almost all social media sites are mostly being used for connecting users with their connections, developing new friendships and meeting with other people that they don't know, creating online areas to meet up, and having a chance to share or make comments. In addition to those opportunities, it also gives chance to its users to view the content their friends share, create profiles to represent themselves to the online world and make it easy to communicate with others. Usability and the opportunity to reach information have become as easy as possible (Manjunath, 2013).

Users of social media sites create public, semi-public, or private profiles for themselves and they create friend lists. Users can see posts of their friends and also, and they can remove or add new friends, organize what they want to see or block the ones that they don't want to see. Hence, the younger generation uses such sites mostly for chatting, sharing various media with their friends, and communicating with other friends. Social media sites allow them to increase interaction with others. With that much use of these sites, social media affects its young users in both positive and negative ways (Chowdhury and Asha, 2015). On the other hand, according to the same research, there are 5 main negative effects of social media on the young generation.

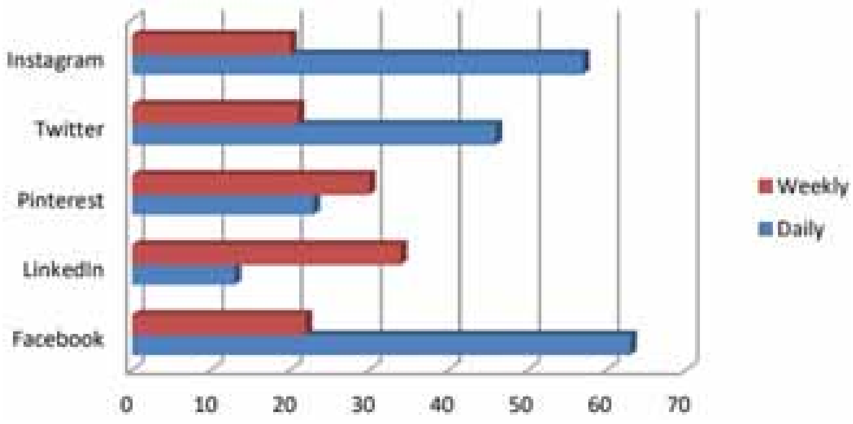
These are:

- **Waste of time:** Most youngsters are checking their social media to see new posts, or controlling their messages to see new ones every minute. Because their minds are always on their social media accounts, they couldn't do anything all day.
- **Decrease in success:** As it was said in the first reason, their mind is always on their social media, and because of that, they don't want to study or work, and those reasons decrease their academic or career success.
- **Decrease in real communication:** Social media makes people forget traditional communication ways like letters, face-to-face meetings, etc. People generally spend their all day chatting with others or using social media. However, in this situation, they couldn't find time to spend on real relationships.
- **Self-centered new generation:** People become self-centered and teenagers use social media mostly for "stalking- in", and searching and learning new information about their friends or non-friends.
- **Increase in crime:** All information, unfortunately, doesn't correct in the online world. They might give missing- formation, and sometimes, they are doing cybercrime easily because they don't know the user at the end of the communication line, or others don't know their real identity. They don't afraid to do mental or sexual crimes in the online world.

According to the research, there are 4 categories of Infor- motion shared on social media platforms. These are "User", "Activity", "Network" and "Content". The data type of User generally gives personal information like name, birthday, e-mail, country, and city about the owner of the profile. Content is the information about what they are sharing on their accounts. Those published materials can be posts, tweets, likes, images, and videos. They give information about the everyday life of a person and allow interaction between people. Also, the posts they shared on their social media account can give information about their Internet Protocol (IP) address or carrier network. Network data type provides information about the connections of, names of them, and contact information of those people. It gives information about personal identity and characteristics on their social media account. Lastly, the Activity type of data gives information about which events people are attending, or where they are going at what times from the posts they published in their profiles or respond to event posts. Data shared on social media accounts give information about the user's everyday life, what they like to do or don't like, characteristics, marital status, and their background and financial status (Arshad, et. al., 2019).

There are varieties of social media platforms for different kinds of data sharing. Some of them are used to share text. On the other hand, some of them are suitable to share photos or videos, or some platforms for different kinds of data. According to Raid, Google+, Facebook, LinkedIn, Pinterest, Myspace, Twitter and YouTube are the most popular ones on all platforms. In theory, the idea behind all of them is increasing interaction. The way of doing it can be changeable. However, by using any of those social media platforms, they can comment or leave messages to each other (Romansky 2014). As can be seen in Figure 3, which is showing the use of Facebook, LinkedIn, Pinterest, and Instagram by adults, Facebook, a platform mainly used for sharing different kinds of media, like text, photos, video, etc., and giving different kinds of opportunities to communicate, is the most popular social media platform between them. The results determined that it was used by 67% in 2012 and 71% in 2013 of the overall adult social media users. It is prepared to be used by users from different demographic groups. LinkedIn, mostly used for commercial purposes, is in the second phase among adults with 20% in 2012 and 22% in 2013, and it mostly connects users from the same company, school, or similar job description workers from different companies. Twitter and Pinterest nearly have the same results. While Twitter was used by 16% of overall users, Pinterest was used by 15% in 2012. On the other hand, Twitter was used by 18% of users, and Pinterest was used by 12% in 2013. Pinterest is used by mostly female adults while Twitter is used by young adults. Lastly, Instagram was preferred to be used by 13% in 2012, and 17% in 2013. It is preferred by young adults who are living mostly in city centers (Duggan and Smith, 2013).

Figure 3. Usage frequency of social media



2.2 Development of Cybercrime

There is another important concept which is cybercrime for this article. According to the research, (Jharkhand et. al., 2014) which was done in 2014 cybercrime is any criminal activity that is committed by using a computer and network in a digital environment, and it is any illegal activity that resulted in a pecuniary loss or any other harmful result. It can have the purpose to be harmful to an individual or the properties of an individual. Within the digital world, criminals have different opportunities to commit crimes. These opportunities were named "keys for transformation", and 4 keys are as they were listed below:

- **"Globalization":** The opportunity to reach everywhere in the world.
- **"Disturbed Network":** One of the opportunities to cause victimization easily.
- "**Synoptics and Panopticons":** Allows the criminals to follow their victims remotely.
- **"Data Trails":** Creating new ways to steal identity without facing any difficulty.

Cybercrime makes traditional crime easier than before. The type of crime which exists in the real world like chipping, stalking, etc. becomes easy in the digital world. Criminals can easily follow or contact their victims. Also, new ways of crime entered our life like hacking, online gender trade, or hate speech. The definition of cybercrime cannot be made properly for a long time, which causes various bad effects on both individuals and businesses. Another study was conducted to analyze the effects of cybercrime on the economy and found that cybercrime has damaged both individuals and businesses. Businesses spend too much money to make their IT Services too strong to be protected from cybercriminals. The amount they spent increased by 12.4% from the previous year and became $114 billion, and in 2019, it increased by 8.7% from 2018 and became $124 billion. When it was looked at the increase from 2015 to nearly $3 trillion, it will be predicted to be $6 trillion spent until 2021 (Krishnan, 2019).

The study which was conducted to analyze crime in the digital environment identified that the increase in the Internet of Things caused an increase in the complex problems in the digital world (Allam et. al., 2020). By 2020, the number of devices with network connections increased 50 billion and there are countless numbers of data shared. This popularity of the Internet of Things brings also negative things to everyday life, and the 3 most important categories appear mainly according to the authors. These are:

- **Cloud forensics level:** It is the attack on the information stored in the cloud. People, nowadays, prefer to store their information in storage that does not physically appear in the real world but is somewhere in the network which is called the cloud. They prefer to use this because of the opportunities it gives to the users. It gives some free storage areas to its users, but when they use all of them, they can easily increase their area by paying some amount which is generally not too much. It is easier than doing it from computer storage. Along with this, cloud computing gives lots of other opportunities to its users like accessibility, capacity, convenience, etc. However, it also allows criminals to reach users' information and commit crimes easily.
- **Network Forensics Level:** There are different kinds of networks; WAN, BAN, HAN, PAN, and LAN, and also, there are different kinds of attacks on the network for every type of network (Allam et. al., 2020). According to another research, network forensics are using data from activities on the internet and web browser to find meaningful information to commit a crime. The

increase in the number of users on the internet causes an increase in network forensics. Email forensics, and web browser forensics are some important and common ways of network forensics (Meghan et. al., 2010).

- **Device Forensics Level:** It is the type of crime that tries to attack the hardware of the computer. The data that will be used for crime is collected from the storage of a computer. The information collected from the device can be important, and it needs to be analyzed by device forensics (Allam et. al., 2020).

2.3 Relationship Between Social Media and Cybercrime

Social media changed the way to share opinions and content. It makes it easier than the traditional way of media sharing. It not only gives chances to its users share their opinions easily, but also, they can reach more people than the traditional way of communication. With one post, they can reach a large proportion of people. However, this large proportion of people can bring some risks to crime. Crime also becomes easy to be committed on social media (Curiel et. al, 2020).

Social media changed the way to share opinions and content. It makes it easier than the traditional way of media sharing. It not only gives a chance to its users share their opinions easily but also, can reach more people than the traditional way of communication. They can reach a large proportion of people only with one post. However, this large proportion of people can bring some risks to crime. Crime also becomes easy to be committed on social media (Curiel et. al, 2020).

Social media is increasing its popularity every day, and the age group of its population is between the ages of 18-25 ages. It makes communication among its users easier and quicker, and also it allows its users to connect with other people without any geographic limitations. They can see the ideas and comments of other people easily. Since everyone with a social media account can create content from their profile and share it with their group, the rate of sharing fake news has increased. Everyone on social media tries to share updated news firstly to increase their awareness by other users. Although it increases the chance of communication, there is a negative effect which is “hate speech”. Since every user has the chance to reach news from different content and can share their idea with others without any restriction, it is not a surprise to see hate speeches towards others on social media, and it has a direct effect on the real-life of users. Social media, unfortunately, makes hate speech toward others easier than to do it in the traditional way of communication (Curiel et. al, 2020).

There are various ways to commit crime in the digital world. The research by Dolly and Smriti (Shaw et. al., 2016) identified gen- earl ways of committing a crime on social media between 2012-2013. The most popular social media attack was “fake offering”. Then, it was followed by “manual sharing”, “like junking”, “fake plug-ins” and “fake apps”. They also categorized the most common crime types for the most popular social media platforms which are Facebook, Twitter, and Myspace. According to the results of the analysis, there are 4 common crime ways for Facebook. These are video attacks which are the way of crimes that is trying to steal the login information of users by giving fake URL addresses to the clickable link of the video and when users click, it asks to them log in again to steal information. The second way of Facebook attack is like junking. It is again an attack with the links, but this time it is not essential to be done by video. If the user clicks the post to see what is inside, they will face a blank page that contains a button to click with the “click here to continue”. If they would click on that, criminals can reach their profile and share it from their profile to find more victims. The third way of Facebook attack is the combination of email and Facebook. Users receive an email with an attractive heading and a Facebook link that is fake. If they click on that and login to their account from there to continue, their profile will be stolen. The last type is “worm-based viruses”. It is done by applications that send users attractive and intriguing messages like “click here to see who viewed your profile” message, and if they download this application, virus files will also be downloaded to their device. Also, that kind of application asks users to log in from there and they learn their login information in that way.

After completing some possible attacks on Facebook, the next is related to the criminal attacks on Myspace. The first type of Myspace attack is the “Kobach Attack”. It is a type of attack done by codes. It is generally embedded in the link to attractive videos. When users click to open the links, the program asks users to download or update the flash player of the browser, and when they click on the okay button, it downloads the “codesetup.exe” file and ID stealers near with flash player to the device and steals information on the device. The second type of Myspace attack is “image attack” where criminals create a transparent image and embed it on the front page of Myspace. When users click on that image without knowing and log in to their account via this transparent image embedded in the page, criminals can learn the email and password of users, and use it anywhere they want.

The last part of that table contains attacks on Twitter. There are 3 types of attacks shown in the table. The first one is a “Denial of Service Attack”. This attack type is using the fast-spreading feature to share files with a virus with as many as people it can be shared in a short time. The second type is “worm infects”. It is an attack done in 2 ways at the same time. An example of this type of virus was seen in 2009, and the attacker was sharing the personal information of users. At the same time, he/she also steals personal information to find another victim. This increased the speed of the virus 4 times from normal. The last type is “phishing” for the virus types of Twitter. Phishing also directs users to a fake login page to steal information.

Another research was conducted to analyze the type of crime on Facebook (Ganesan and Mayilvahanan, 2017). It identified 7 common ways to commit crimes there. The first one is scams. They try to attack people by using the most attractive links or websites. Criminals also try to confuse users’ minds with gift cards or astrology news. After they catch their victims, they try to learn credit cards and other information about victims that can be used to be harmful, especially economically. The second type of common criminal activity on Facebook is cyberbullying. It is mostly common among young generations. It can be resulted in committing suicide or killing a friend. When these kinds of online behaviors or crimes are performed by adults, they can be named cyber-harassment or cyberstalking. The next type of crime on Facebook is stalking. It is a common and serious crime way for all social media. Cyberstalking contains harassing messages, threats online, and other security attacks for people. It is the action that should be treated to not cause too important danger for both criminals and victims. Robbery is the fourth type of crime way on Facebook. From the information users distribute on their accounts, the thief faced no difficulty identifying users’ physical addresses, views, education, job, and the time they come and leave their homes. Knowing all those information makes the thief’s job easier. The fifth type is identity theft. In this type of crime, criminals try to copy all the personal information like photos, names, and surnames and make fake money by harming their email. Then, they perform illegal activities with users’ identities, have an impact on financial aspects, and also cause security problems for users in real life because they can do illegal things also on digital with the name of victims. Defamation is the sixth type of crime on Facebook. Criminals try to trick third parties by lying and making fake announcements from victims’ social media accounts or even making bad saying to someone with the victims’ identity. The last type of crime on Facebook is harassment. It is very common for Facebook. Criminals prefer to sexually harass not only adults but also young people, adolescents, or individuals of college age.

Social media sites are the most commonly and widely used tool in networks. Most social media sites' popularity is formed by the age interval of 20-27, and the most popularly used social media site is Facebook, and its population is increasing day by day (Irshad and Soomro, 2018). According to the research (Waldman, 2016), the number of daily users of Facebook is 1.09 billion, and number of monthly active users is 1.65 billion. Users give the most important personal information like gender, email, name, surname, birthday, phone number, photo, hobbies, etc. about them on Facebook to create their profile (Waldman, 2016) making criminals choose Facebook to commit crimes mostly. Although new prevention techniques were applied to prevent crime on Facebook, there were too many problems with it. There are many problems with customers and their privacy. The cases that show the link between Facebook and crime were identified. It was really hard to delete accounts of users from Facebook and this made it to be seen as an unethical or disgraceful book and bullying by people. There are too many identified cases that are dangerous, especially for young people. Another important danger is for businesses. It can be critical in terms of crime for both individual accounts and business accounts because it is used by both groups widely (Milivoje Vic, 2011). Because of its popularity, criminals changed their ways of committing crimes and changed their direction directly to the huge data pool which is Facebook. Every activity on social media can cause one to be chosen as a victim by the criminal. People think that Facebook is the most trustable area of social media because they think they know their friends on social media (Irshad and Soomro, 2018). However, according to the survey on identifying criminal actions on social media, the users were asked a variety of questions about their social media. As a result of that survey, users who believe that social media hurts social media mostly, share personal information from their social media accounts, and nearly half of the responders (40%) are accepting friends that they are not known from the real world on their social media account (Hamas et. al., 2018). The most widely applied crime type on Facebook is stealing identity. Since they share every bit of information about themselves, it is easy for criminals to reach all information and use it in different places. They are mostly using Scam website techniques to reach information of users from Facebook accounts. They are directing users to those fake sites by sending URLs from private messages (Irshad and Soomro, 2018).

Another popular social media application used for crime is Twitter. It is another big source of cyber-attacks (Irshad and Soomro, 2018). According to the results of research in the UK, there are at least 350,000 accounts that are not representing the real identity of users, which means they are created most probably for criminal purposes, and they will be used for criminal purposes most probably. There are nearly 319 million Twitter accounts that continue to be actively used, and 48 million of those profiles are fake (Irshad and Soomro, 2018). Those numbers can give information about the higher risk at those platforms.

The impact of social media on our lives has both positive and negative aspects. A positive of social networking sites like Instagram, Snapchat, Facebook, and Twitter is that they allow people who live far apart to stay in touch with loved ones they've left behind via audio and video chats, chat rooms, and a variety of other features. By just using their mobile devices, the general public can now stay up to speed with current events throughout the world. Social networking sites make it easier for people who are looking for work or any other purpose (educational purpose) to do so. Sharing your thoughts and ideas with the world is also the quickest and most convenient way. Social media makes people's lives more convenient and pleasurable (Kainya, 2022).

Another and one of the most dangerous versions of digital criminal activities is the Blue Whale Challenge game. According to research, the Blue Whale game is a digital game developed by Russia that poses a danger to children worldwide, especially for children. The game consists of 50 levels, the steps become increasingly difficult and reach life-threatening dimensions, eventually resulting in the suicide of people. The levels of the game pose a serious risk both for people's own life and for the people around them. A large part of the tasks of this game, which ensnares its victims through social media applications, is in the form of social media sharing (Candan, 2018).

3. PROPOSED MODEL

The research was constructed by using a sentence analyzer tool that was developed using Python Language. Python language is a programming language that is interactive, interpreted, and object-oriented. It is the language working with English keywords (Das and Patra, 2020). The tool is using Artificial Intelligence also to make it develop itself after every analysis that it finds new keywords not added to the document. Facebook posts were used to analyze posted crime on social media. The program analyzed the sentence in terms of containing criminal words, and it analyzed and found the percentage of the crime rate in the sentences analyzed. The program is suitable to be used for all social media platforms to check all text posts published there to identify criminal sentences right after they were published. Facebook was chosen because it is the most popular social media platform according to the aforementioned research, and also it is the most popular platform to be used for criminal purposes.

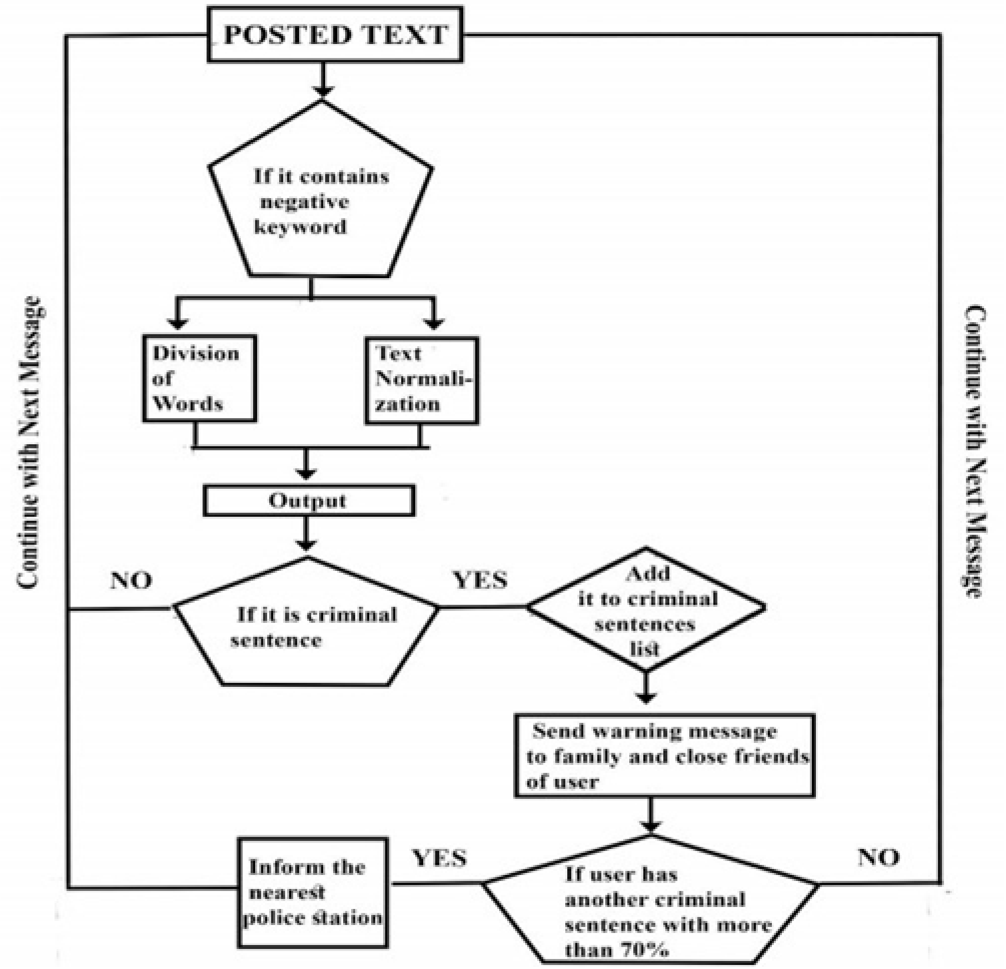
There are different techniques to analyze crime conducted on social media. Some of the researchers are using the survey method to analyze the psychology of committing the crime on social media after it was committed. However, this only helps to understand the psychology and way of cybercrime. It is not the way to prevent cybercrime because it is conducted after the crime is committed. Another research conducted to analyze crime on social media analyzed the most successful programs developed to identify crime on social media (Baca et. al, 2013). The authors analyzed Cashback, Internet Evidence Finder, and EnCase Forensic. Cashback is used for analyzing chats on Facebook. Internet Evidence Finder is another application used to analyze crime on Twitter, Myspace, or Google +. EnCase is the last application used for analyzing crime on Internet browsers using cache or cookies. They are identifying posted crimes on different platforms. However, none of them is suitable to be used on different platforms at the same time. This is the critical point of needing new tools to be used in different platforms to test posted text whether it is criminal or not. For this purpose, a sentence analyzer tool was developed to test text in terms of crime on social media. It is also be used to prevent crime on social media because it can analyze and identify criminal sentences right after it was published on social media platforms. It can also suitable to be used in different popular social media platforms. The sentence analyzer tool can identify the criminal word in a sentence on social media with the percentage of crime rate on sentence. Furthermore, it can be used in coordinating with government services and if it is needed, police can take place and intervene in the situation.

This research was performed by analyzing the sentences published on Facebook. Analyses were conducted by making sentences suitable for the analysis. The posted texts which are criminal and non-criminal on Facebook were acquired without including the identification information of the user. They were divided into parts to make keywords clear to be analyzed. 50 messages were chosen randomly from Facebook.

All 40 sample messages can be seen in the appendix, the program was designed to continue analyzing until all sentences on the "message.txt" file are finished. The results of the analysis will be categorized as the ones including crime with the percentage of crime rate in the sentence and the ones not including. If the sentence that was analyzed does not include any crimes, the program will continue with the next sentence. However, if the sentence is a criminal sentence, then it will save the message posted with details to the sheet that was created to save possible people at risk. Then, it will send an automatic warning message to the parents and close friends of a user. If the same person posts another criminal sentence with more than 70% percent, the nearest police station will be informed about the situation. Then, it will continue to analyze the next sentences

We designed the sentence analyzer tool to make criminal keywords being able to identify criminal keywords in text posted on social media. The program has mainly 5 files; bad nouns, bad verbs, normal nouns, normal words, and messages. The message file is the place with the posted text in it. Bad nouns and Bad verbs files contain criminal nouns and verbs. Lastly, normal nouns and normal verbs files contain normal verbs and nouns that have some examples to be used in criminal sentences also. Figure 4 above shows the analysis process. The sentences analysis tool obtained the posted text from the sentence file. Then, it will be prepared to be understood by a program by dividing it into words. After preparing it for the analysis, sentences will be analyzed by looking at the words it contains. Every word and its mean-

Figure 4. Structure of Sentence Analyzer Tool


POSTED TEXT
If it contains negative keyword
Division of Words
Text Normalization
Output
If it is criminal sentence
NO
YES
Add it to criminal sentences list
Send warning message to family and close friends of user
If user has another criminal sentence with more than 70%
YES
NO
Inform the nearest police station
Continue with Next Message
Continue with Next Message

ing in the sentence will be checked. If the meaning of the sentence is negative, it will be showing the "This sentence is negative!" message with the word used negatively and the percentage of crime rate in a sentence. The program is also able to identify the crime rate of a sentence by looking at the number of words the sentence contains. For example, the "I will kill you" sentence including1 a negative word, so the crime rate of the sentence is 25%. After completing the analysis of the first sentence, the analysis started with the next message. After completing the analysis of sentences, the ones with the risk according to the results of analyses will be saved to the sheet, and parents and close friends are informed about this if it is the first time publishing a criminal sentence. If the same person shares more than one criminal sentence with more than a 70% crime rate, then the nearest police officer will be informed about the situation to prevent crime. While doing those analyses, if the program found a word that was used with criminal words and the percentage of the sentence is high, the unknown word was also added to the list.

By developing the "Sentence Analyzer Tool", criminal activities, especially those that aim at human life and are carried out through social media, could be identified on time and prevented. Thanks to the structure of the program, the program can develop itself and even if the words are not registered in the system, thanks to AI, it can understand the sentence structures and integrate the dangerous words into its system and identify it.

4. RESULTS

Considering that words can be used with different meanings or for joke purposes, it defines sentences above a certain percentage as risky sentences by looking at the ratio of the words in the sentences, not reaching a conclusion from a single word. This feature is a very important development, especially for the Blue Whale game developed by Russia. Since the patterns of the sentences to be used are clearly defined, victims can be found before the 50-step instructions of this game, in which targets, especially young children, are reached, and people's lives can be saved before the conclusion of suicide is reached.

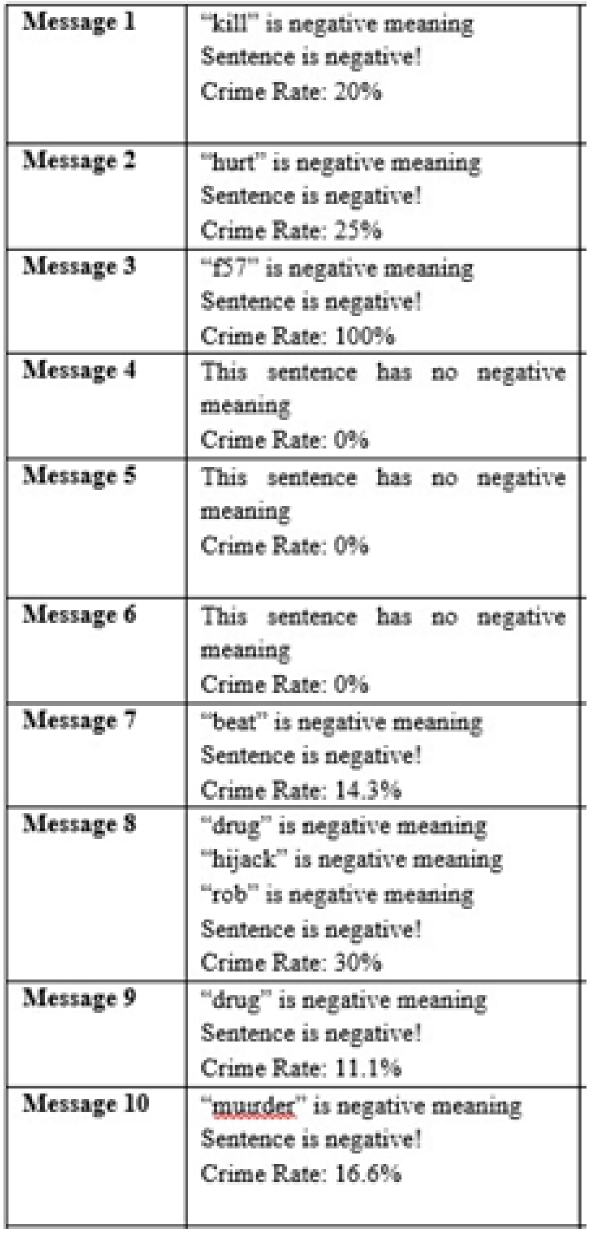
The program analyzed 40 sample sentences to identify whether they are criminal sentences. These sentences were chosen to understand the effectiveness of the program. Some of them were chosen as criminal sentences, but some of them were normal and non-criminal sentences to understand whether the program was understood and identify the crime in the sentences.

Analysis has 4 steps. Firstly, messages were normalized to clear emoji, punctuations, or symbols. After normalizing the text, it started to analyze each message in the message.txt file. The ones including negative keywords in it were marked as criminal sentences, and by looking at the number of criminal words in each sentence, the percentage of crime was also identified. The analysis was conducted with 40 sentences as listed in Table 1. 35 sentences of these 40 sentences were found as criminal sentences. The program worked until finishing all the messages in the list.

The ones without the criminal keyword have a message as "This sentence has no negative meaning". On the other hand, sentences that contain negative keywords in it and keywords that have a negative meaning in the sentence have been marked as "Sentence is negative".

The crime analysis of sentences was done, and 63% of analyzed sentences were found as criminal sentences, and 37% of the sentences were found as non-criminal sentences. This shows that the program can successfully identify the crime rate on sentences, and it can separate sentences as criminal and non-criminal. It potentially can be used for crime analysis of social media tools.

Table 1. Results of Sentence Analyzer Tool



Message 1	"kill" is negative meaning Sentence is negative! Crime Rate: 20%
Message 2	"hurt" is negative meaning Sentence is negative! Crime Rate: 25%
Message 3	"f57" is negative meaning Sentence is negative! Crime Rate: 100%
Message 4	This sentence has no negative meaning Crime Rate: 0%
Message 5	This sentence has no negative meaning Crime Rate: 0%
Message 6	This sentence has no negative meaning Crime Rate: 0%
Message 7	"beat" is negative meaning Sentence is negative! Crime Rate: 14.3%
Message 8	"drug" is negative meaning "hijack" is negative meaning "rob" is negative meaning Sentence is negative! Crime Rate: 30%
Message 9	"drug" is negative meaning Sentence is negative! Crime Rate: 11.1%
Message 10	"murder" is negative meaning Sentence is negative! Crime Rate: 16.6%

However, there is only one critical point about the sentence analyzer tool. Keywords can successfully be analyzed in terms of crime rate, and the percentage analysis of sentences was done successfully, but when the keywords in bad nouns and bad verbs are used positively like "This class will kill me", it cannot understand that this keyword was used positively. To do also this, it should be developed to analyze each word in a sentence with each other.

5. CONCLUSION

With the development of technology, 4 important concepts entered into life; the internet, social media, video game, and unfortunately cybercrime. The Internet made everything to be done in seconds without much effort from reservations, and shopping to communication and entertainment. When it comes to communication, the most important development is Social Media. Social media is the tool that allows its users to create their digital identity, and their friends list and communicate, share opinions and media with them, and react to the posts they published. Social media tools try to increase interaction and communication between their users. While creating their digital identity, users give any personal information about them like name, surname, school, address, email, or even phone number. They can also have a chance to share their current locations. They can share all of such information with people on their list, or even the ones they don't know and are not included in their profile. However, although all these things are done to increase interaction, be- tween users, there might be some malicious people who might try to use that information in criminal ways. The crime done in the internet environment is named cybercrime. Cybercrime is the commitment of crime in the internet environment. Cybercrime can aim to be harmful in financial, security, or psychological ways, and most of the victims of cybercrime are unfortunately children and adolescents. Another important risk factor for children and adolescents in a digital world is violent video games. These are the games that are mostly preferred to be played in online environments and these are the ones whose only objective is crime, fighting, war, and killing other users. There are some negative effects of those games, but psychological effects are one of the most important ones. They make their users harmful to themselves and other people around them, and aggression is one of the most common effects of them. This also affects their use of social media usage. Sine users have the intention to share everything they do on their social media accounts; they prefer to share their experiences about those games also on their accounts with their friends. Also, it affects the usage of social media, and they start to show problematic and harmful behaviors on their accounts. On the other hand, there are some criminal games used in coordinating with social media to make them more popular and find new possible users. All of those above can cause an increase in the criminal use of social media.

This research was conducted to develop a tool to analyze texts posted on Facebook in terms of criminal purposes. Facebook was chosen because it is the most popular social media platform, and also, as it was mentioned above, it is the most popular social media platform used for criminal purposes. The program, the crime analysis tool, was designed to get sentences from social media and divide them into words to make the sentence ready to be analyzed. Each word and its meaning in the sentence were analyzed and if the sentence contains criminal keywords, it is added to the possible people under risk table which can be shared with the nearest police station and psychology center. To test the effectiveness of the program, 50 sentences were chosen for analysis. Some of the sentences are used criminally and some of them are normal and non-criminal sentences. According to the results, it was found that 70 percent of 50 sentences were identified as criminal sentences with criminal words within. This shows that the program is eligible to analyze sentences successfully and decide whether it is a criminal sentence, and it is suitable to be used for crime analysis of social media platforms, but it should be developed to analyze keywords whether it is negative or not.

To conduct this research, the sentence analyzer tool was a devil- opted for. There are some other techniques, which were mentioned above, applied before to analyze crime on social media. All of the abovementioned techniques were applied after the crime was conducted. The first research conducted for this purpose by Alessandra Brainard (Brainard 2018), analyzed the text published after the crime was conducted to understand the psychology behind publishing those activities on social media and found that they are publishing these sentences to increase their popularity over there. The second technique used was to analyze the text published on social media with a special program after a crime was conducted and the criminal was caught. The last research analyzed the pre-developed programs Catch Back, Internet Evidence Finder, and EnCase. All of them are suitable to be used in different types of platforms. Sentence Analyzer Tool which was developed to conduct this research tries to combine all the features of different techniques. First of all, Sentence Analyzer Tool doesn't need any criminal activity to analyze sentences. It can analyze all text published on social media platforms. The second important feature of this is that it can be used on all social media platforms, unlike previous techniques. The main differences between them were shown in me below accordingly;

6. FUTURE WORK

The analysis of this research was conducted by using text shared on social media. They were analyzed in terms of including possible keywords. The results show that the program can successfully identify keywords in sentences and differentiate between negative and positive sentences. However, this is not enough to prevent crime on social media. Media, audio, and photo are other possible ways of publishing crime. As a future work of this research, the program can be developed to be able to identify criminal signals inside the published media on social media.

REFERENCES

Allam, H. F., Aleeza, A., Alas Safi, M. O., Ashdod, A. A., & Wills, G. B. (2020). Security, Cybercrime and Digital Forensics for IoT. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* (pp. 551–577). Springer. doi:10.1007/978-3-030-37468-6

Allam, S. S., Hashim, N. M. H. N., Ahmad, M., Well, C. A. C., Nor, S. M., & Omar, N. A. (2014). Negative and positive impact of internet addiction on young adults: Empirical study in Malaysia. *Intangible Capital*, *10*(3), 619–638. doi:10.3926/ic.452

Arshad, H., Jannat, A., & Osmolar, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126–138. doi:10.1016/j.diin.2019.02.001

Baca, M., Cusic, J., & Cusic, Z. (2013). Forensic analysis of social networks (case study). In *Proceedings of the ITI 2013, 35th International Conference on Information Technology Interfaces* (pp. 219 223). IEEE.

Bhola, R. M., & Mamaku, G. C. (2014, March). A qualitative analysis of social networking usage. *International Journal of Research & Development of Health*, *2*(1), 34–44.

Brainard, A. (2018). *A Content Analysis of Crimes Posted on Social Media Platforms*. Academic Press.

Burcher, M., & Whelan, C. (2018). Social network analysis as a tool for criminal intelligence: Understanding its potential from the perspectives of intelligence analysts. *Trends in Organized Crime*, *21*(3), 278–294. doi:10.100712117-017-9313-8

Candan, F., & Yılmaz, M. (2018). *Oyun Sanal İntihar Gerçek: "The Blue WhaleChallange/Mavi Balina*. Oyunu Üzerinden Kurulan İletişimin Neden Olduğu İntiharlar Üzerine Kuramsal Bir Değerlendirme.

Cheol, C. (Ed.). (2012). *Transformation in teaching: Social media strata- goes in higher education*. Informing Science Press.

Chowdhury, I. R., & Asha, B. (2015). Impact of Facebook as a social networking site (suns) on youth generations. a case study of Kolkata city. *International Journal of Humanities and Social Science Invention*, *4*(6), 28–42.

Curiel, R. P., Cresco, S., Munteanu, C. I., & Bishop, S. R. (2020). Crime and its fear in social media. *Palgrave Communications*, *6*(1), 1–12.

Das, A., & Patra, R. (2020). *A Textbook of IT Workshop on Python Programming*. Cengage.

Datooga, M., & Balco, P. (2017). The analysis of advantages and disadvantages of use of social media in European Union. *Procedia Computer Science*, *109*, 1005–1009. doi:10.1016/j.procs.2017.05.446

Duggan, M., & Smith, A. (2013). *Social media update 2013: 42% of online adults use multiple social networking sites, but Facebook remains the platform of choice*. Pew Internet & American Life Project.

Ganesan, M., & Mayilvahanan, P. (2017). Cybercrime Analysis in Social Media Using Data Mining technique s. *International Journal of Pure and Applied Mathematics*, *116*(22), 413–424.

Goodwill Community Foundation. (2013). *What is the Internet?* Author.

Hamas, S., Singh, A. & Pancake, N. (2018). *Study on Effect of Social Networking Sites on the Young World of Cyber Crime*. Academic Press.

Irshad, S., & Soomro, T. R. (2018). Identity Theft and Social Media. *International Journal of Computer Science and Network Security*, *18*(1), 43–55.

Jharkhand, H., Al-Namrata, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149–164). Singers.

Kainya, V. (2022). *How Social Media Influence Crimes*. Academic Press.

Krishnan, S. (2019). Role and Impact of Digital Forensics in Cyber Crime Investigations. *INROADS-An International Journal of Jaipur National University*, *8*(1-2), 64-75.

Leaner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... Wolff, S. (2009). A brief history of the Internet. *Computer Communication Review*, *39*(5), 22–31. doi:10.1145/1629607.1629613

Manjunath, S. (2013). The usage of social networking sites among the college students in India. *International Research Journal of Social Sciences*, *2*(5), 15–21.

Manning, J. (2014). Definition and classes of Social Media. Encyclopedia of social media and politics, 1158-1162.

Meghan, N., Allam, S. R., & Moore, L. A. (2010). *Tools and techniques for network forensics*. preprint arXiv:1004.0570.

Milivoje Vic, S. (2011). *Social networking sites and crime: Is Facebook more than just a place to procrastinate?* Academic Press.

Romansky, R. (2014). Social Media and Personal Data Protection. *International Journal on Information Technologies and Security*, *6*(4), 65–80.

Sharma, S. (2016). A study on social networking sites (SNSs) and adjustment of undergraduates. *International Journal of Management and Social Sciences*, *4*(1), 160–168.

Shaw, U., Das, D., & Mehdi, S. P. (2016). Social Network Forensics: Survey and Challenges. *International Journal of Computer Science and Information Security*, *14*(11), 310.

Wail, A. (2017). *The Social Media (Concept, Types, Uses, Positives).* Available at https://www.researchgate.net/publication/322128709

Waldman, A. E. (2016). Privacy, sharing, and trust: The Facebook study. *Case W. Res. L. Rev.*, *67*, 193.

APPENDIX

1. Carve with a razor “f57” on your hand, send a photo to the curator.
2. Wake up at 4.20 a.m. and watch psychedelic and scary videos that curator sends you.
3. Cut your arm with a razor along your veins, but not too deep, only 3 cuts, send a photo to the curator.
4. Draw a whale on a sheet of paper, send a photo to curator.
5. If you are ready to “become a whale”, carve “YES” on your leg. If not, cut yourself many times (punish yourself).
6. Task with a cipher.
7. Carve “f40” on your hand, send a photo to curator.
8. Type “#i_am_whale” in your VKontakte status.
9. You have to overcome your fear.
10. Wake up at 4:20 a.m. and go to a roof (the higher the better)
11. Carve a whale on your hand with a razor, send a photo to curator.
12. Watch psychedelic and horror videos all day.
13. Listen to music that “they” (curators) send you.
14. Cut your lip.
15. Poke your hand with a needle many times
16. Do something painful to yourself, make yourself sick.
17. Go to the highest roof you can find, stand on the edge for some time.
18. Go to a bridge, stand on the edge.
19. Climb up a crane or at least try to do it
20. The curator checks if you are trustworthy.
21. Have a talk “with a whale” (with another player like you or with a curator) in Skype.
22. Go to a roof and sit on the edge with your legs dangling.
23. Another task with a cipher.
24. Secret task.
25. Have a meeting with a “whale.”
26. The curator tells you the date of your death and you have to accept it.
27. Wake up at 4:20 a.m. and go to rails (visit any railroad that you can find).
28. Don’t talk to anyone all day.
29. Make a vow that “you’re a whale.”

30-49. Every day you wake up at 4:20am, watch horror videos, listen to music that “they” send you, make 1 cut on your body per day, talk “to a whale.”

50. Jump off a high building. Take your life.