DESIGN OF IDENTIFICATION PEDOPHILE ACCOUNT IN TWITTER PLATFORM BASED ON MACHINE LEARNING

THESIS

Written work as one of the requirements
to obtain a Masters degree from
Bandung Institute of Technology

By
ERICSON SIREGAR
NIM: 23219066
(Electrical Engineering Master Program)

BANDUNG INSTITUTE OF TECHNOLOGY
February 2021

ABSTRAK

PERANCANGAN MODEL IDENTIFIKASI AKUN PEDOFIL PADA *PLATFORM* TWITTER BERBASIS *MACHINE LEARNING*

Oleh
ERICSON SIREGAR
NIM: 23219066
(Program Studi Magister Teknik Elektro)

Kejahatan pedofil identik dengan percabulan anak dan pornografi *online*. Berdasarkan data yang dihimpun Direktorat Tindak Pidana Siber Bareskrim Polri, jumlah kejahatan pornografi *online* cenderung meningkat setiap tahunnya, pada tahun 2019 meningkat sebesar 33% yaitu 364 kasus dimana terdapat 79 anak yang menjadi korban perilaku menyimpang pedofil melalui media sosial. Menurut Dittipidsiber dalam laporan *National Center of missing exploited children* (NCMEC) sepanjang tahun 2019, menempatkan platform Twitter sebagai media sosial yang subur konten pornografi dengan jumlah akun pelaku pedofil sebanyak 3.105 akun. Akun Twitter bisa didapatkan dengan mudah sehingga memudahkan para pedofil untuk melakukan perilaku menyimpang. Pedofil dan korban tidak saling mengenal karena predator anak memiliki cara unik untuk mengelabui korban, misalnya dengan menggunakan identitas palsu, mengirimkan pesan ekspresif di *tweet*, mengaku sebagai guru korban atau mengaku sebagai dokter yang melakukan meneliti, berpura-pura mengetahui di dunia nyata, kemudian sang predator merayu (*online grooming*) korban dan meyakinkan korban untuk mau menuruti perintah sang predator, baik dengan mengirimkan foto maupun video yang berisi konten pornografi anak. Dalam penelitian ini, tujuan dari penelitian adalah merancang model yang dapat mengidentifikasi akun pedofil berdasarkan karakteristik platform twitter. Model ini dirancang agar dapat dengan cepat dan akurat mengidentifikasi akun pedofil. Ini dapat dilakukan dengan mengekstrak fitur berbasis akun dan konten. Kemudian model menggunakan fitur tersebut untuk melakukan pelatihan dengan membandingkan akurasi algoritma pembelajaran mesin. Dari hasil uji *confusion matrix*, penelitian ini mengklasifikasikan akun pedofil dan non-pedofil dengan hasil akurasi terbaik menggunakan algoritma *Random Forest* 97,79% sedangkan algoritma SVM 96,32%, *Decision Tree* 95,59%, KNN 91,18%, dan *Naïve Bayes* 94,85%.

Kata kunci: Kejahatan *Pedofil, Twitter*, identifikasi akun, *account based, content based, Machine learning*.

ABSTRACT

DESIGN OF IDENTIFICATION PEDOPHILE ACCOUNT IN TWITTER PLATFORM BASED ON MACHINE LEARNING

By
Ericson Siregar
NIM: 23219066
(Magister's Program in Electrical Engineering)

Paedophile crime is synonymous with child fornication and online pornography. Based on data compiled by the Directorate of Cyber Crime, Bareskrim Polri, the number of online pornographic crimes tends to increase every year, in 2019 it increased by 33%, namely 364 cases where there were 79 children who were victims of paedophile deviant behavior through social media. According to Dittipidsiber in the National Center of missing exploited children (NCMEC) report throughout 2019, placing the Twitter platform as a social media that is fertile for pornographic content with a total of 3,105 accounts of pedophiles. Twitter accounts can be obtained easily so that it facilitates paedophiles to engage in deviant behavior. Paedophiles and victims do not know each other because the child predator has a unique way to deceive the victim, for example by using a false identity, sending expressive messages on tweets, claiming to be the victim's teacher or claiming to be a doctor who is doing research, pretending to know in the real world, then the predator seduces (online grooming) the victim and convinces the victim to be willing to follow the predator's orders, either by sending photos or videos containing child pornography content. In this study, the objective of this research is to design a model that can identify paedophile accounts based on the characteristics of the twitter platform. This model is designed to be able to quickly and accurately identify paedophile accounts. This can be done by extracting the account based and content based feature. Then the model uses these features to conduct training by comparing the accuracy of machine learning algorithms. From the results of the confusion matrix test, this study classifies paedophile and non-paedophile accounts with the best accuracy results using the Random Forest algorithm 97,79% while the SVM algorithm is 96,32%, the Decision Tree 95,59%, KNN 91,18%, and Naïve Bayes 94,85%

Keywords: *Paedophile crimes, Twitter, account identification, account based, content based, machine learning*.

DESIGN OF IDENTIFICATION PEDOPHILE ACCOUNT IN TWITTER PLATFORM BASED ON MACHINE LEARNING

Oleh
Ericson Siregar
NIM: 23219066
(Program Studi Magister Teknik Elektro)

Institut Teknologi Bandung

Disetujui untuk maju sidang tesis
Pembimbing

8 Februari 2021

Yudistira Dwi Wardhana Asnar, S.T., Ph.D.
198008272015041002

THESIS USAGE GUIDELINES

The Unpublished S2 thesis is registered and available at the Bandung Institute of Technology Library, and is open to the public provided that the copyright is with the author by following the IPR rules that apply at the Bandung Institute of Technology. Literature references are allowed to be recorded, but quotations or summaries can only be done with the author's permission and must be accompanied by scientific rules to specify the source.

The citation of the research results of this thesis can be written in Indonesian as follows:

Siregar, Ericson. (2021): Perancangan Model Identifikasi Akun Pedofil Pada *Platform* Twitter Berbasis *Machine Learning*, Tesis Program Magister, Institut Teknologi Bandung.

and in English as follows:

Siregar, Ericson. (2021): *Design Of Identification Paedophile Account In Twitter Platform Based On Machine Learning*, Master's Thesis, Institut Teknologi Bandung.

Replacing or publishing part or all of the thesis must be approved by the Dean of the Postgraduate School, Bandung Institute of Technology.

It is dedicated to my parents, wife, children, my beloved family who always support physically and mentally.

ACKNOWLEDGEMENTS

Thank you to the Lord Jesus Christ, The Almighty God, because of his gift this thesis titled Design Of Identification Paedophile Account In Twitter Platform Based On Machine Learning can be completed.

The writing of this thesis was not spared from the help of many parties, for that with a sense of humility and respectfully, the authors thank:

1. Parents, sibling and all relatives who have provided support and prayers;
2. Mr. Yudisthira Dwi Asnar as the supervisor who patiently guided the writer until the completion of this thesis;
3. Cybercrime Directorate of CID, INP who are willing to be the locus of research and all who have participated and played a role in the preparation of this thesis.

Thus the author can convey, the author apologizes for errors both in deeds, words, and in writing this thesis.

TABLE OF CONTENTS

APPENDIX LIST

LIST OF PICTURES AND ILLUSTRATIONS

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

ABBREVIATIONS	NAME	First time use on page
Dittipidsiber	Direktorat Tindak Pidana Siber	1
Bareskrim	Badan Reserse Kriminal	1
Polri	Kepolisian Republik Indonesia	1
NCMEC	*National Center of Missing Exploited Children*	1
CT	*Crime Total*	1
CC	*Crime Clearance*	1
Kemenkominfo	Kementrian Komunikasi dan Informatika	2
UNICEF	*The United Nations Children's Fund*	2
KNN	*K-Nearest Neighbour*	3
DT	*Decision Tree*	3
NB	*Naïve Bayes*	3
RF	*Random Forest*	3
SVM	*Support Vector Machine*	3

SYMBOLS

Chapter I Introduction

This chapter contains the background, problem formulation, research objectives, research benefits, research limitations and writing systematics related to thesis writing.

I.1 Background

Online pornography crimes often occur in Indonesian society. This is evidenced by the data collected by the Directorate of Cyber Crime (Dittipidsiber) of the Indonesian National Police, seen in Figure I.1 that the number of online pornography crimes has tended to increase over the last 5 years, in 2019 it increased by 33%. (Ditsiber Bareskrim Polri, 2019).

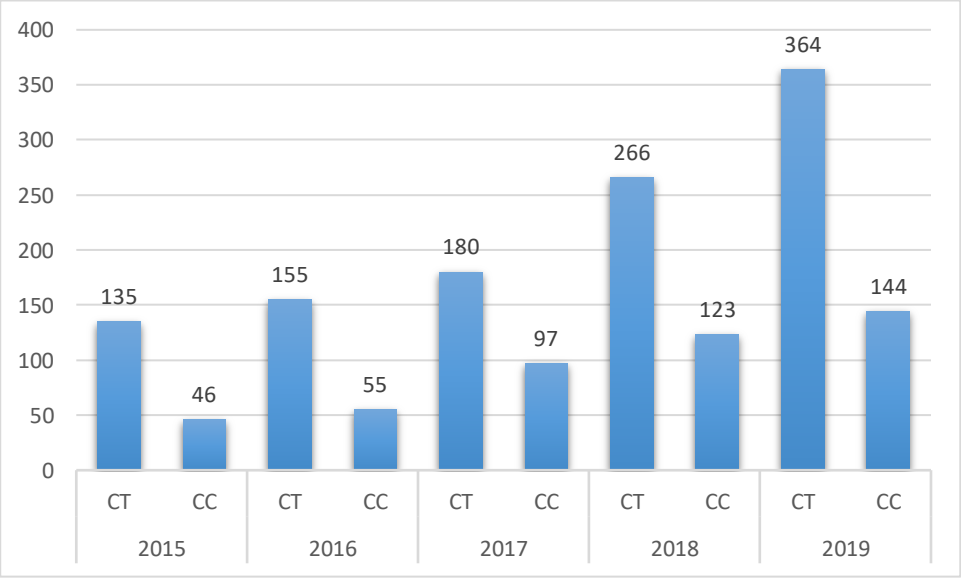

Figure I.1 Total Crime (CT) and Crime Clearance (CC) of Online Pornography

In the online pornographic crime data, it can be seen that there are 2 victim objects, namely adults and children. Throughout 2019, of the 144 cases that had been resolved, there were 79 child victims. Children become victims as a result of pedophile perpetrators who have deviant sexual orientations (Probosiwi and Bahransyaf, 2015). According to the reporting data received by Dittipidsiber from the National Center of Missing Exploited Children (NCMEC), the social media platform is a shelter for pedophiles, it can be seen in Figure I.2.

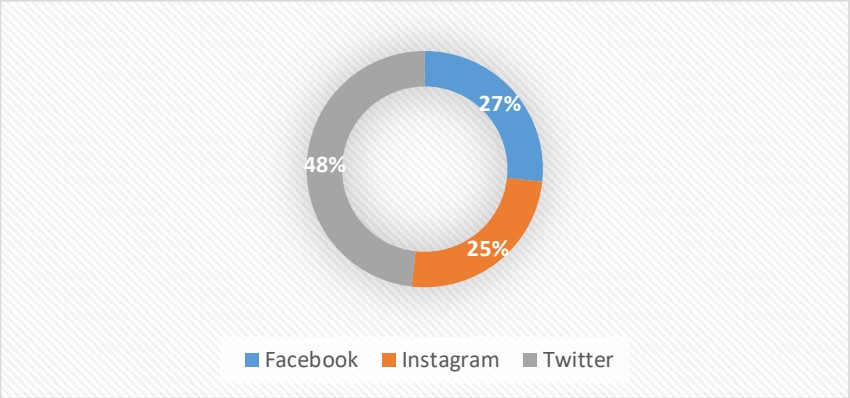

Figure I.2 Percentage of Accounts Reported by NCMEC by Platform

In this data, it is known that the twitter platform contributed the largest number, namely 47% or 3,051 accounts of pedophiles, followed by the Facebook platform 27% or 1,703 accounts of pedophiles, and Instagram 25% or 1,542 accounts of pedophiles. According to research conducted by the Ministry of Communication and Informatics, and UNICEF (The United Nations Children's Fund) on the behavior of children and adolescents on the internet, it is found that around 80% of children and adolescents in Indonesia access the internet every day. Research also reveals that around 24% of the population of these children communicate with strangers via the internet and 25% of them share their addresses and mobile numbers (KemenKomInfo, 2014).

The frequent occurrence of online pornography crimes with child victims is in line with the fairly high reporting of pedophile offenders' accounts on social media platforms. We cannot deny that the freedom to surf in cyberspace and the weakness of parental supervision, brings new threats to children as a vulnerable young group (Alodia et al., 2019).

There are several previous studies that have discussed online pornographic crimes with child victims, based on research (Fournier and Danisch, 2014) which designed a semantic framework to detect pedophile activity with certain keywords in peer to peer networks. In the study (Belbeze et al., 2009), the detection of pedophile offenders with word features was complemented by an expert assessment manual. In a study (Gupta et al., 2012), the chatter of pedophiles using the term online

grooming was detected by the Social Network Analysis method for complete mapping of the anomaly conversations between the perpetrator and the child victim in raw text format.

Based on previous research, there is a research opportunity to identify pedophile accounts on social media platforms, using a more universal model including feature analysis on account profiles (account based) and account timeline text extraction (content based). This is also supported by the results of data collection and interviews with stakeholders, which states that in 2019 online pornography crimes often occur in Indonesians on social media platforms, especially on the twitter platform (Kustoni, 2019). Therefore, this study raises the title of designing a pedophile account identification model on a machine learning-based twitter platform. Modeling is done using the Support Vector Machine (SVM) algorithm, Decision Tree, Naïve Bayes, K-Nearest Neighbor, and Random Forest. Furthermore, from the five algorithms, we will look for a model that is able to classify the pedophile account with the best accuracy. This research is expected to be able to provide early warning to law enforcers regarding the existence of pedophiles in online pornography crimes on the Twitter platform.

I.2 Formulation of Problem

Based on the background description above, the formulation of the research problem is how to identify pedophile accounts based on account profiles which include followers, following, account age, and the number of status and content extraction on the account timeline which includes word weighting, the number of urls on tweets, and the total. retweet.

I.3 Research Objectives

The general objective to be achieved from this research is to produce a method of identifying pedophile accounts on the twitter platform so that it can be used by law enforcement to prevent cyber crime.

In order to achieve these general goals, specific objectives are needed, namely to produce a collection of datasets from pedophile accounts, produce relevant features

from the dataset collection, and produce effective and efficient techniques for analyzing the characteristics of pedophile twitter accounts.

The main output of this research is a pedophile account identification method to prevent cybercrime and builds a model that can identify early on if there is a potential account as a pedophile account, while the specific output is a collection of datasets on pedophile twitter accounts. dataset on pedophile twitter account.

I.4 The Scope of Research

The scope of the problems in this study are as follows.

1. The research was conducted on the twitter platform.
2. Pedophile account identification modeling based on account profiles and twitter account timelines.
3. The research was conducted using the pornographic account tweets for the period December 1 - December 30 2020 on the internal database of the National Police Criminal Investigation Agency (Dittipidsiber).
4. The research was conducted by manually labeling accounts by two experts, focusing on pornographic tweets, account profiles, and unique words that often appear.
5. The perpetrator's account data used is open data and does not use intelligence or confidential data in identifying pedophile and non-pedophile accounts.

I.5 Research Hypothesis

From the formulation of the problem above, the following research questions can be drawn.

1. What is the method of collecting pedophile account data on the twitter platform to create a pedophile account dataset?
2. How to use text weighting to identify pedophile and non-pedophile accounts?
3. How to analyze the profile properties of a pedophile twitter account on the twitter platform?

I.6 Research Methodology

The method used in this research is CRISP-DM (Cross Industry Standard Process for Data Mining) which consists of 6 stages, namely:

1. Business Understanding Phase

   In this stage, the researcher conducts interviews, document analysis, and studies literature on Polri stakeholders to find some evidence or indication that supports the assumptions in formulating research objectives realistically.

2. Data Understanding Phase

   The data understanding stage was carried out to improve understanding of design and success factors using a literature review of empirical research. At this stage, data collection from the twitter platform was carried out using crawling tools to form a dataset of pedophile and non-pedophile accounts.

3. Data Processing Phase

   At this stage, the researcher prepares the available data, then analyzes the data attributes intensively. At this stage, the best feature is also selected by looking for significant differences in the data. So that we get a good dataset for modeling.

4. Modeling phase

   In the modeling stage, the researcher selects and applies the appropriate modeling technique, by calibrating the model rules to optimize the expected results.

5. Evaluation Phase

   This stage evaluates one or more models used in the modeling phase to obtain quality and effectiveness before being deployed for use, and determines whether there are models that meet the objectives in the early phase.

6. Deployment Phase

   The dissemination stage, through the resulting model, tries to make predictions with data that has never been recognized.

I.7 Systematic of Writing

1. **Chapter I Introduction**

   This chapter describes a brief description of the research background, the formulation of research problems, the objectives of the research, and the scope of the research, the methodology and writing systematics used.

2. **Chapter II Literature Review**

   This chapter describes references and research that has been done previously related to research topics. In addition, this chapter also describes literature studies related to techniques that can be used to identify pedophile and non-pedophile accounts on the twitter platform.

3. **Chapter III Research Methods**

   This chapter describes the research method that outlines the stages to be carried out in completing research using the CRISP-DM to identify pedophile accounts on the Twitter platform. In more detail, the steps in each stage of the research will be described as well as the results.

4. **Chapter IV Results and Analysis**

   This chapter describes the process of collecting data to form a dataset of pedophile accounts. From this dataset, a property analysis will be carried out. In addition, this chapter also describes the results of training and test results from the pedophile account dataset collection to design pedophile account identification methods on the Twitter platform. Starting from selecting the technique used to analyzing the model that has the best performance in identifying pedophile accounts.

5. **Chapter V Closing**

   This chapter contains the conclusions of the research results that have been carried out as well as suggestions for the development and improvement of further research.

Chapter II Literature Review

II.1 Cyber Crime Database

In general, the cyber crime database at the Directorate of Cyber Crime contains data characteristics of each type of online crime. However, when conducting interviews with stakeholders it is known that not all computer crimes have databases, only in cases of concern such as hoax crimes, online pornography, and hate speech which are very disturbing to the public (Kustoni, 2019). Cybercrime is taken from the definition according to the United Nations (United Nations Congress, 2000), defining the definition of cyber crime into two categories as follows:

1. Computer crime is any illegal act by means of electronic operations that target the security of the computer system and the data it processes. Examples of this are defacement (changing website pages illegally), Denial Distribution Of Service (making the system not running or functioning properly after being flooded with data by many infected computers and becoming a network robot), keylogging (recording every typing activity. on computer keyboards and applications displayed on the screen), identity theft (theft of important data from the people who are the target), illegal access (illegally entering into a computer), and hacking (hacking) computer networks.
2. Computer-related crime, which is any illegal act committed by, or related to, a computer system or network (computer network). This definition includes all forms of conventional crimes such as theft, robbery, pornography, murder, corruption, drugs and others, where in the crime there is electronic evidence such as computers and cell phones used by the perpetrator to communicate with each other or store data relating to the planning, process and results of the crime.

Currently, computer related crime online pornography has been categorized as an extraordinary crime, because the number of cases of pedophile perpetrators and many child victims was triggered by the growing development of online pornography. Researchers dig knowledge in investigations conducted by law enforcement, namely about the opportunities for pedophiles in online pornography crimes. Furthermore, this research will focus on the database of pornographic account tweets.

II.2 Twitter

Twitter is a social networking service, which allows users to communicate with each other. Users can send and read messages with a maximum of 280 characters, which are called tweets. Tweets from other users who are being followed or followed will appear on the home page to read. Users can retweet or resend messages sent by other users. In the message that is sent, if you mention the name of another user, the tweet is written at the @ sign followed by the username. Users can use the # sign (hashtag) to compose messages based on topic. Twitter was founded in March 2006 by Jack Dorsey. The growth in the number of Twitter users is increasing rapidly, so that now there are 326 million Twitter users (Wearesocial.com, 2019). In Figure II.1, it can be seen that Twitter has several main features which are the identity of Twitter itself, which distinguishes it from other social media. These features include:

1. Profile Tweet

   Tweet is a post on Twitter, which only allows messages up to 280 characters in length. By default, users' tweets are visible to the public, but users can limit sending tweets to their followers. Users can send tweets via the Twitter site. Users can subscribe to other users' tweets by following the user in question, and users who follow these will become followers for the users they follow. Other names are tweeps, short for Twitter and peeps. Users can check people who unfriend (unfollowing) through third party services. Apart from that, users can also block other users who have followed them. On the tweet profile, there is also a username, biography, and time of creation of a Twitter account.

2. Tweet content

   Content is the content of the user's tweet. Data stored in content is very useful if it can be processed into information. Before being processed into information, the data on Twitter must be collected first, for further analysis and information extraction is carried out. According to (Saputra, 2017) information is obtained that content from Twitter contains: • 93% contains text only, without images or videos • 65% of text contains links to other web pages • Tweets contain links, 86% are retweeted more often • Between images and videos, images are the most common in users' tweets • 62% of images are

humorous, the remaining 38% are other types • Text that contains how-to or list-based articles are three times more likely to be retweeted than plain text. Users can group their tweets by topic or type using hashtags - words or phrases that start with a "#" sign. Meanwhile, the "@", followed by the username, is used to send or reply to tweets to other users. To repost other users' tweets and share them with their own followers, there is a retweet feature, which is denoted by "RT". Twitter has also used its own domain, namely t.co, to auto-abbreviate all URLs posted on its site. A word, phrase, or topic that is discussed more than any other topic is called trending topics. A topic can become trending because of a concerted effort by users, or because of an event that prompts people to talk about a particular topic. This topic helps Twitter and its users to understand what's going on in the world. Twitter itself has changed the algorithm of previous hot topics to prevent manipulation of trends.

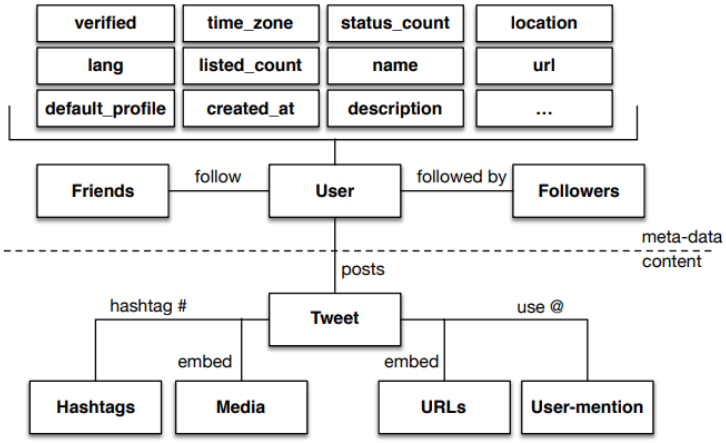

Figure II.1 Information on Twitter account (Uddin et al., 2014)

On Twitter everyone makes a tweet regardless of the type of tweet, sometimes in someone's tweet there are tweets that only consist of fragments of words whose meaning is difficult to know, it is not uncommon for someone to make junk tweets that are really meaningless in big references such as in the Big Indonesian Dictionary if they only specialize on tweets in Indonesian. The resulting data is valuable but little knowledge is obtained from these data, therefore the role of a science called Data Mining. Twitter provides space or opportunity for perpetrators of online pornography crimes, one of which is pedophiles to commit their crimes with messages that deceive and convince vulnerable youth groups to become

victims. It can be seen in Figure II.2, the type of features on the twitter platform to explore the characteristics of an account, referring to research (Gheewala and Patel, 2018).

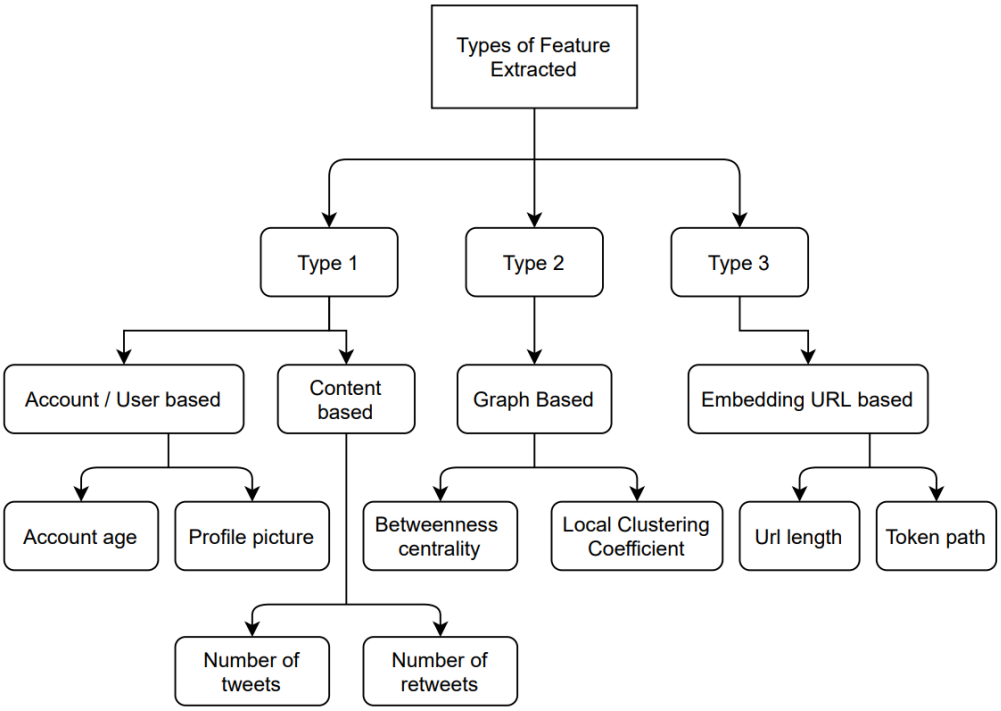

Figure II.2 Types of Twitter features (Gheewala and Patel, 2018)

II.3 Online Pornography Crimes

The definition of pornography according to Law No.44 of 2008 in Article 1 Point 1 is pictures, sketches, illustrations, photos, writings, voices, sounds, moving pictures, animations, cartoons, conversations, gestures, or other forms of messages through various forms. communication media and / or public performances, which contain obscenity or sexual exploitation that violate the norms of decency in society. Whereas in Article 1 point 4, the definition of a child is someone who is not yet 18 (eighteen) years old (Pornography Law, 2008).

Criminal threats for perpetrators of sexual violence against children are regulated in Article 82 jo. Article 76E perpetrators of 'obscene acts' against children who are committed through violence or threats of violence, commit deception, commit a series of lies, or persuade children to commit or allow obscene acts are also punishable by a maximum sentence of 15 years and a maximum fine of IDR 5 billion (Child Protection Law, 2014).

The criminal threat for the perpetrators of spreading pornographic content online is regulated in article 45 paragraph 1 jo. Article 27 paragraph 1 Any person who knowingly and without right distributes and / or transmits and / or makes accessible Electronic Information and / or Electronic Documents that have contents that violate decency as referred to in Article 27 paragraph (1) shall be punished with imprisonment at the most. 6 (six) years and / or a maximum fine of Rp1,000,000,000.00 (one billion rupiah) (UU ITE, 2016).

Figure II.3 shows the types of perpetrators and victims of online pornography crimes in Indonesia. There are several studies that have categorized pornographic crimes based on the type of pornographic perpetrators, namely human traffickers (Alvarez, 2019), pedophiles (Fournier and Danisch, 2014), pornographic spammers (Abozinadah et al., 2015).

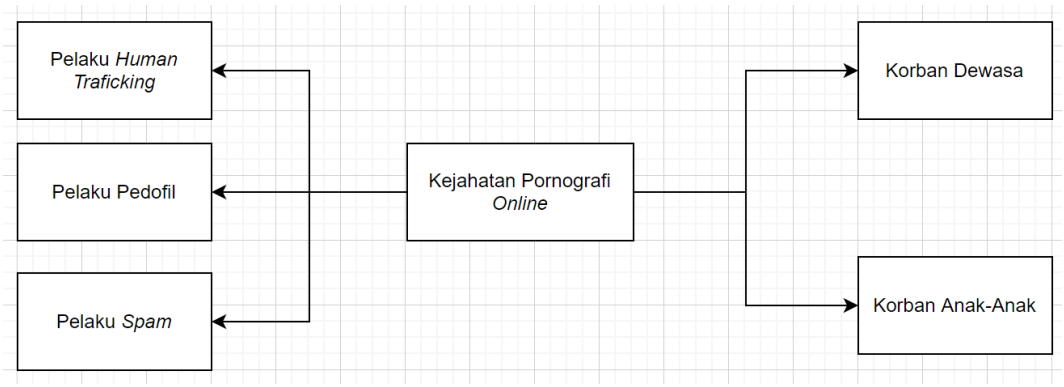

Figure II.3 Types of Perpetrators and Victims of Online Pornography Crimes in Indonesia (Ditsiber Bareskrim Polri, 2019)

According to research conducted by the Ministry of Communication and Informatics, and UNICEF (The United Nations Children's Fund) on the behavior of children and adolescents on the internet, it is found that around 80% of children and adolescents access the internet every day or at least once a week. The study also revealed that around 24% of the population of these children communicated with strangers via the internet and 25% shared their address as well as their home phone number. Meanwhile, 52% of children in Indonesia have encountered pornographic content in cyberspace from advertisements and unsuspecting sites they visited, while only 14% of them visited these sites voluntarily (KemenKomInfo, 2014).

II.3.1 Perpetrators of Pedophiles in Online Pornography Crimes

Pedophile perpetrators have certain characteristics, as shown in Figure II.4 Illustration of Pedophile Behavior. According to (Durkin, 1997) deviant behavior of pedophiles on the internet is trading child pornographic content in the form of text or images, doing online grooming through chat messengers, and communicating with other pedophiles through social media with validation requirements through sharing text-based stories and sharing images of victims. Perpetrators of pedophiles are categorized as extraordinary crimes, because the victims are a group of vulnerable groups, namely children.

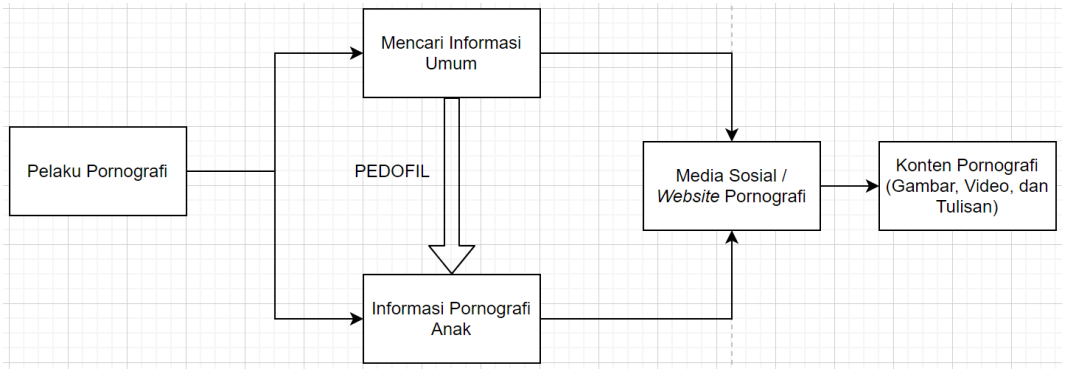

Figure II.4 Illustration of Pedophile Behavior

The number of cases of sexual violence against children is triggered by the growing development of online pornography. Strengthened by the freedom to access the internet, making it easier for social media users to spread pornographic content, find and share information.

Sexual crimes against children are not only committed in the real world, but also in cyberspace as a new trend of sexual crimes (Probosiwi and Bahransyaf, 2015). Some cases of pedophilia that have occurred in Indonesia (Ditsiber Bareskrim Polri, 2019) and which have attracted the attention of the public at large include:

1. In 2014, a pedophile perpetrator was arrested by the National Police Criminal Investigation Unit in Surabaya, for distributing ten thousand pornographic photos of minors, through the Facebook media under the guise of an adolescent reproductive health doctor then asking the victim to take a picture fully clothed naked, taken a picture. The number of child victims who were identified was 12 children.

2. In 2017, eight pedophiles were arrested by Polda Metro Jaya in Jakarta for distributing child pornography content on the loly candy facebook group and twitter. The number of child victims who were identified was 13 children.
3. In 2018, a pedophile perpetrator was arrested by the Tangerang Police, for spreading child pornography content on twitter and facebook. The number of child victims who were identified was 41 children.
4. In 2018, a pedophile perpetrator was arrested by the Jambi Regional Police in Jambi for spreading child pornographic content on Instagram and Twitter. The number of child victims who were identified was 87 children.
5. In 2019, a pedophile perpetrator was arrested by the Criminal Investigation Unit at the Madura Pamekasan prison for distributing child pornographic content on google plus media, facebook, and twitter under the guise of a school teacher. The number of child victims who were identified was 50 children.

Pedophilia cases that occur today are increasingly worrying and threatening the world of children, in the five cases above, the average age of children is 13 to 17 years. According to data collected by Dittipidsiber in 2019, online pornography crimes increased by 33%, where there were pedophiles in online pornography with a total of 79 child victims. In the reporting data, the National Center of missing exploited children (NCMEC) places the Twitter platform as a fertile social media with online pornographic content, there are 360 reports of pornographic accounts on the Twitter platform in 2019 (Ditsiber Bareskrim Polri, 2019). Seen in Figure II.5, accounts with pornographic nuances can be found on the twitter platform by searching for words that contain pornographic elements, and on pornographic accounts there is an opportunity for crime of pedophile perpetrators where children as a vulnerable group can become victims of deviant behavior.

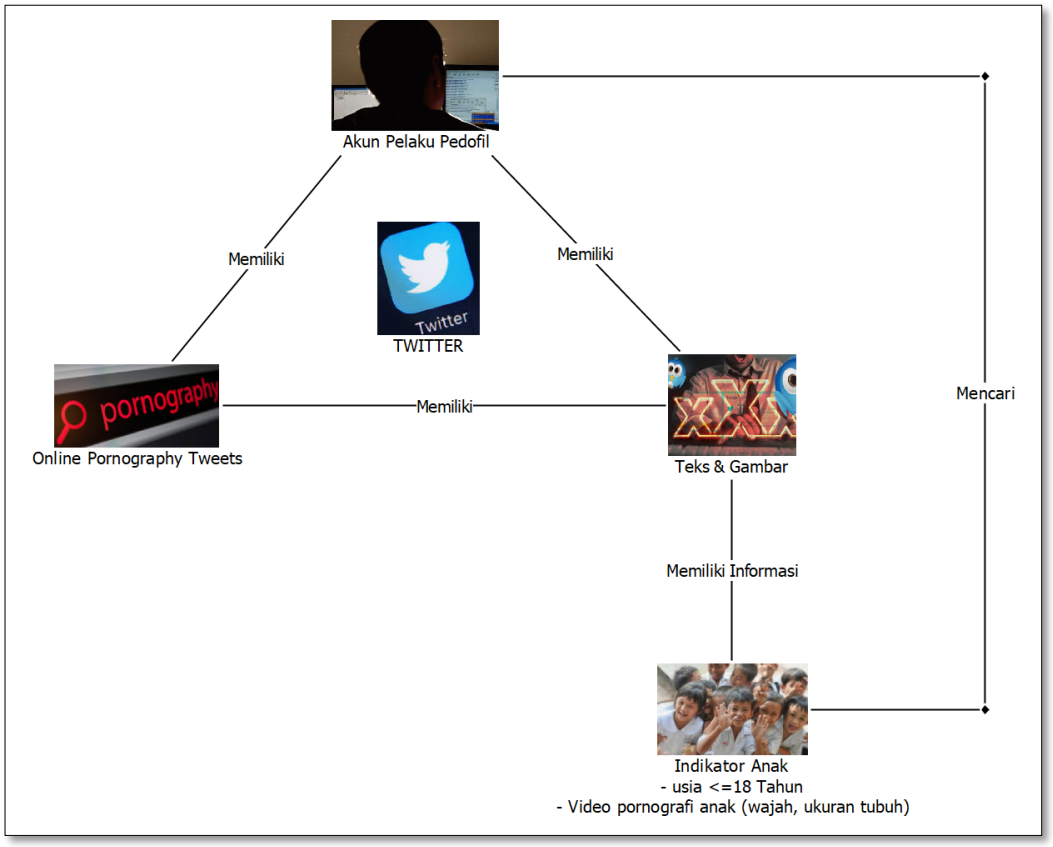

Figure II.5 Illustration of Pedophile Perpetrators on Twitter

The deviant behavior of pedophile actors appears in social interactions on social media by taking actions that interfere with ongoing social interactions (Nur Rosyidah and Nurdin, 2018). A variety of deviant behavior by a person in interactions on social media can be in the form of sexual harassment. In Figure II.6, according to the editorial of liputan6.com, pedophiles use cyber space by means of coercing, threatening, persuading victims with the lure of money, comics, novels, and internet pulses, even the perpetrators are hiding behind anonymity with the characteristic of using special hashtags in the pedophile world. (Ditsiber Bareskrim Polri, 2019).

Figure II.6 Punishment for Pedophiles ("HEADLINE: Pedophilia Cases Are Increasing, Is It Time For Perpetrators To Be Castrated? - News Liputan6.com," 2018)

Pedophile crimes on online pornography will damage the next generation of the nation because of the tendency of victims to become perpetrators when they are adults (Probosiwi and Bahransyaf, 2015). The identity of the pedophile account can be identified using various approaches (Gupta et al., 2012). This could include, among other things, investigating account profiles, or using non-verbal indicators (Pendar, 2007) such as the time between opening an account and the first posted entry and the content of tweets on the account timeline.

II.4 Text Mining

Text mining is the process of obtaining high-quality information from text. High-quality information is usually obtained by paying attention to patterns and trends

by studying statistical patterns. Text mining is a technique used to deal with classification, clustering, information extraction and information retrival problems (Berry & Kogan, 2010).

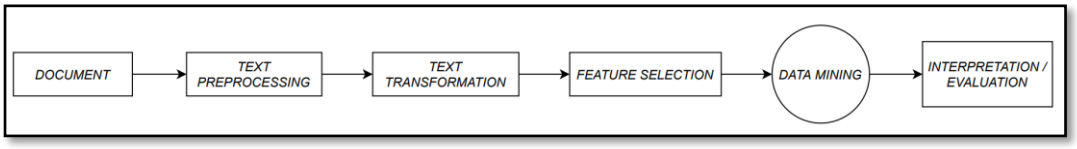

Figure II.7 Text Mining Process

The most popular areas of text mining application are:

1. Information extraction (information extraction): Identification of key phrases and linkages in the text by looking at a certain sequence through pattern matching.
2. Topic tracking (topic tracking): Determination of other documents of interest to a user based on the profile and documents the user has viewed.
3. Summarization (summarization): Making a document summary to streamline the reading process.
4. Categorization (categorization): Determination of the main theme of a text and grouping text based on these themes into predetermined categories.
5. Clustering: Grouping similar documents without prior categorization.
6. Concept linking: Document linking is concerned with identifying shared concepts that help users to find information that would otherwise not have been found using only traditional search methods.

Figure II.7 is a text mining process in which researchers extract simple information on the word content of pornographic tweets to see the differences in words that often appear on the accounts of pedophiles and non-pedophiles. When extracting word features, it is necessary to pay attention to the unique indicators of pedophiles who often use children's age in their chats (Gupta et al., 2012). in text that is visible in numeric form so that it needs to be converted into word form. Broadly speaking, implementing text mining consists of two major stages, namely preprocessing and processing (Anggaradana, 2013).

II.4.1 Text Preprocessing

Text preprocessing is the stage for preparing text into data that will undergo processing at the next stage. Initial input in this process is a complete document (Mustaqhfiri et al., 2012). Text preprocessing in this study consists of several stages, namely: the case folding process, the process of breaking sentences into words (tokenizing), the process of filtering words by changing words into normal slang words and eliminating words that have no meaning to stop words, and the stemming process (Pendar, 2007).

a. Case Folding

   Case folding is a step in the process of changing all letters in the document text to all lowercase, deleting URLs, @mention, #hashtag and delimiters (numeric characters & symbols).

b. Tokenizing

   Sentence splitting is the process of breaking a long document text string into a collection of sentences. With a space "" as a delimiter to cut the document string. By removing these marks the document will be cut into words.

c. Filtering

   It is a process of changing slang words, in words that are unique and often used and then modified into normal words. Furthermore, the stop word is omitted, in words that often appear in documents but whose meaning is not descriptive and has no connection with a particular theme. In Indonesian, the stop word is a liaison word and can be called an insignificant word, for example "in", "by", "on", "a", "because" and so on.

d. Stemming

   It is the process of finding the root word of each word token, namely by returning an affixed word to its basic form (stem). In this study the authors used the literary library on Python 3.9.1 for the stemming process.

II.4.2 Text Processing

The processing stage is the most important stage of the entire text mining process. The technique used at this stage is to weight the terms from the results of the prepocessing stage. Each term is given a weight according to the weighting scheme chosen, be it local, global or a combination of both. Many applications apply combination weighting in the form of multiplying the weight of the local term frequency and the global inverse document frequency written in TF-IDF. This research will use the TF-IDF (Term Frequency Inverse Document Frequency) method, a method used to determine the frequency value of a word in a document or article and also the frequency in many documents. This calculation determines how relevant a word is in a document. This weighting is a statistical measure to measure how important a word is in a document. The level of importance increases when a word appears several times in a document but is offset by the frequency of occurring the word in a document (Pendar, 2007). TF-IDF can be formulated as follows:

$$\text{TF IDF}\left(t_{k,}d_j\right) = TF\left(t_k, d_j\right) * IDF(d_j) \tag{2.1}$$

Where previously the Term Frequency (TF) was calculated, namely the frequency of appearance of a term in each document. Then calculated Inverse Document Frequency (IDF), which is the weight value of a term calculated from the frequency with which a term appears in several documents. The more often a term appears in many documents, the smaller the IDF value. Following are the TF and IDF formulas

$$TF\left(t_k, d_j\right) = f\ (t_k, d_j) \tag{2.2}$$

$$IDF(t_k) = log\ \frac{N}{df\ (t)} \tag{2.3}$$

In TF-IDF weighting, then dimensionally reduction is carried out on the formed word vectors (Pendar, 2007), this is useful for making computational time efficiency and with unique word vectors, can make a significant difference when modeling the classification of accounts of pedophiles and non-pedophiles.

II.5 Data Mining

Data mining is the process of using statistical, mathematical, artificial intelligence and machine learning techniques that are used to extract and identify useful information and related knowledge from various large databases (Larose, D. T., 2014). The following are the characteristics of data mining: Data mining is related to the discovery of something hidden and certain data patterns that have not been known before, data mining can use very large data. Very large data is usually used to make data mining results more reliable. Data mining has several techniques based on the tasks performed and each technique has its own algorithm. The following are techniques in data mining which are divided into six categories:

a. Description. Researchers usually try to find ways to describe patterns and trends hidden in the data.
b. Estimation.This estimation technique is similar to the classification technique, except that the objective variables are more numerical than categorical.
c. Prediction, has similarities with estimation and classification. However, the predicted results indicate something that has never happened or may happen in the future.
d. Classification, in the variable classification, objectives are categorical. For example, we will classify income into three classes, namely high income, medium income and low income.
e. Clustering, is more towards grouping records, observations and cases in classes that have similarities.
f. Association, identifies the relationship between various events that occur at one time.

II.5.1 Stages of Data Mining

Data mining can be divided into several stages, the data mining stage is carried out as a series of processes, and is interactive, in which the user is directly involved or through a knowledge base. The following are the stages in data mining:

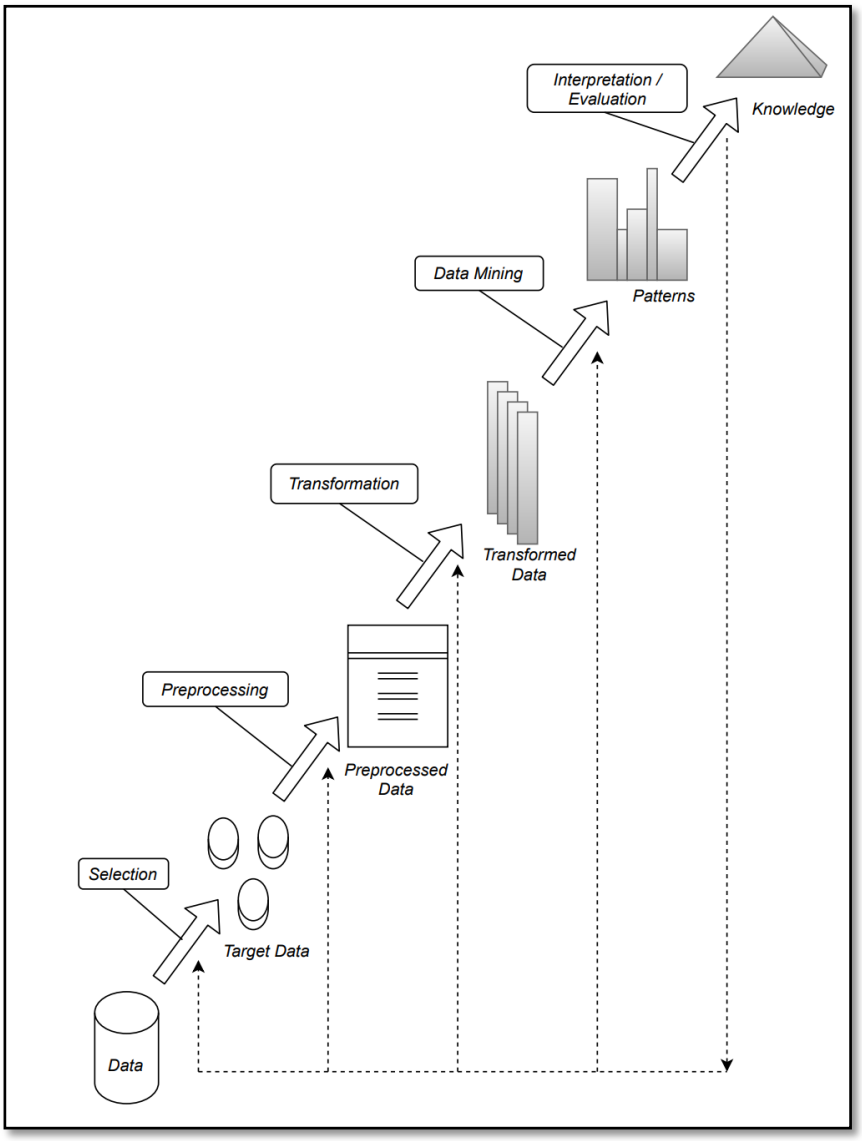

Figure II.8 Stages of Data Mining

Description in Figure II.8:

1. Data Cleaning

   Data cleaning is performed to remove noise and inconsistent or irrelevant data. Often the data obtained from a company database or obtained through experimental results has incomplete data entries such as missing, invalid data and / or just a typo. In addition, there are data attributes that are not relevant to the data mining hypothesis that is owned and then discarded. Data cleaning will affect the performance of data mining techniques. Because the processed data will be reduced in number and complexity (Gupta et al., 2012).

2. Data Integration

   Data integration is the merging of data from various databases into one new database. The data used in data mining is not only obtained from one database but also obtained from several databases or text files. Data integration can be done on attributes that identify unique entities such as attributes for account names, account timelines and so on. In carrying out data integration, it must be carried out carefully so that the results do not deviate and mislead future action taking. In doing data integration, it is necessary to transform and clean data because data from two databases are often written differently and even the data in one database is not in another database.

3. Data Selection

   Not all data in the database is used, therefore only appropriate data will be taken for analysis. As an example of a case examining the suspicious account trend factors in research (Alvarez, 2019), it is not necessary to take all hashtags, but enough with the relevant hashtags.

4. Data Transformation

   Some data mining techniques require a special data format before they can be applied. Before being processed in data mining data will be converted and combined into an appropriate format (Gupta et al., 2012). The data transformation strategy includes:

   a. Attribute construction (or feature construction), where new attributes are built and added from a given attribute set to aid the mining process.
   b. Normalization, trying to give the same weight to all attributes. Normalization is very useful for classification algorithms, in this study we will use the Min-Max. Min-max normalization performs linear transformations on the original data.

5. The Mining Process

   This stage is the main process when methods are applied to find valuable and hidden information or knowledge from data.

6. Evaluate Patterns

   To identify interesting patterns into the found knowledge based. At this stage the results of data mining techniques in the form of distinctive patterns or predictive

models will be evaluated to assess whether the existing hypotheses have been achieved. However, if the results obtained do not match the hypothesis, several alternatives will be made, such as making feedback to improve the data mining process, trying other data mining methods and accepting these results as unexpected results that may be useful.

7. Knowledge Presentation

   The last stage of the data mining process is how to formulate decisions or actions from the results of the analysis obtained. Visualization and presentation of knowledge regarding the methods used to obtain user-acquired knowledge. There are times when this should involve people who do not understand data mining. Therefore the presentation of data mining results is in the form of knowledge that can be understood by everyone in one necessary stage in the data mining process. In this presentation, visualization can also help communicate the results of data mining.

II.5.2 Classification

Classification is one of the most important tasks in data mining. Organizing and grouping data into different classes is the main purpose of classification. Seen in Figure II.9, the definition of classification is a function that is predictive and classifies certain data items into a class (Pendar, 2007). A classification is made from a set of training data with a class that has been determined and known for its characteristics beforehand. Classification performance is usually measured with precision.

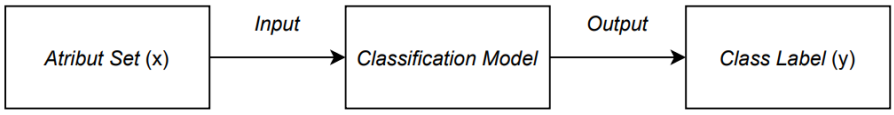

Figure II.9 Block Diagram of Classification

In this study, a supervised learning method will be used to form a model that can predict the pedophile or non-pedophile account. Supervised learning is a machine learning technique using training data to carry out learning. The training data in supervised learning are labeled data. This method aims to be able to identify new input labels by using existing features to make predictions and classifications.

Some of the algorithms included in supervised learning include the following:

1. **Support vector machine,** SVM is a technique for data classification that can produce non-linear decision fields and classify data that has an irregular distribution. This avoids properties with a larger numeric range dominating those with a smaller numeric range and avoids numerical difficulties during computation because kernel values usually depend on the product in the feature vector. SVM works in two phases, namely training and testing.

2. **K-Nearest neighbor**, KNN is a machine learning algorithm for classifying new objects based on the number of k closest neighbors. The purpose of using k-NN is to predict whether the object belongs to one particular group or another. In k-NN the data will be expressed in vector space. As the name implies, "Nearest neighbor", k-NN uses a classification based on "proximity" to neighbors (Pendar, 2007).
3. **Naive Bayes,** is one of the algorithms contained in the classification technique. Naive Bayes is a classification using probability and statistical methods proposed by the British scientist Thomas Bayes, which predicts future opportunities based on previous experience, so it is known as the Bayes Theorem. It is a classification algorithm that is quite reliable in handling large data. Naïve Bayes works with the assumption that each property has conditional independence between each property. This assumption is what makes Naïve Bayes able to process data quickly because it has computations that do not pay attention to dependencies between properties (Han et al., 2012)

4. **Decision Tree,** DT describes dependent and independent properties in the form of a tree. This algorithm extracts rules in the form of tree branches from the model used. This algorithm is very effective in explaining the rules of a classification model. This algorithm generates rules from trees and can handle numerical properties, missing values and can also generate error estimates from the resulting tree diagram (Bhowmik, 2008). In performing classification, DT divides the properties based on their entropy and information gain.

Entropy on DT is a coefficient that has a value between 0 and 1, which is used to measure the randomness of the data. If the entropy is 0, it means that all data come from the same class and if the entropy is 1 then some of the data are in one class and some are in another class (binominal classification).

5. **Random Forest**, RF is a protected learning algorithm. As can already be seen from the name, creating a forest and making it somehow random. The "forest" he built, was a Decision tree ensemble, trained most of the time in the "pocket" method. The general idea of the bagging method is that a combination of learning models improves the overall outcome. Simply put, RF builds multiple DTs and combines them to get more accurate and stable predictions. The great advantage of RF is that forests can be used for both classification and regression problems, which make up the majority of machine learning systems today. This research will talk about RF in classification, because classification is sometimes considered as the building block of machine learning. RF has a hyperparameter similar to a decision tree or bagging classifier.

II.6 Cross Validation Testing

Cross Validation is a process for evaluating the accuracy of predictions from a data mining model. Cross Validation is used to obtain predictions using an existing model and then compare these results with known results, this represents the most important step in the process of building a model.

Cross Validation is a validation technique by dividing data randomly into k parts and each part will be carried out a classification process. In Cross Validation, the fixed number of folds or partitions of data is self-determined. The standard way to predict the error rate of a learning technique from a fixed sample of data is to use tenfold cross validation.

II.7 Confusion Matrix Testing

Confusion matrices are often used to describe the performance of a classification model. The confusion matrix contains information about the actual and predicted classifications (Pendar, 2007), as shown in Figure II.10

	Actually Positive (1)	Actually Negative (0)
Predicted Positive (1)	True Positives (TPs)	False Positives (FPs)
Predicted Negative (0)	False Negatives (FNs)	True Negatives (TNs)

Figure II.10 Confusion Matrix

There are 4 components in the confusion matrix, namely True Positive, True Negative, False Positive and false negative.

To evaluate the performance of each model, the Confusion matrix uses accuracy, False Positive rate (FPR), precision, recall and F1 score. The following is the calculation formula used:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad 2.1$$

$$FPR = \frac{FP}{FP+TN} \quad 2.2$$

$$Precision = \frac{TP}{TP+FP} \quad 2.3$$

$$Recall = \frac{TP}{TP+FN} \quad 2.4$$

$$F1\ score = \frac{2\ x\ Precision\ x\ Recall}{Precision+Recall} \quad 2.5$$

II.8 Related Research

There are many studies discussing the classification of online pornography, the most commonly used method is the use of the unique keywords of pedophiles on peer websites or networks. However, this study will discuss the classification of pedophile accounts with an adaptive model on the Twitter platform by not only paying attention to the text on the content of tweets but also paying attention to the descriptive profile of the account. Seen in table II.1 related research.

Table II.1 Previous Research Related to Online Pornography

Researcher	Research Title	Basic Research Ideas	Solution Used
Raphaël Fournier, Maximilien Danisch 2014	Mining bipartite graphs to improve semantic pedophile activity detection	Identify pedophile activity with queries indicating pedophiles.	Perform detection Using filtering and semantic techniques on peer to peer media by sorting keywords.
Nick Pendar 2007	Toward Spotting the Pedophile Telling victim from predator in text chats	Identification of sexual predators online using text categorization.	Perform automated text categorization to identify online sexual predators. Using SVM and k-NN. K-NN classification f-size 0.943 on child-differentiating test data victim side of the text chat between sexual predators. This study involved volunteers who disguised themselves as underage victims.
Aditi Gupta, Ponnurangam Kumaraguru, Ashish Sureka 2012	Characterizing Pedophile Conversations on the Internet using Online Grooming	Use simple keywords to find sexual content for detection.	Look for the presence of a predatory conversation. By investigating the linguistic style and psycho-linguistic profile created for each of the six stages using a Social Network analysis.
Myriam Hernandez Alvarez 2019	Detect possible human trafficking on Twitter	Identification of suspicious tweets on the trafficker's twitter account via the	Mining tweets with pornographic keywords and hashtags typical

		pornographic keywords in Spanish	of human trafficking #escort, #prep ago, #oven, #Dulce, #Fresca, #nova, #lolita, and #flaquita and combine common features (account age, followers, and friends). Furthermore, testing the classification of human trafficking twits using: Naïve Bayes and SVM.
Ehab A. Abozinadah, Alex V. Mbaziira, and James H. Jones Jr. 2015	Abusive Account Detection with Arabic Tweets	Identify accounts with spam tweets from Arabic pornographic tweet data	Mining tweets with pornographic spam keywords in Arabic, then using text mining with a minimum number of tweets as a feature. Furthermore, classification testing using Naïve Bayes, SVM, and Decision Tree.
A.Mbaziira and J.Jones, 2016	Text-Based Fraud Detection Model for Cyber Crimes	Detect fraud in messages cyber crime network	Mining then uses the NLP feature for fraud detection in text messages in the web genre on the Enron model and the FB model using Naïve Bayes, SVM and IBK.
Nur Izzah, Indra Budi, and Samuel Louvan, 2018	Classification of pornographic content on twitter uses SVM and Naïve Bayes	Pornography detection can be done with way: text and image based	Mining pornographic tweets then using TFIDF to give weight to words with a combination of

			unigram and bigram, then classified, SVM is the best compared to Naïve Bayes.
F. Benevenuto, G. Magno, T. Rodrigues and V. Almeid, 2010	Spam Detection on Twitter	Creating a model with User and content based. For spam detection	Perform spam detection with the Non-linear SVM classifier. The results showed about 70% of Spammers and 96% of Non-Spammers Classified True
Dani Gunawan, Rendra Mahardika, Feri Ranja, Sarah Purnamawati, Ivan Jaya, 2019	Identification of Pornographic Sentences in Indonesian	Creating a Pornographic and Non-Pornographic Corpus	This study uses a classification algorithm to identify pornographic sentences. To determine two labels, namely pornography label and non-pornography label. Uses supervised methods for classification.

Chapter III Research Methodology

The research methodology used in this research is CRISP-DM (Cross Industry Standard Process for Data Mining). CRISP-DM is a consortium of companies founded by the European Commission in 1996 and has been established as a standard process in data mining that can be applied in various industrial sectors. The following is a general reference model from the CRISP-DM.

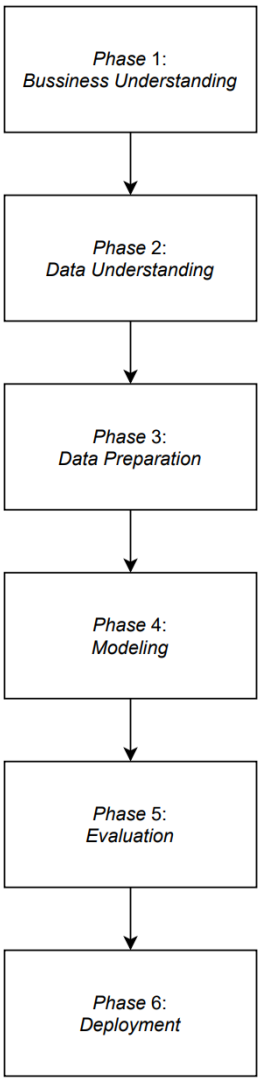

Figure III.1 CRISP-DM General Reference Model

All sequential phases that exist are adaptive. The next phase in the sequence depends on the output of the previous phase. The important relationships between the phases are depicted by arrows. For example, if a process is in the modeling

phase, based on the behavior and characteristics of the model, the process may return to the data preparation phase to further refine the data or move forward to the evaluation phase. Based on the reference model shown in Figure III.1, the following is an explanation:

1. **Business Understanding**

   The first stage is to understand the goals and needs from a business point of view. Then this knowledge is translated into defining problems in data mining. Furthermore, plans and strategies will be determined to achieve these goals.

2. **Data Understanding**

   At this stage it begins with data collection then continues with a process to gain a deep understanding of the data, identify data quality problems, and to detect interesting pieces of data that can be used to hypothesize for hidden information.

3. **Data Preparation**

   This stage includes all activities to build the final dataset (data to be obtained in modeling) from raw data. This data preparation can be repeated several times. This stage also includes the selection of tables, records, and data attributes, including the process of cleaning and transforming data to be used as input in the modeling stage.

4. **Modeling**

   At this stage, various modeling techniques are selected and applied and some of the parameters will be adjusted to obtain optimal values. In particular, there are several different techniques that can be applied to the same data mining problem. On the other hand there are modeling techniques that require a special data format. So that it is possible at this stage to return to the previous stage.

5. **Evaluation**

   In this evaluation stage, the model has been formed and is expected to have good quality from a data analysis point of view. In this stage, before the model is used, whether the model can achieve the objectives set in the initial phase, namely Business Understanding, will be evaluated on the effectiveness and quality of the model. The key at this stage is to determine if there are any business issues that have not been considered.

6. Deployment

At this stage the knowledge and information that has been obtained will be organized and presented in a special form, so that it can be used by users. The deployment stage can take the form of creating a simple report or implementing an iterative data mining process within the company. In many cases, the deployment stage involves consumers, as well as data analysis, because it is very important for consumers to understand what actions must be taken to use the model that has been created.

III.1 First Phase

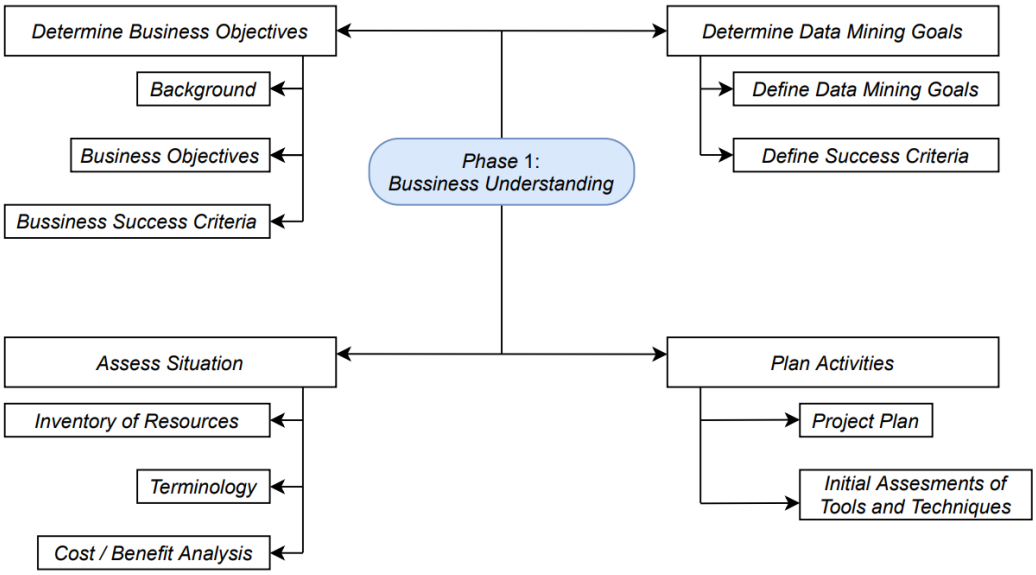

Figure III.2 First Phase, Bussiness Understanding

In Figure III.2, this phase contains four processes, namely:

1. Determine business objectives to understand the objectives the researcher wants to achieve from a business perspective as a whole.
2. Asses situation is carried out to involve facts that exist in the database belonging to the Directorate of Criminal and Criminal Investigation Police regarding resources, constraints, assumptions and other factors that must be considered in determining the purpose of data analysis and plans to be carried out in the study.
3. Determine data mining goals, namely stating the technical data mining objectives for the research being carried out.

4. Plan activities, namely explaining plans aimed at achieving data mining objectives and thereby achieving business objectives, then determining the tools to be used.

III.2 Second Phase

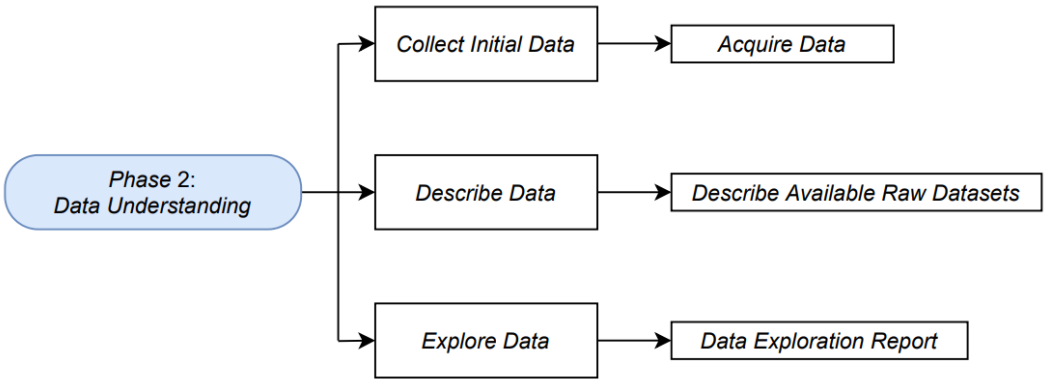

Figure III.3 Second Phase, Data Understanding

Seen in Figure III.3, in this phase there are three processes, namely:

1. Collect initial data, namely obtaining data or access to open data that will be used in research. This initial collection includes loading data if necessary to understand the data.
2. Describe the data, namely checking the data obtained and reporting the results.
3. Explore data, namely exploring the contents of the data obtained, then providing a description of the contents of the data.

III.3 Third Phase

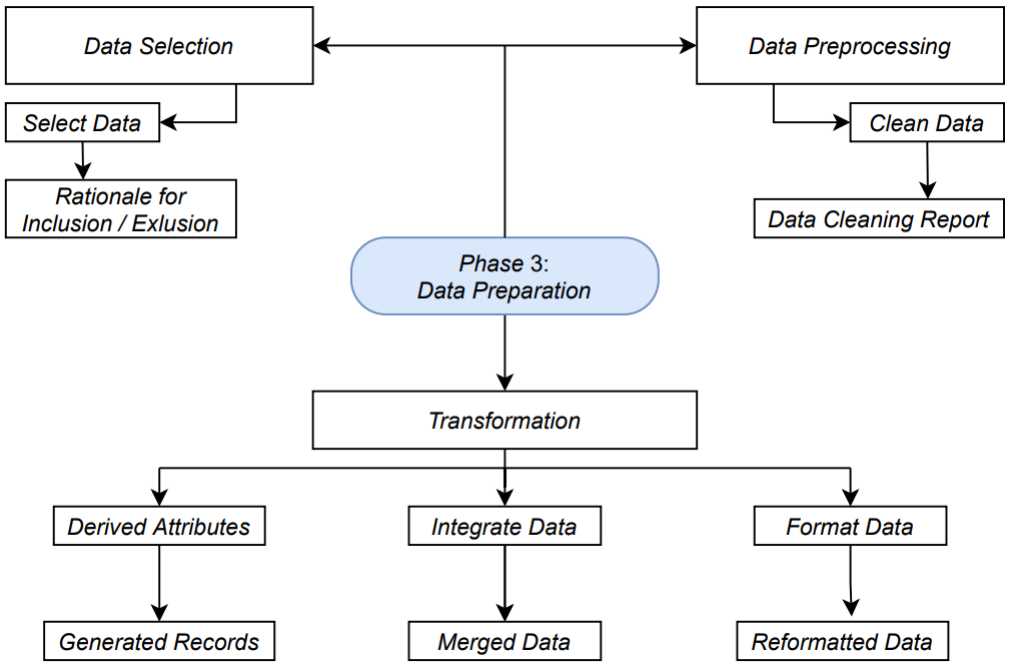

Figure III.4 Third Phase, Data Preparation

Seen in Figure III.4, in this phase there are three processes, namely:

1. Data selection, namely selecting data to be used in the data mining process. In this process, attributes that are adjusted to the data mining process are also selected.

2. Data preprocessing, namely ensuring the quality of the data that has been selected in the data selection stage, at this stage the problem that must be faced is if there are noisy data and missing values. The data cleaning or cleansing process is carried out to find data anomalies that may still be present in the data.

3. Transformation, namely grouping the attributes or fields that have been selected into a new database for data mining materials.

III.4 Fourth Phase

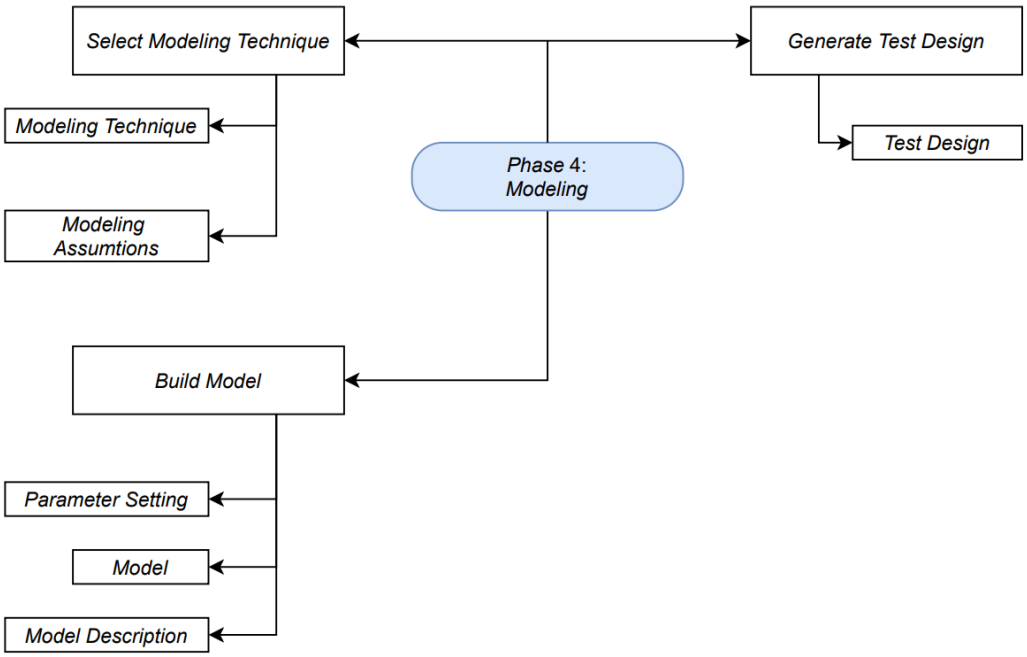

Figure III.5 Fourth Phase, Modeling

Seen in Figure III.5, in this phase there are three processes, namely:

1. Select modeling technique is the first step in modeling, namely by using modeling techniques that have been determined in the business understanding phase.

2. Build a model, namely running the modeling tool according to the procedure.

3. Generate test design, which is to test the model's quality and validity using the prepared dataset.

III. 5 Fifth Phase

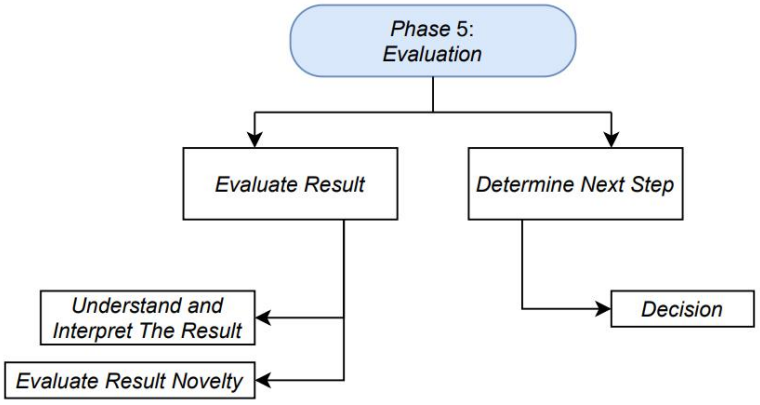

Figure III.6 Fifth Phase, Evaluation

Seen in Figure III.6, in this phase there are two processes, namely:

1. Evaluate result, which summarizes the results of the assessment in terms of business success criteria, including a final statement regarding whether the research has met business objectives.

2. Determine next step, namely to provide a decision whether the modeling technique used can be used as a standard in determining research objectives.

III.6 Sixth Phase

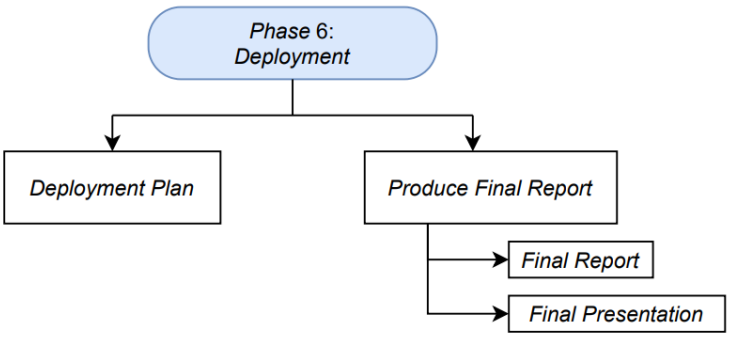

Figure III.7 Sixth Phase, Deployment

Seen in Figure III.7, in this phase there are two processes, namely:

1. Deployment plan, which describes an overview of the plans for making reports that will be made.

2. Produce final report, which provides a visualization of the reports that have been made based on the deployment plan.

Chapter IV Analysis and Design

This chapter describes the steps or processes in designing a pedophile account identification model using machine learning. The stages carried out will be presented scientifically and systematically in accordance with the research methodology used, namely CRISP-DM (CRISP-DM).

IV.I Business Understanding Phase

At this stage, we will explain Determine business objectives which are useful for understanding the goals the researcher wants to achieve from a business perspective as a whole. Some literature analysis evidence, which can support assumptions in formulating research objectives realistically.

1. Determine business objectives, on November 21, 2020, the researcher conducted an interview with the end user, namely Dittipidsiber Bareskrim Polri, represented by Mr. Dani Kustoni, as Head of Sub-Directorate for Dittipidsiber Bareskrim Polri. End users need technology to identify pedophile offenders' accounts on social media. Then based on the results of the interview, there is an online pornography database that can be used to find the existence of the pedophile offender's account on the twitter platform.

2. Asses situation, in this study, the researcher describes that in the database sourced from the Twitter platform belonging to the Criminal and Criminal Investigation Agency's Twitter there are data on online pornography, hoaxes, and hate speech which have relevance to cyber crime which is of course very unsettling to the Indonesian people. In this study, the focus of the researcher was the online pornography crime database, which was then used for in-depth analysis together with experts working on the pornography task force of the Dittipidsiber Bareskrim Polri. The assumption of researchers is that in the collection of online pornography accounts there are accounts of pedophile offenders which then need to be identified, for example in pornographic tweets there are opportunities for pedophiles to spread child pornography content and persuade (online grooming) of potential victims (Gupta et al., 2012). So that knowledge from hidden patterns of accounts of pedophiles can be used for data mining purposes.

3. Determine data mining goals, namely preparing a complete dataset with a collection of pedophile accounts from samples of online pornographic tweets, then from the results of data exploration it can produce relevant features from the dataset, and can be used for modeling the classification of pedophile accounts and non-pedophile accounts.

IV.2 Data Understanding Phase

In this phase, there are two processes: Data collection, namely obtaining data or access to open data to be used in research, and exploring data, namely exploring the contents of the data obtained, then providing a description of the contents of the data.

IV.2.1 Data Collection

At the data collection stage, researchers conducted interviews about online pornography crimes against stakeholders of the Police Criminal Investigation Unit. Then the researchers got knowledge about the data collection techniques by the National Police, including the source of the raw data purely from the Twitter platform. Generally, the data is used by the National Police for investigations into perpetrators of pornography on the Twitter platform (Kustoni, 2019). The technique of collecting pornographic tweets by Bareskrim Polri uses a crawler via the Twitter API with 33 pornographic keywords to produce pornographic tweets which are then exported in ms.excel format as shown in Table IV.1 as follows:

Table IV.1 Keyword Pornography on Twitter Database

Keyword	Keyword	Keyword	Keyword	Keyword	Keyword	Keyword
bokep	bispak	ngewe	jilboob	bokepjepang	vgk	gaybrondong,
sange	bokepindo	toket	stwsange	bokepsma	gaysmp	anak kecil
ngentot	abgsange	openbo	tantesange	videobokepviral	brondong	bocah
memek	jilbob	vcsbugil	bokepindonesia	SMAhijab	bocil	-
bugil	colmex	vcscolmek	jandasemok	SMPhijab	loli	-

IV.2.2 Data Exploration

The sample of accounts on pornographic tweets was taken in the period 1 - 30 December 2020, and obtained 10 attribute columns with 12,469 rows in the form

of pornographic tweets in the format ms.excel. Researchers used ms-excel for analysis of 10 columns and 12,469 rows of tweets data.

B	C	D	E	F	G	H	I	J	K
id	content	datetime_ms	user.screen_name	user.description	user.created_at	user.followers_count	user.friends_count	user.statuses_count	retweet_count
1,34E+18	@brendanwa	1607795831	KasepPutra1	fuck you	1605699471	25	32	67	0
1,34E+18	@BryanPrase	1607915000	ArdianHedra		1606921730	12	139	19	0
1,31E+18	@aldijr57 W	1600939739	Dani25611111		1600853425	1	13	5	0
1,31E+18	@Gudang_Br	1601276045	Afifhid60088337		1601230400	3	0	1	0
1,34E+18	https://t.co/\	1607492271	Jay21574005		1591473462	31	64	80	0
1,31E+18	@Aditya691	1601682052	RezaRevandy	like chubby kids	1601680611	58	30	4	0
1,31E+18	@dimas1688	1601773887	Hantu09258167	im 14	1592512671	1	0	3	0
1,32E+18	RT @g5cUhJ	1602837206	Hakim24806324		1585545328	11	2	49	0
1,31E+18	@vgk_smp B	1601326744	Rangga69258109		1600222911	40	6	4	19

Figure IV.1 Snapshot of Twitter Database

Seen in Figure IV.1, there are 10 attribute columns, consisting of Id, content, datetime_ms, user.screen_name, user.description, user.created_at, userfollowers_count, userfriends_count, user.status_count, user.retweet_count. Descriptions of the 10 attribute columns can be seen in Table IV.2.

Table IV.2 Twitter Database Attributes

Column	**Data Type**	**Attribute Position**	**Information**
Id	Ratio	Account Based	Unique number that identifies the user
Content	Nominal	Content Based	Fill in the user's tweet post
Datetime_ms	Interval	Account Based	Time to post user tweets
User.screen_name	Nominal	Account Based	Account username
User.description	Nominal	Account Based	Biographies of account users
User.created_at	Interval	Account Based	Time of account creation
User.followers_count	Ratio	Account Based	Amount followed by other accounts
User.friends_count	Ratio	Account Based	Amount following other accounts
User.statuses_count	Ratio	Account Based	Number of statuses on the account timeline
Retweet_count	Ratio	Account Based	The number of retweets on account posts

Then the researcher removes duplicates of tweets on the same account in order to get a single account and single tweets. The results of remove duplicates resulted in 2,126 pornographic twitter accounts. Then the account labeling was done manually with the help of two experts who worked on the Dittipidsiber pornography task force. During the process of labeling the accounts of pedophiles, researchers focused on the text content of the account timeline and account profile content (Abozinadah et al., 2015). Then when doing manual labeling, the researcher validates by visiting the account via the twitter.com website, and gets an overview of the perpetrator's account profile and the content of the perpetrator's account. Furthermore, to make it efficient in the labeling process, researchers check account profiles and account content, by looking at general information and at least 5 tweets and relevant unique hashtags or words (Alvarez, 2019). From the labeling process, the researchers obtained 338 pedophile accounts and 1788 non-pedophile accounts. Followed by re-validating the labeled account data to ensure whether the account's existence is still active or has been suspended. In some accounts there is a notification that the account is in limited condition but the researcher can still see the account timeline. It is possible that the account has violated Twitter policy. The notification details can be seen in Figure IV.2.

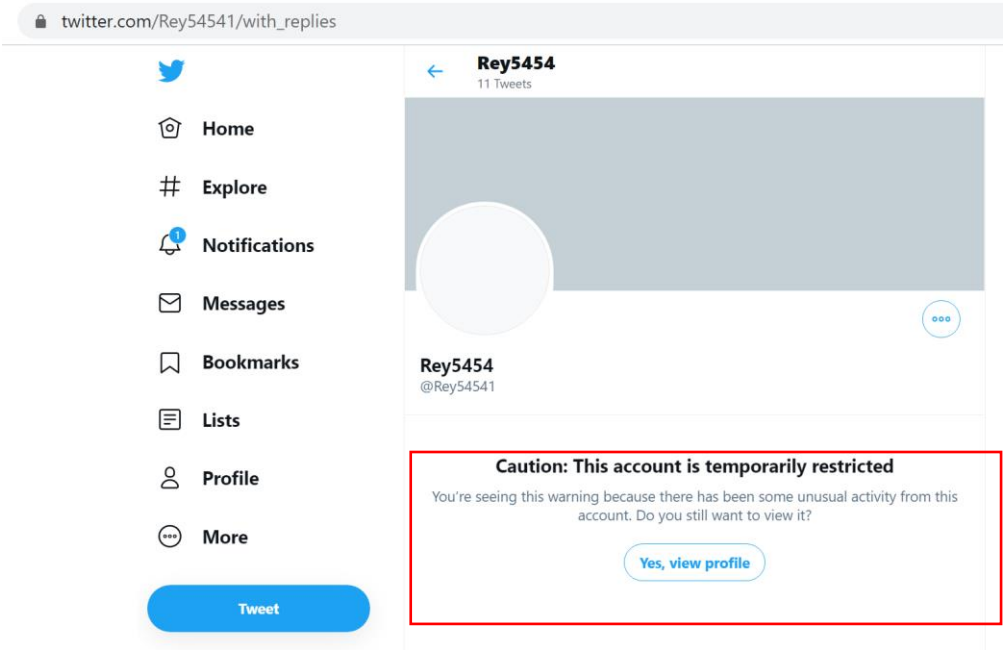

Figure IV.2 Account Notification in Limited Condition

Furthermore, because the number of pedophile accounts was not balanced with the number of non-pedophile accounts, the researchers adjusted the number of accounts by randomly taking from 1788 accounts, taking 338 for non-pedophile accounts. To get the hidden pattern of knowledge from these accounts, the researcher crawled with the help of the Twitter API to get tweets from 338 accounts labeled pedophiles and 338 accounts labeled non-pedophiles, details of the data collection process can be seen in table IV.3.

Table IV.3 Data Collection Process

Data Collection Process	**Device**	**Period**	**Data Description**
Retrieval of Tweets on the Pornography Database belonging to Dittipidsiber Bareskrim Polri	Ms-Excel Manual labeling of accounts, with the help of the twitter.com mobile application	1 Desember – 30 Desember 2020	- 10 Columns and 12,469 lines of tweets. - Remove duplicates tweets on the same account, totaling 2,126 accounts. In these pornographic tweets, there are 338 pedophile accounts, and 1788 non-pedophile accounts.
Crawling tweets on accounts labeled	- Twitter crawler	Adjusted Twitter API	- 10 columns and 16,316 rows of pornographic

pedophile and non-pedophile	-Ms-Excel -Python 3.9.1	with a limit of 1 account = 1,000 tweets	tweets on accounts labeled pedophiles - 10 columns and 52,378 pornographic tweets on accounts labeled non-pedophile

Table IV.4 Comparison of Number of Accounts and Number of Tweets after Crawling

Category	Number of Accounts	Number of Tweets
Pedophile	338 Accounts	16.316 Tweets
Non-Pedophile	338 Accounts	52.248 Tweets
Total	676 Accounts	68,564 Tweets

Furthermore, the researcher checks the quality of the collected data from the crawling. As seen in table IV.4, there are a total of 676 accounts with 68,564 tweets. From the 10 data columns in 676 accounts, the researcher checked the missing value, on the user.description attribute with a total of 165 rows, because the data type in this attribute was nominal, then the fill was replaced to Null. Then for the other 9 columns, they are filled and ready to be used for the next stage.

IV.3 Data Processing Phase

In this study, the focus of the researcher was account identification, so for efficiency and effectiveness the researcher carried out 2 data processing groupings, namely data processing on account based data which was listed in the account profile and data processing on content based which was the data listed in the account timeline content.

IV.3.1 Data Processing on Account Based

At the data processing stage on account based, the researcher chose 7 attributes in the based account for preprocessing data.

Data Cleaning, in this process, the researcher gets the knowledge that the User.created_at column is a numeric attribute that can be used as the age of the account, however, the crawled data is still in the UNIX Time stamp format, so it needs to be converted to normal time.

Data Construct, the researcher uses ms-excel and the datetime module in python to convert the time in the User.created_at column from the UNIX Time stamp to the year-month-date format. Then the researcher created a new column named datetime_convert. Then to improve data quality and to make it easy to read the model that will be used. In this process the researcher reduces the time in the datetime_convert column minus the present date so that the output becomes numeric in days, and the researcher creates a new column called Age. The output of the change in account age can be seen in Figure IV.3.

user.created_at	datetime_convert	Age
1605699471	2020-12-13	23
1605699471	2020-12-12	24
1605699471	2020-12-08	28
1605699471	2020-12-07	29
1605699471	2020-12-05	31
1605699471	2020-12-01	36
1591473462	2020-09-30	98

Figure IV.3 Time Conversion Snapshot Image

Data Integrate, because the data in the dataset is not correlated with data from other datasets and tables, integration with other datasets and tables is not carried out at this stage so that there are no changes in the data structure on the account based.

Data Format, Transformation refers to syntactic modifications made to data but not changing its meaning, by modeling tools. Furthermore, the researcher made a comparison by making an average using the help of the average function on ms-excel to the attributes of followers, followings, age, and status_count because the crawl results are numerical based.

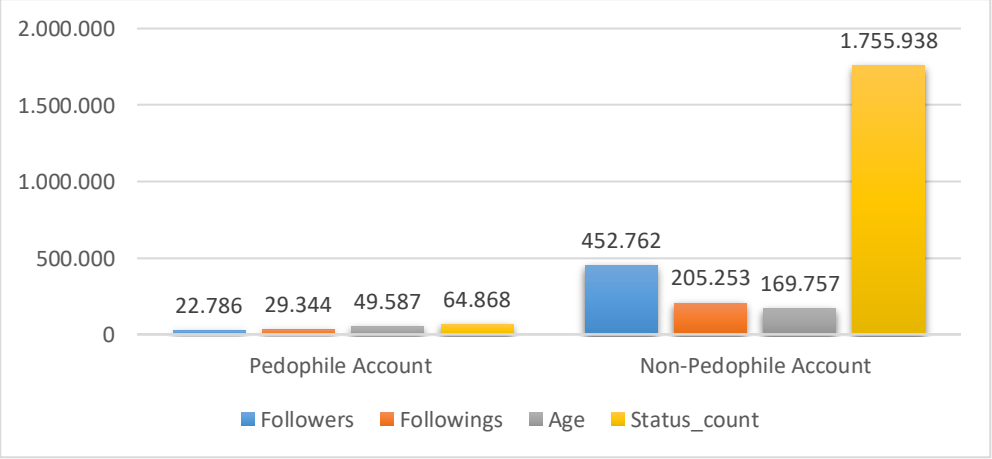

Figure IV.4 Comparison of the Proportion of Total Followers, Followings, Age, and Status_count on Account Based

In Figure IV.4, you can see a comparison of the proportion of the total number of attributes on the pedophile account, namely the followers attribute of 22,786 followers while the non-pedophile account has a total of 452,762 followers. The followings attribute the pedophile account was 29,344, while on the non-pedophile account the total was 205,253 followings. Then for the age attribute account, there is also a very significant difference, the proportion of the total age on the pedophile account is 49,587 days while the non-pedophile account is 169,757 days. The status_count attribute for pedophile accounts was 64,868, while for non-pedophile accounts there were 1,755,938 statuses. Overall, it can be seen that it is significant that the pedophile accounts have a smaller nominal proportion than the non-pedophile accounts, so this attribute is quite informative and can be used as a feature for the classification of pedophile and non-pedophile accounts.

In the Id column, the researcher sees that the Id attribute is a unique number of an account so that it is not representative and the researcher has not used it as a differentiator. Furthermore, the researcher also conducted an analysis on the Datetime_ms (posting time) attribute in the research data grouping based on the frequency of posting times per month which can be seen in Figure IV.5, but it tends not to be used as a differentiator because the posting pattern of pedophile and non-pedophile accounts is uncertain.

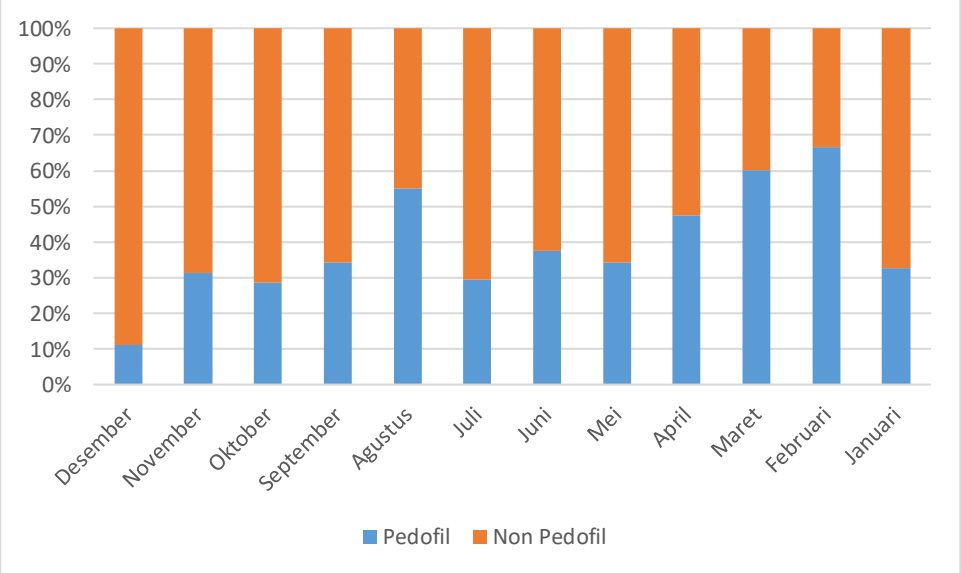

Figure IV.5 Attribute Proportion Number of Posts / Month

Then in the UserSN attribute (user name), the researcher saw the tendency of anonymous account names in the form of a combination of letters and numbers on pedophile and non-pedophile accounts so that it was difficult to distinguish, researchers did not use the UserSN column as a feature in this study. In the user description (biographical) attribute of the pedophile and non-pedophile accounts, because almost 30% of the accounts do not include biographies and there is little information content that has meaning in the biographical text, so it is less informative, descriptive comparisons are shown in table IV.5. This research does not use UserSN and User Description columns as features.

Table IV.5 Comparison of User Description

Authors	User Description
	PEDOFIL
marnodisuratno	ipa ips
yudiz913	biarlah tersakiti yang penting kamu bahagia
CyFrendi	Kekasih gelapmu
Salsabi44429423	nyenyenyenye
AriantoPd	Selalu disini
	NON-PEDOFIL
dustbutcomfy	hust... diem diem aja yaaa gantenk😉
pilumembiiru	Suka nongkrong di @unionsenayan
Dickneyprincess	BI || cnxsaxmc || a masked emperor
jakarta12344	Chub | FWB
Alien_Loku	♈ | alTer | 1% hooman 99% elyen | space enthusiast

IV.3.2 Data Processing on Content Based

At the data processing stage on account based, the researcher chose 3 attributes for content-based data preprocessing.

Data Cleaning, before the text preprocessing stage the researcher conducted an analysis of the content attributes. In this process the researchers used the ms-excel and python tools. The first time the researcher combined the entire contents of the tweets on the content attribute belonging to each account because the data on ms-excel was not yet structured.

```
def convertDatasetToDict(dtf):
  data = {}
  for i, sn in enumerate(dtf['user.screen_name']):
    if sn not in list(data):
      data[sn] = {'content': []}
    data[sn]['content'].append(dtf['content'][i])
```

Figure IV.6 Snippet of Combining Words in Content Attributes Using Python Syntax

In Figure IV.6, it can be seen how researchers combine unstructured tweets from crawled data so that they can become a structured part. The researcher created a data variable that had a Dictionary value, then looped the user.screen_name and content attributes. So that we get the output of the word content in the tweets that have been joined from each account.

Table IV.6 Table of Word Content in Content Attributes

Content	Author
RT @ketekcowo1: #217 Username : @AnggakrwAngga Role: #gaysmp Top Ukuran: 16-17 Umur: 26 Dom: Karawang https://t.co/NAAxyAkTlA	MrHerwa
@RianArjuna20 @PakSyafrizal @AyuAman52490172 @AbahAlatas @andisantoso1538 Kalau sama aku mau ga ? Umur aku masi 16 tahun	Gaybeka34999339
@EmbohAs nyaribtemen seumuran 15 yo kalau ada yg bohong auto blok no 082118372172	ryan12827477
Bot yg free fun yok skrng, ada tempat nih,Cari yg seumuran 17,18 Stay depok #gaylokal #gaybrondong #gaykids… https://t.co/hqYfnJEu1X	Dimas09210231
Yg solo ada gk tg sepantaran umur 15 gtu😊	Rijal82832507

After the word content in the content attributes are combined. With regard to the content of tweets in the content attribute, the term child's age is often found, so that researchers extract numbers but not partially, because the child age limit is someone who is not yet 18 years old (Child Protection Law, 2014) The purpose of extracting this figure is due to a unique pattern of accounts of pedophiles who often use terms indicating children, such as 15 yo (15 years) are shown in Table IV.7. Then with

the split syntax in python the researcher changes from numbers to words, specifically changing numbers 13 to 17. so that it is useful to be a significant differentiator in content attributes.

Table IV.7 Table of Changes in Numbers 13 - 17 into Words in Content Attributes

Before	After
RT @ketekcowo1: #217 Username : @AnggakrwAngga Role: #gaysmp Top Ukuran: 16-17 Umur: 26 Dom: Karawang https://t.co/NAAxyAkTlA	RT @ketekcowo1: #217 Username : @AnggakrwAngga Role: #gaysmp Top Ukuran: enambelas – tujuhbelas Umur: 26 Dom: Karawang https://t.co/NAAxyAkTlA
Yg solo ada gk tg sepantaran umur 15 gtu😊	Yg solo ada gk tg sepantaran umur limabelas gtu😊
@RianArjuna20 @PakSyafrizal @AyuAman52490172 @AbahAlatas @andisantoso1538 Kalau sama aku mau ga ? Umur aku masi 16 tahun	@RianArjuna20 @PakSyafrizal @AyuAman52490172 @AbahAlatas @andisantoso1538 Kalau sama aku mau ga ? Umur aku masi enambelas tahun
Bot yg free fun yok skrng, ada tempat nih,Cari yg seumuran 17,18 Stay depok #gaylokal #gaybrondong #gaykids… https://t.co/hqYfnJEu1X	Bot yg free fun yok skrng, ada tempat nih,Cari yg seumuran tujuhbelas,18 Stay depok #gaylokal #gaybrondong #gaykids… https://t.co/hqYfnJEu1X

Furthermore, researchers calculated the occurrence of relevant words in content attributes (Alvarez, 2019). There is a tendency for the accounts of pedophiles to use hashtags and words with the nuances of child pornography (Gupta et al., 2012). shown in Figure IV.7, the researcher compared the number of unique word occurrences to the data on the pedophile account and the non-pedophile account with the sum function on MS-Excel so that it can be the difference between pedophile and non-pedophile accounts.

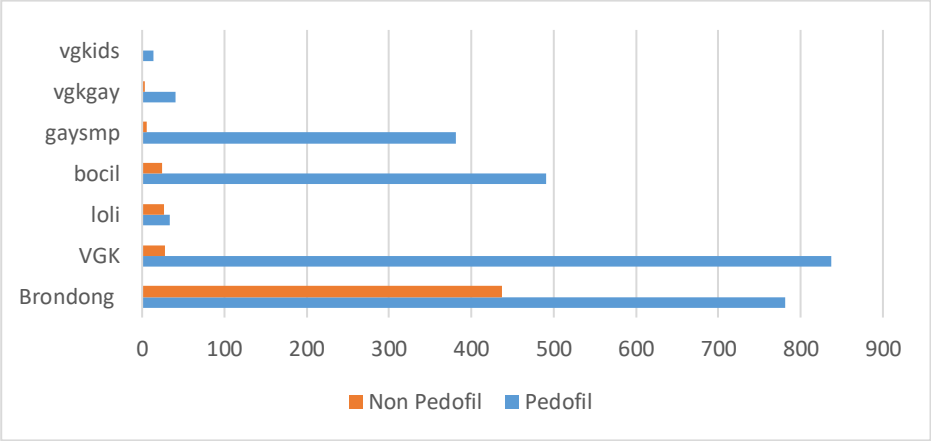

Figure IV.7 Occurrence of Unique Words in Content Attributes

Data Construct, Twitter represents images and videos in the form of URLs, and the assumption of researchers is that all pornographic accounts have posted pornographic images or videos on tweets. So that the researchers extracted the content attributes using the Python regex module to get the URL of the entire tweets of each account. The researcher creates a new column, namely URL_count, which can be seen in Figure IV.8.

B	C
content	url_count
@brendanv	2
@thadashi	1
RT @clipsm	42
Video bigo	2
RT @Massi	66
@AndiUba	1
RT @lokalv	159
RT @rian_s	193
RT @OJOLN	188

Figure IV.8 Total URL Attribute Snippet

Data Integrate, because the data on the content-based dataset is not correlated with data from other datasets and tables, integration with other datasets and tables is not carried out at this stage so that there is no change in the data structure on the content based.

Data Integrate, because the data on the content-based dataset is not correlated with data from other datasets and tables, integration with other datasets and tables is not

carried out at this stage so that there is no change in the data structure on the content based.

The URL_count attribute is a derived attribute of the content attribute, with the proportion of the number of URLs on the pedophile account is 8,786 URLs, while on non-pedophile accounts 19,706 URLs. The ratio of URL appearances on pedophile accounts is 70% smaller than non-pedophile accounts, it is possible that pedophile accounts are closed and only want to be passive connoisseurs of pornographic content, besides that it is possible to avoid the suspicion of child victims of the perpetrator during interactions. The URL_Count attribute will be used as a tool because it is quite informative and can be an account differentiator.

Then for the retweet_count attribute, the content of the tweets shows the popularity of the posts on each account, the more people retweet_count, the more trending the tweet is. The proportion of retweets on pedophile accounts was 235,249 retweets, while on non-pedophile accounts it was 11,678,785 retweets. The comparison of the appearance of retweets on non-pedophile accounts was quite dominating, because on non-pedophile accounts, the perpetrators were looking for popular adult pornographic posts, while on pedophile accounts it was possible that the perpetrators only looked for posts from children which were not popular.

The comparison of the average attribute on content based can be seen in Figure IV.9

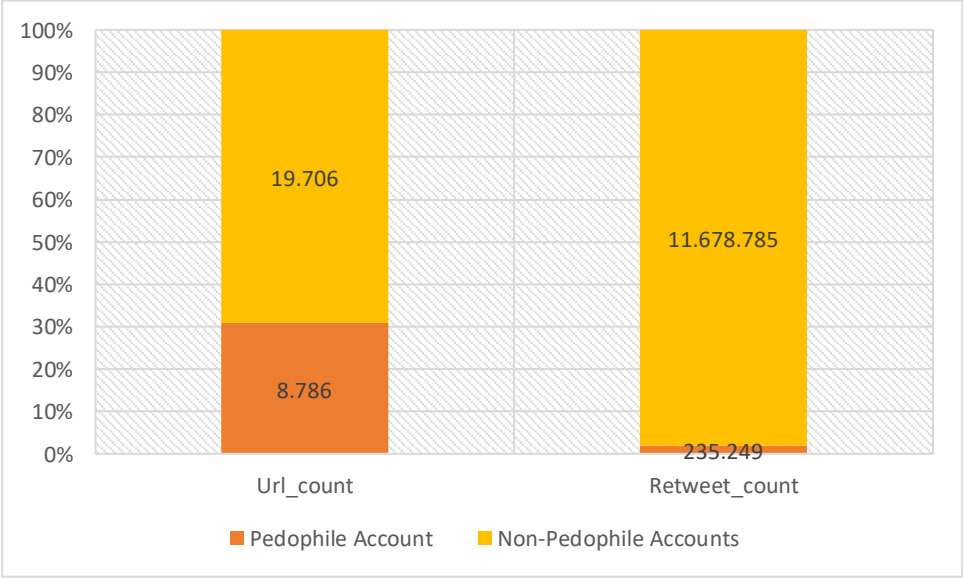

Figure IV.9 Comparison of Proportion of Total Number of URLs and Retweets on Content Based

Text Mining, then in the content sub-attribute, the researcher does simple text mining (Pendar, 2007) with several stages to prepare text into structured data, so that hidden patterns can be seen that can be used for the TF-IDF (Term Frequency-Inverse) weighting process. Document Frequency). Initial input in this process is in the form of complete documents from 338 pedophile accounts of 16,316 tweets and 338 non-pedophile accounts of 52,248 tweets that have gone through the data cleaning stage. In research (Pendar, 2007) the stages of text preprocessing are: case folding, the process of breaking sentences into words (tokenizing), the process of filtering words by changing slang words to their normal form, eliminating stopwords, and the stemming process.

In the case folding process, researchers used python tools to remove text content in tweets in the form of a collection of words such as removing hashtags (#) and mention (@), deleting numbers, removing white space "", deleting punctuation, and deleting multiple letters in all tweets. not required, word changes can be seen in Table IV.8.

Table IV.8 Table of Word Changes on Case Folding

Before	After
@letpeopleenjoy mau doong nyari waria atau bot...	mau dong nyari waria atau bot yg mau nyepong g...
@alvin27622498 @sakurai55305645 https://t.co/7...	oh ya bnr to kok pke kaki oh kok bisa okok cim...
@evilchildh yuk mana yg gondrong ky gini... lg...	yuk mana yg gondrong ky gini lg pgn ngisep nih...
@bukalakap rep @sam_salim1 makane ak pusing mu...	rep salim makane ak pusing mual trus hamil gap...
siang❤ avail serpong yah info rr dm/wa di bio ...	siang avail serpong yah info r dm wa di bio sa...
@BryanPrasetyo4 Mau donk msukin grup #brondong...	mau donk msukin grup brondong kuy colbar kuy m...
@aldijr57 Wa https://webtoon.com aldi manah @T...	wa aldi manah videonya ada ngak sma aldi masuk...
@Gudang_Brondong Vgk 14 kids & bocil 16	brondong vgk kids amp bocil
manga https://t.co/wRI3Ls5zsT sma @mbulanabul ...	manga sma mau bangt cocok smp di mulut ck enak...

Furthermore, in the tokenizing process, researchers used python tools to break sentences into single words, then the words were entered into the list with the aim

of efficiency in the analysis of each word, the word separation can be seen in Table IV.9.

Table IV.9 Table of Word Separation on Tokenizing

Before	After
mau dong nyari waria atau bot yg mau nyepong g...	[mau, dong, nyari, waria, atau, bot, yg, mau, ...
oh ya bnr to kok pke kaki oh kok bisa okok cim...	[oh, ya, bnr, to, kok, pke, kaki, oh, kok, bis...
yuk mana yg gondrong ky gini lg pgn ngisep nih...	[yuk, mana, yg, gondrong, ky, gini, lg, pgn, n...
rep salim makane ak pusing mual trus hamil gap...	[rep, salim, makane, ak, pusing, mual, trus, h...
siang avail serpong yah info r dm wa di bio sa...	[siang, avail, serpong, yah, info, r, dm, wa, ...
mau donk msukin grup brondong kuy colbar kuy m...	[mau, donk, msukin, grup, brondong, kuy, colba...
wa aldi manah videonya ada ngak sma aldi masuk...	[wa, aldi, manah, videonya, ada, ngak, sma, al...
brondong vgk kids amp bocil	[brondong, vgk, kids, amp, bocil]
manga sma mau bangt cocok smp di mulut ck enak...	[manga, sma, mau, bangt, cocok, smp, di, mulut...

Then in the filtering process the researcher takes important words from the tokenizing results by doing the term frequency. Researchers use python tools for the filtering process, by reading tweets on both pedophile and non-pedophile accounts, then building a dictionary for slang words (Gupta et al., 2012), which is unstructured words converted into structured word forms. The researcher first makes a condition if the word in the token is in the dictionary, then the word will change according to the form of the word in the dictionary. In the slang word dictionary, there are 709 words that have changed, where researchers adopted the pornography corpus in the study (Izzah et al., 2018). examples of word changes are shown in Table IV.10.

Table IV.10 Table of Changes in the Slang Word Dictionary

Before	**After**
skrng	sekarang
flbck	follback
org	orang

apalg	apalagi
elu	kamu
bpleh	boleh
gblk	bodoh
bodo	bodoh
cwk	cewek
cwo	cowok

Furthermore, the researcher also made a dictionary stoplist to remove words that are less important or have no meaning. In Table IV.11, you can see an example of a stoplist which is words that are not descriptive so that the researcher makes a condition if the word is in the dictionary stoplist then the word is discarded (Pendar, 2007). There are 25,094 words in Dictionary stop which are not descriptive or relevant.

Table IV.11 Dictionary Example Table on Stoplist

Word	**Word**	**Word**	**Word**
kritis	baper	dar	buncit
aldi	jos	nyenyak	telen
tmen	power	maksa	ug
ajh	stim	gasken	slm
solusi	point	msuk	glow

Then the researcher did the stemming to return the word to its basic form, the researcher used the Literature module in python which is a stemmer for Indonesian. In this process, the researcher took quite a long time, which was about 2 hours to

process the entire word in the content of the pedophile and non-pedophile account tweets, the results of stemming can be seen in Figure IV.10 and Figure IV.11.

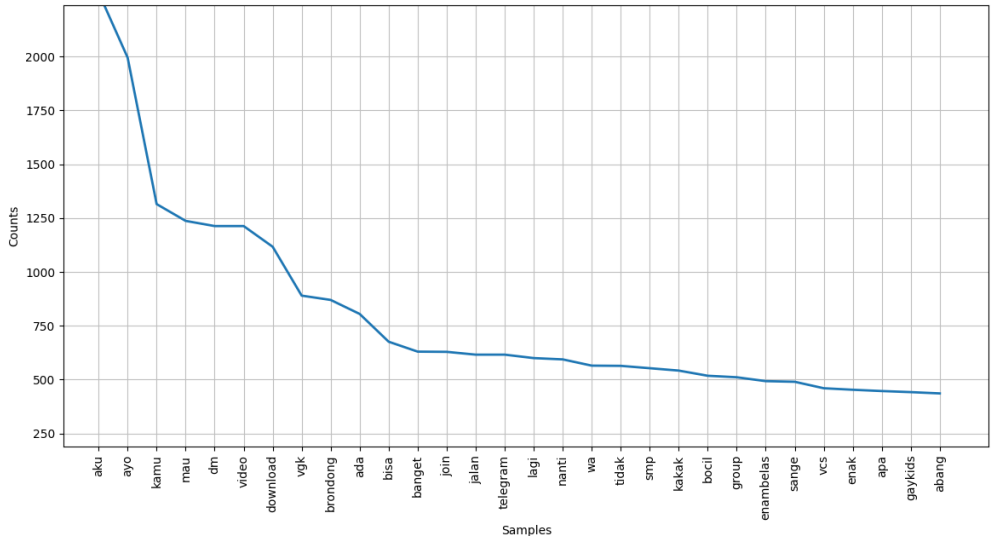

Figure IV.10 Image of Stemming Result on Pedophile Account

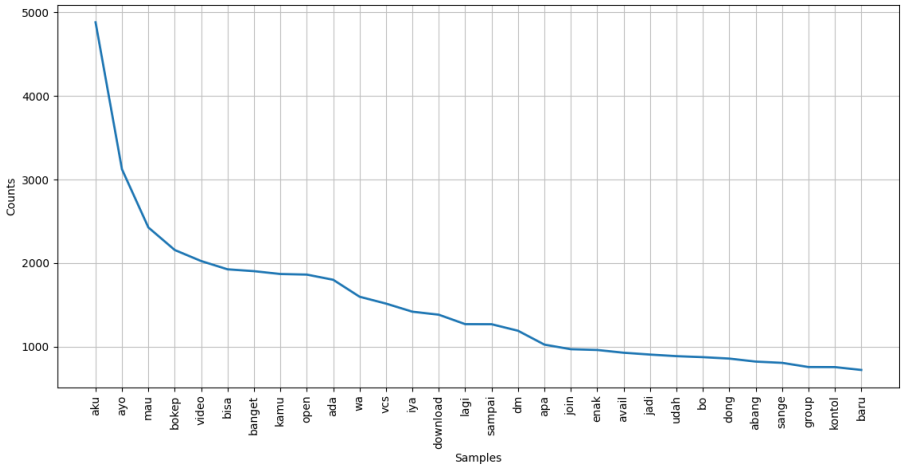

Figure IV.11 Snippet Image of Stemming Results on Non-Pedophile Accounts

IV.3.3 Feature Selection

To meet the goals, namely making a classification model for pedophile and non-pedophile accounts with Machine Learning, the word content in the content attribute that has passed preprocess text needs to be changed from text to numeric form (Pendar, 2007). Then the researcher uses TF-IDF weighting using the vectorizer function and fit transform in the pyhton sklearn module, this parameter

is used to control the size of the vector to be included in the machine learning model, in order to avoid overfitting and improve training efficiency in the model (Xu and Li, 2007) . Furthermore, in calculating the weight value of word occurrences and the accumulative value of each document on 338 pedophile accounts and 338 non-pedophile accounts, the researchers used 200 word vectors in the TF-IDF attribute (Gupta et al., 2012). So that researchers can use it to differentiate between pedophile accounts and non-pedophile accounts.

Furthermore, based on descriptive analysis so that in the Based and content-based accounts the researcher uses seven attributes as features in this research, the feature groups and descriptions are shown in Table IV.12 as follows:

Table IV.12. Table of Feature Taking on Account Based and Content Based

No	Feature Family	Position Features	Description	Information	Type of Data
1.	Status_count	Account Based	Total number of account posts	There are significant differences	Numeric
2.	Age	Account Based	Account Age	There are significant differences	Numeric
3.	Follower_count	Account Based	Amount followed by other accounts	There are significant differences	Numeric
4.	Following_count	Account Based	Amount following other accounts	There are significant differences	Numeric
5.	Retweet_count	Content Based	The number of retweets on account posts	There are significant differences	Numeric
6.	Url_count	Content Based	Number of URLs on account posts	There are significant differences	Numeric
7.	Text	Content Based	TF-IDF weighting on word content in tweets	There is a significant difference in words	Numeric

The researcher then prepared 4 features with numeric type on account based and 2 features with numeric type on account based for the scaling process. In this process, the researcher uses MinMaxScaler in the python sklearn module. feature scaling on numeric attributes is to make numerical data in the dataset have the same range of values, there is no longer one data variable that dominates other data variables. Seen in table IV.13, 6 features that have experienced scale changes, namely follower_count, following_count, status_count, age, url_count, and retweet_count. Then the researcher combines the account-based and content-based data to prepare the data that is ready for use in a machine learning model.

Table IV.13 Scaling Changes on Feature Selection

BEFORE SCALLING					
follower_count	**following_count**	**url_count**	**age**	**retweet_count**	**status_count**
25	32	2	62	0	67
12	139	0	48	0	19
1	13	1	118	0	5
1317	517	7	176	101542	2158
813	728	15	512	54011	5505
AFTER SCALING					
0,000842006	0,005317381	0,005291	0	0	0,000794597
0,000404163	0,023097375	0	0	0	0,000216708
3,36802E-05	0,002160186	0,002646	0	0	4,81574E-05
0,044356876	0,08590894	0,018519	0	0,060111341	0,025968866
0,027382035	0,120970422	0,039683	0,1	0,031973702	0,066264553

IV.3.4 Data Modeling

In the data modeling process, researchers used 5 algorithms in supervised learning, namely Support Vector Machine, Decision Tree, Naïve Bayes, K-Nearest Neighbor, and Random Forest. The dataset will then be divided into two parts as training data and testing data which has a variable ratio of 80:20. In this research, model training will use python in the .fit function of the Sklearn module. Furthermore, with the training data, by calling the shared dataset, it is hoped that the model will be able to identify pedophile and non-pedophile accounts quickly and accurately. Data modeling can be seen in Figure IV.12.

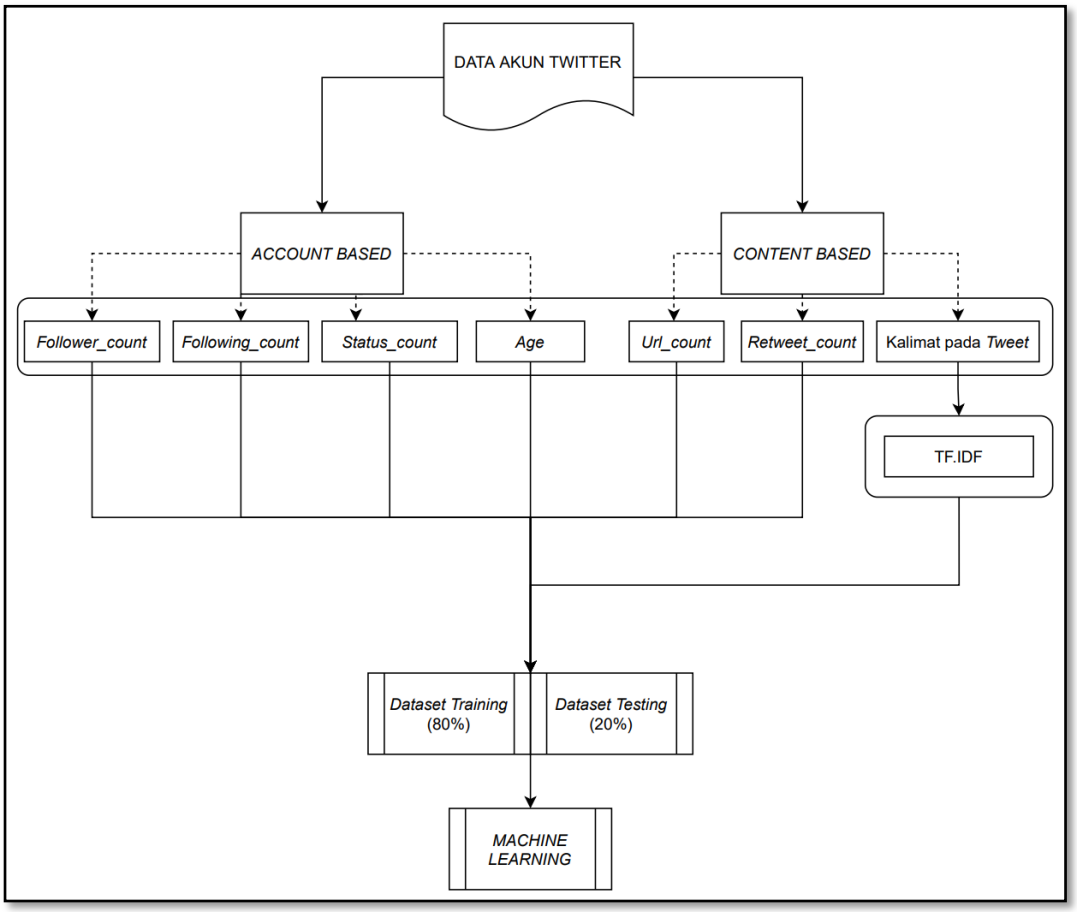

Figure IV.12 Modeling Classification of Pedophile Accounts and Non-Pedophile Accounts

IV.4 Data Testing Phase

To prepare an optimal model for machine learning, researchers used GridSearchCV which is a hyperparameter function in the python sklearn module. GridSearchCV can help search for the best parameters based on the algorithm and training data used (Syarif et al., 2016). The model training process in the Machine Learning algorithm will be accompanied by model optimization. It aims to get the best learning results from each Machine Learning algorithm. GridSearchCV is also used, by determining the cross validation strategy through hyperparameters that have adjusted the training set model.

Table IV.14 Optimization of Five Algorithms with GridSearchCV

Support Vector Machine	
Hyperparameter	Value
C	52
gamma	0.01
Naïve Bayes	
Hyperparameter	Value
var_smoothing	1,00E-14
Decision Tree	
Hyperparameter	Value
criterion	gini
max_depth	2
K-Nearest Neigbours	
Hyperparameter	Value
n_neighbours	12
weights	distance
Random Forest	
Hyperparameter	Value
criterion	entropy
max_depth	12
max_features	auto
n_estimators	33

Seen in table IV.14, the best parameter search results for each model in the machine learning algorithm. Shows the best hyperparameter in the support vector machine algorithm by using C = 52 and gamma = 0.01 to control errors. Then in the decision tree algorithm, the criterion parameters used are gini to measure the split quality and max_depth = 2 to measure the tree depth. Furthermore, in the K-nearest neighbors algorithm, the parameter n_neighbors = 12 which means that it will look for the value of K = 12 closest neighbors and weights = distance, which means that the distance of the neighbors that are closer to the query point will have a greater influence than those that are further away. Then in the Naïve Bayes algorithm, the parameter var_smoothing = 1.00E-14 is used to calculate the largest variant of each feature. Furthermore, in the Random Forest algorithm, the criterion parameter used is entropy to measure the quality of the split and max_depth = 12, with max_features auto at n_estimator = 33 to measure tree depth.

IV.5 Data Evaluation Phase

After obtaining the optimal parameters for each algorithm, these parameters are then used to perform model testing. In the configuration matrix, the test data used is data as much as 20% of the total sample. The test data is data that has never been recognized by the previous model, so that it can really test the quality of the model. Then the test data, namely the data for each iteration selected randomly, the output of the configuration matrix from the model is True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) as follows:

Figure IV.13 Testing Support Vector Machine

It can be seen from Figure IV.13, in testing the SVM algorithm, this model has an accuracy value of 96.32% for identifying pedophile and non-pedophile accounts. The classification results show that the optimal model with variables c = 52 and gamma 0.01 is able to predict 56 pedophile accounts and 75 non-pedophile accounts without detecting errors. Meanwhile, there are 5 false negative accounts.

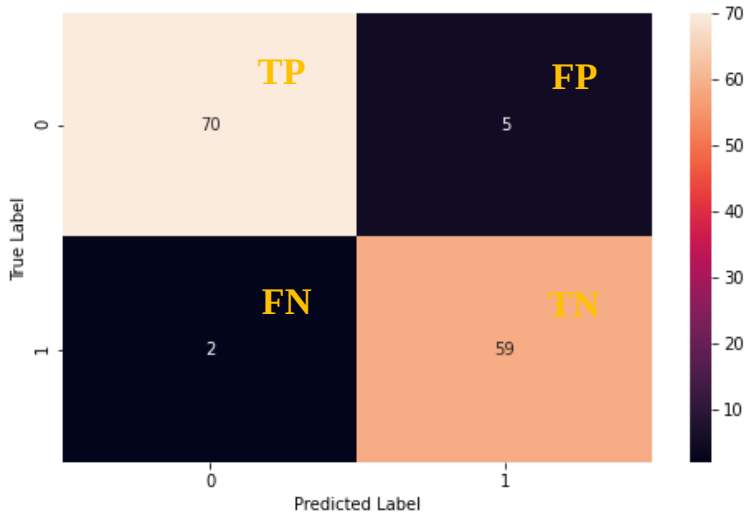

Figure IV.14 Naïve Bayes Testing

It can be seen from Figure IV.14, in testing the Naïve Bayes algorithm, this model has an accuracy value of 94.85% to identify pedophile and non-pedophile accounts. The classification results show that the optimal model with the variable var_smoothing = 1.00e-12 is able to predict 59 accounts of pedophiles and 70 non-pedophile accounts. Whereas on the pedophile accounts there were 2 false negative accounts and 5 false positive accounts on the non-pedophile accounts.

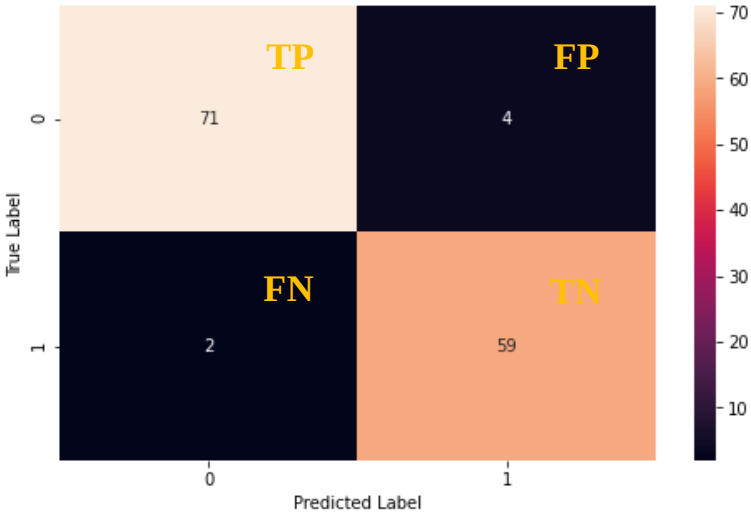

Figure IV.15 Decision Tree Testing

It can be seen from Figure IV.15, on the Decision Tree algorithm test, this model has an accuracy value of 95.59% to identify pedophile and non-pedophile account data. The classification results show that the optimal model with criterion = gini at max-depth = 7 is able to predict 59 pedophile accounts and 71 non-pedophile accounts. Meanwhile, there were 2 false negative accounts and 4 false positive accounts for non-pedophile accounts.

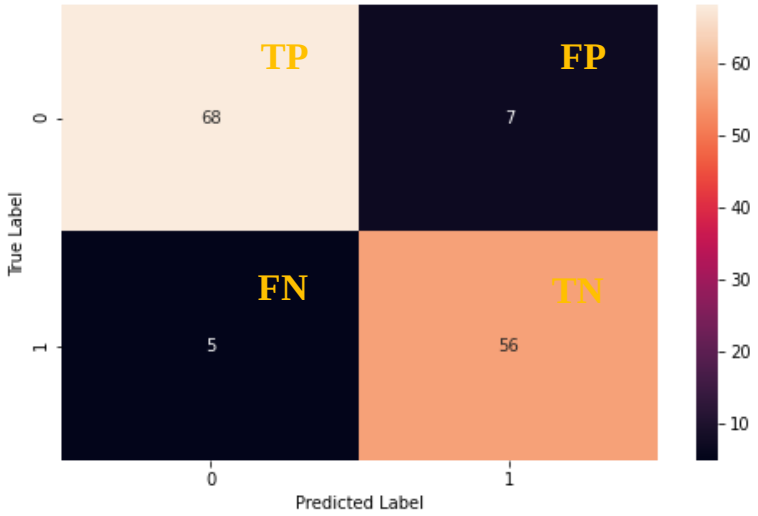

Figure IV.16 Testing of K-nearest neighbors

Seen from Figure IV.16, in testing the K-nearest neighbors algorithm, this model has an accuracy value of 91.18% for identifying pedophile and non-pedophile accounts. The classification results show that the optimal model with n_neighbour = 8 and weight = distance is able to predict 56 pedophile accounts and 68 non-pedophile accounts. Meanwhile, false negative 5 accounts and false positive 7 accounts for non-pedophile accounts.

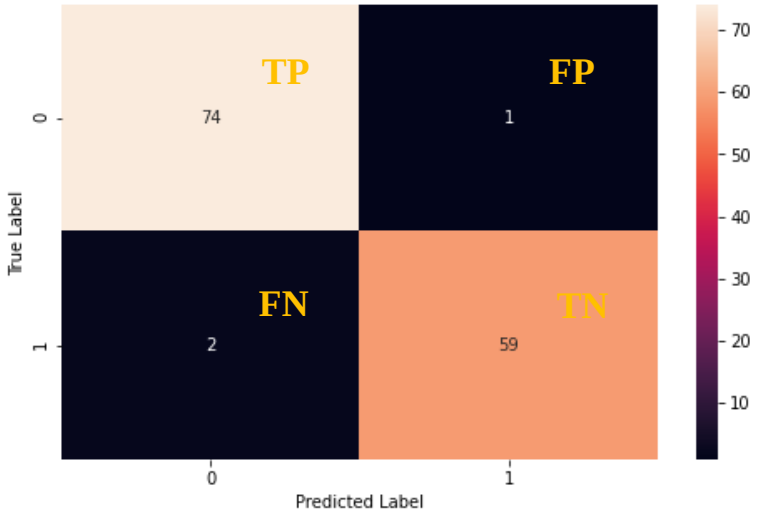

Figure IV.17 Random Forest Testing

Seen in Figure IV.17, the Random Forest algorithm, this model has an accuracy value of 97.79% to identify pedophile and non-pedophile account data. The classification results show that the optimal model with criterion = gini variable at max_depth = 11, max_features = auto on n_estimators = 41 is able to predict 59 pedophile accounts and 74 non-pedophile accounts. Meanwhile, false negative 2 accounts and false positive 1 account on non-pedophile accounts.

Testing of each algorithm is also carried out using Cross validation. Cross validation is a technique suitable for model testing (Par et al., 2020). In this study, the cross validation used was 10 fold, or 10 iterations. This aims to see the classification accuracy obtained from each of these iterations. The results of CV 10 fold testing are shown in table IV.15

Table IV.15 Test Results of Cross Validation 10 Fold

	Iteration 1	Iteration 2	Iteration 3	Iteration 4	Iteration 5	Iteration 6	Iteration 7	Iteration 8	Iteration 9	Iteration 10
Support Vector Machine	0,97	0.82	0,91	0,98	1.	0,95	0,98	1	0,92	0,95

Naïve Bayes	0,94	0,92	0,97	0,97	1	0,86	0,94	0,92	0,95	0,97
Decision Tree	0,94	0,98	0,97	1	1	0,88	0,92	0,97	0,91	0,97
Kneigbours Classifier	0,91	0,75	0,80	0,89	0,89	0,85	0,88	0,95	0,86	0,94
Random Forest Classifier	1	0,94	1	0,97	1	0,91	0,98	0,97	0,97	0,98

In the SVM algorithm, the best accuracy is 1 in the 5th and 8th iterations, while the lowest accuracy is in the 2nd iteration, which is 0.82.

In the Naïve Bayes algorithm, the best accuracy is 1 in the 5th iteration, while the lowest accuracy is in the 6th iteration, which is 0.86.

In the Decision Tree algorithm the best accuracy is 1 in the 4th and 5th iterations, while the lowest accuracy is in the 6th iteration, which is 0.88.

In the KNN algorithm, the best accuracy is 0.95 in the 8th iteration, while the lowest accuracy is in the second iteration, which is 0.75.

In the Random Forest algorithm, the best accuracy is 1 in the 1st, 3rd and 5th iterations, while the lowest accuracy is in the 6th iteration, which is 0.91.

IV.5.1 Analysis of Test results

Based on table IV.16, in general it can be seen that the highest accuracy value is 97.79% using the Random Forest algorithm, and the lowest is 91.18% with the KNN algorithm. Then for the highest precision is 100% with the SVM method and the lowest is 88.89% with the KNN method. Furthermore, the highest recall was Naïve Bayes, Decision Tree, Random Forest with 96.72%, while the lowest was

KNN and SVM with 91.80%. Then for the highest F1-score using the Random Forest method, namely 97.52% and the lowest is 90.32% with the KNN method. Seen in Figure IV.18, the results of the prediction model configuration matrix test in the Random Forest algorithm outperform other algorithms, namely with a precision of 98.33%, Recall 96.72%, F1-score 97.52%, and 97.79% accuracy.

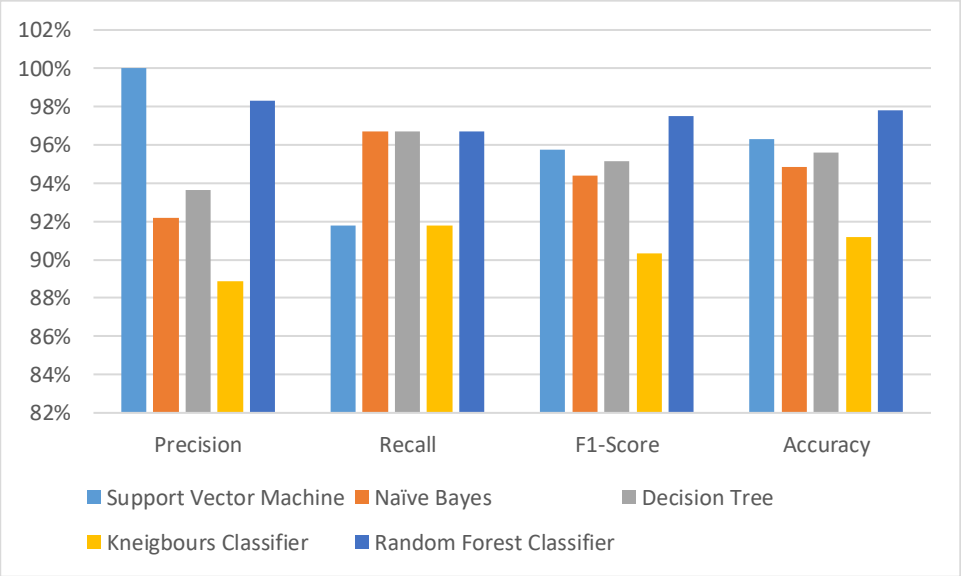

Figure IV.18 Comparison of Five Machine Learning Algorithms in Confusion Matrix

Furthermore, in testing with cross validation of 10 folds, it can be seen in Figure IV.19 that the highest accuracy achieved by the Random Forest method is 97.33% and the lowest is with the KNN method 87.59%. Then there are 4 algorithms that produce the best accuracy in the 5th iteration, namely SVM, Naïve Bayes, Decision Tree and Random Forest.

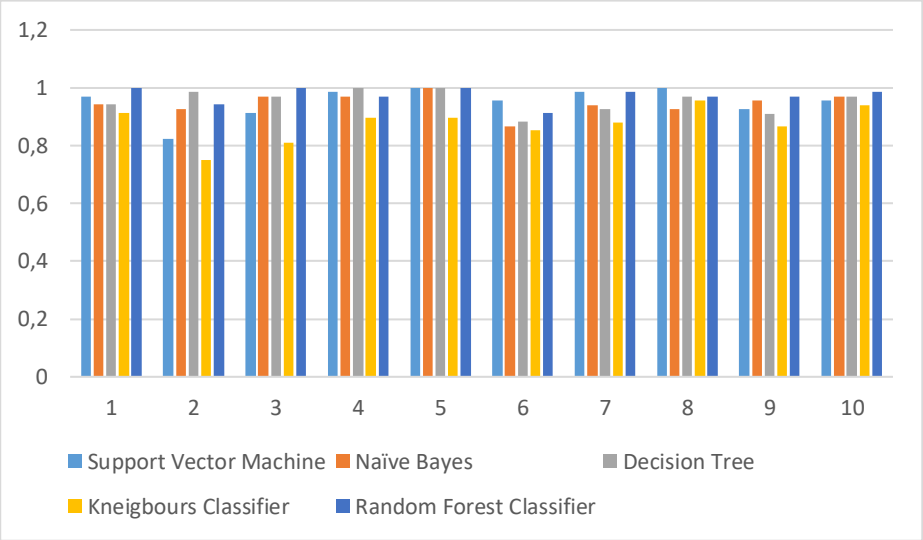

Figure IV.19 Comparison of Five Machine Learning Algorithms on CV 10 Folds

Table IV.16 Comparison of Confusion Matrix and Cross Validation Results 10 folds

Algoritma	*Accuracy* CV 10 *folds*	*Confussion Matrix*			
		Precision	*Recall*	*F1-score*	*Accuracy*
Support Vector Machine	95,12%	100%	91,80%	95,73%	96,32%
Naïve Bayes	94,67%	92,19%	96,72%	94,40%	94,85%
Decision Tree	95,55%	93,65%	96,72%	95,16%	95,59%
Kneigbours Classifier	87,59%	88,89%	91,80%	90,32%	91,18%
Random Forest Classifier	97,33%	98,33%	96,72%	97,52%	97,79%

IV.6 Deployment Phase

In the last phase, namely the Deployment Process, by using a model that has been formed using python tools, the researcher returns to the test using new data from pornographic tweets that have been determined by the expert, to test the validity of the classification results. Then the researchers did realtime crawling of 60 accounts consisting of 30 pedophile accounts and 30 non-pedophile accounts. Researchers used five machine learning algorithms including SVM, Naïve Bayes, Decision Tree, KNearest Neighbor, and Random Forest. It can be seen in table IV.17 that the Random Forest Algorithm performs the best predictions compared to the other 4 algorithms.

Table IV.17 Comparison of Model Testing with New Data

	Pedophile		Non-Pedophile	
NB	Right	Wrong	Right	Wrong
	27	3	29	1
DT	Pedophile		Non-Pedophile	
	Right	Wrong	Right	Wrong
	26	4	29	1
RF	Pedophile		Non-Pedophile	
	Right	Wrong	Right	Wrong
	29	1	29	1
SVM	Pedophile		Non-Pedophile	
	Right	Wrong	Right	Wrong
	16	14	29	1
KNN	Pedophile		Non-Pedophile	
	Right	Wrong	Right	Wrong
	16	14	29	1

Chapter V Closing

V.1 Conclusion

1. In this study, the model can predict pedophile accounts and non-pedophile accounts on the 80:20 performance variable using the status_count, following, follower, age, url_count, retweet_count, and 200 vector words features.

2. The Random Forest algorithm predicts the best among the other four algorithms with an F1-score level of 97.79%.

3. The model that has been deployed to detect unrecognized accounts of pornographic tweets on the Twitter platform uses new data, namely 60 accounts consisting of 30 pedophile accounts and 30 non-pedophile accounts. The Random Forest algorithm predicts 58 true and 2 false accounts. So that this modeling can be used to identify pedophile accounts according to end user needs.

V.2 Advice

1. It is necessary to develop a model using test data from other social media platforms to test the performance of the detection model on the accounts of pedophiles.
2. It is necessary to carry out further testing using the word feature extraction technique to get better testing accuracy.
3. It is necessary to build a model utilizing friendship attributes using graph based to perform community detection.

REFERENCES

Abozinadah, E., Mbaziira, A., Dan Jr, J. (2015): Detection Of Abusive Accounts With Arabic Tweets, Dipresentasikan Pada International Journal Of Knowledge Engineering-Iacsit, **1**. Https://Doi.Org/10.7763/Ijke.2015.V1.19

Alodia, D., Lie, J., Dan Anggreini, V. (2019): Kejahatan Pedofilia Sebagai Perilaku Menyimpang Dan Upaya Penegakan Hukumnya, *Jurnal Muara Ilmu Sosial, Humaniora, Dan Seni*, **2**, 534. Https://Doi.Org/10.24912/Jmishumsen.V2i2.1060

Alvarez, M. (2019): *Detection Of Possible Human Trafficking In Twitter*, 191, 187. Https://Doi.Org/10.1109/Ici2st.2019.00034

Belbeze, C., Chavalarias, D., Denoyer, L., Fournier, R., Guillaume, J.-L., Latapy, M., Magnien, C., Valadon, G., Vehovar, V., Dan Žiberna, A. (2009): Automatic Identification Of Paedophile Keywords, *Measurements And Analysis Of P2p Activity Against Paedophile Content Project*.

Berry, M. W., Dan Kogan, J. (2010): *Text Mining: Applications And Theory*. Https://Doi.Org/10.1002/9780470689646

Bhowmik, R. (2008): Data Mining Techniques In Fraud Detection, *Journal Of Digital Forensics, Security And Law*. Https://Doi.Org/10.15394/Jdfsl.2008.1040

Chapman, C., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., Dan Wirth, R. (2000): *Crisp-Dm 1.0*.

Ditsiber Bareskrim Polri, B. (2019): Statistik Tindak Pidana Siber, Dittipidsiber Bareskrim Polri.

Durkin, K. (1997): Misuse Of The Internet By Pedophiles: Implications For Law Enforcement And Probation Practice, *Federal Probation*, **61**, 14–18.

Fournier, R., Dan Danisch, M. (2014): Mining Bipartite Graphs To Improve Semantic Pedophile Activity Detection, *2014 Ieee Eighth International Conference On Research Challenges In Information Science (Rcis)*, 1–4. Https://Doi.Org/10.1109/Rcis.2014.6861035

Gheewala, S., Dan Patel, R. (2018): Machine Learning Based Twitter Spam Account Detection: A Review, 79–84. Https://Doi.Org/10.1109/Iccmc.2018.8487992

Gupta, A., Kumaraguru, P., Dan Sureka, A. (2012): Characterizing Pedophile Conversations On The Internet Using Online Grooming, *Arxiv:1208.4324 [Cs]*, Diperoleh 7 Februari 2021melalui Situs Internet: Http://Arxiv.Org/Abs/1208.4324.

Han, J., Kamber, M., Dan Pei, J. (2012): *Data Mining: Concepts And Techniques*. Https://Doi.Org/10.1016/C2009-0-61819-5

Headline: Kasus Pedofilia Kian Marak, Saatnya Pelaku Dikebiri? - News Liputan6.Com. (2018): , Diperoleh 22 Januari 2021, Melalui Situs Internet: Https://Www.Liputan6.Com/News/Read/3216893/Headline-Kasus-Pedofilia-Kian-Marak-Saatnya-Pelaku-Dikebiri.

Izzah, N., Budi, I., Dan Louvan, S. (2018): Classification Of Pornographic Content On Twitter Using Support Vector Machine And Naive Bayes, *2018 4th International Conference On Computer And Technology Applications (Iccta)*, 156–160. Https://Doi.Org/10.1109/Cata.2018.8398674

Kemenkominfo, P. (2014): Siaran Pers No. 17/Pih/Kominfo/2/2014 Tentang Riset Kominfo Dan Unicef Mengenai Perilaku Anak Dan Remaja Dalam Menggunakan Internet, , Diperoleh 2 Februari 2021, Melalui Situs Internet: Http:///Content/Detail/3834/Siaran-Pers-No-17pihkominfo22014-Tentang-Riset-Kominfo-Dan-Unicef-Mengenai-Perilaku-Anak-Dan-Remaja-Dalam-Menggunakan-Internet/0/Siaran_Pers.

Kustoni, D. (2019): Kejahatan Pedofil Tahun 2019 Pada Direktorat Siber.

Larose, D. T. (2014): Discovering Knowledge In Data : An Introduction To Data Mining.New Jersey: John Wiley & Sons, Inc.

Mustaqhfiri, M., Abidin, Z., Dan Kusumawati, R. (2012): Peringkasan Teks Otomatis Berita Berbahasa Indonesia Menggunajan Metode Maximum Marginal Relevance, *Matics*. Https://Doi.Org/10.18860/Mat.V0i0.1578

Nur Rosyidah, F., Dan Nurdin, M. (2018): Media Sosial: Ruang Baru Dalam Tindak Pelecehan Seksual Remaja, *Sosioglobal : Jurnal Pemikiran Dan Penelitian Sosiologi*, **2**, 38. Https://Doi.Org/10.24198/Jsg.V2i2.17200

Par, Ö. E., Sezer, E. A., Sever, H., Dan Üniversitesi, Ç. (2020): Sınıflandırmada Küçük Ve Dengesiz Veri Kümesi Problemi Small And Unbalanced Data Set Problem In Classification, 4.

Pendar, N. (2007): Toward Spotting The Pedophile Telling Victim From Predator In Text Chats, *International Conference On Semantic Computing (Icsc 2007)*, 235–241. Https://Doi.Org/10.1109/Icsc.2007.32

Probosiwi, R., Dan Bahransyaf, D. (2015): Pedofilia Dan Kekerasan Seksual: Masalah Dan Perlindungan Terhadap Anak, *Sosio Informa*, **1**(1). Https://Doi.Org/10.33007/Inf.V1i1.88

Saputra, P. (2017): Implementasi Teknik Crawling Untuk Pengumpulan Data Dari Media Sosial Twitter, , Diperoleh 21 Januari 2021, Melalui Situs Internet: /Paper/Implementasi-Teknik-Crawling-Untuk-Pengumpulan-Data-Saputra/Ee504fc50df223bbeacae0aed4430ae213b33a37.

Syarif, I., Prugel-Bennett, A., Dan Wills, G. (2016): Svm Parameter Optimization Using Grid Search And Genetic Algorithm To Improve Classification Performance, *Telkomnika (Telecommunication Computing Electronics And Control)*, **14**(4), 1502. Https://Doi.Org/10.12928/Telkomnika.V14i4.3956

Uddin, M., Imran, M., Dan Sajjad, H. (2014): Understanding Types Of Users On Twitter.

United Nations Congress (2000): *Report Of The Tenth United Nations Congress On The Prevention Of Crime And The Treatment Of Offenders* (Congress Report Tenth United Nations Congress On The Prevention Of Crime And The Treatment Of Offenders Vienna), United Nations, Vienna Austria, Diperoleh Melalui Situs Internet: Https://Digitallibrary.Un.Org/Record/404748?Ln=En, 46.

Uu Ite (2016): *Undang-Undang Republik Indonesia Nomor 9 Tahun 2016 Tentang Perubahan Atas Uu Ite Nomor 11 Tahun 2008*.

Uu Perlindungan Anak (2014): *Undang-Undang Republik Indonesia Nomor 35 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2002 Tentang Perlindungan Anak*.

Uu Pornografi (2008): Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 Tentang Pornografi.

Wearesocial.Com (2019): Hootsuite Wearesocialindonesiandigitalreport 2019.

Xu, H., Dan Li, C. (2007): A Novel Term Weighting Scheme For Automated Text Categorization, *Seventh International Conference On Intelligent Systems Design And Applications (Isda 2007)*, 759–764. Https://Doi.Org/10.1109/Isda.2007.26

APPENDIX

Appendix A Cyber Crime Statistics 2015-2019

NO	JENIS KEJAHATAN	2015			2016			2017			2018			2019		
		CT	CC	%	CT	CC	%	CT	CC	%	CT	CC	%	CT	CC	%
1	BERITA BOHONG / BERITA PALSU	0	0	0	0	0	0	15	8	53,3	60	23	38,3	97	69	71,1
2	PORNOGRAFI	135	46	34,1	155	55	35,5	180	97	53,9	266	123	46,2	364	144	39,6
3	PERJUDIAN	16	14	87,5	26	19	73,1	24	12	50,0	35	24	68,6	35	20	57,1
4	PENCEMARAN NAMA BAIK	588	146	24,8	848	232	27,4	886	375	42,3	1258	593	47,1	1333	597	44,8
5	PEMERASAN	18	11	61,1	17	3	17,6	22	6	27,3	36	18	50,0	132	58	43,9
6	PENIPUAN	1494	347	23,2	1570	465	29,6	1430	802	56,1	1781	1030	57,8	1617	966	59,7
7	UJARAN KEBENCIAN / SARA	37	3	8,1	91	14	15,4	124	74	59,7	238	104	43,7	247	88	35,6
8	PENGANCAMAN	90	13	14,4	108	28	25,9	132	60	45,5	168	85	50,6	92	33	35,9
9	AKSES ILEGAL	107	17	15,9	147	34	23,1	153	73	47,7	263	138	52,5	248	91	36,7
10	PENCURIAN DATA / IDENTITAS	49	14	28,6	20	3	15,0	47	27	57,4	88	44	50,0	143	75	52,4
11	PERETASAN SISTEM ELEKTRONIK	0	0	0,0	0	0	0,0	35	21	60,0	43	26	60,5	148	82	55,4
12	INTERSEPSI ILEGAL	7	2	28,6	15	5	33,3	10	6	60,0	5	3	60,0	3	3	100,0
13	PENGUBAHAN TAMPILAN SITUS	27	6	22,2	42	10	23,8	5	0	0,0	5	0	0,0	4	2	50,0
14	GANGGUAN SISTEM / DDOS	41	5	12,2	71	40	56,3	13	3	23,1	1	1	100,0	9	3	33,3
15	MANIPULASI DATA	0	0	0,0	0	0	0,0	33	46	139,4	113	61	54,0	114	51	44,7
TOTAL		2609	624	23,9	3110	908	29,2	3109	1610	51,8	4360	2273	52,1	4586	2282	49,8

2019 NCMEC Report Data

Social Media Platform	Number of Pedophile Accounts
Facebook	1703 Accounts
Instagram	1542 Accounts
Twitter	3051 Accounts

Appendix B. Interview with Kasubdit I Dittipidsiber Bareskrim Polri

Topic: Online Pornography Crimes on Cybercrime

Date: 21 November 2020

Place: Office of the Directorate of Criminal and Criminal Investigation of the National Police.

No	**Interview Transcript**	
1.	Question	Do you, as the representative of the Head of Sub-Directorate I of the Directorate of Cyber Crime, wish us to interview?
	Answer	Yes, I am willing.
2.	Question	What is the responsibility of the Director in the organizational structure of the National Police Criminal Investigation Directorate for Cybercrime?
	Answer	Based on the Chief of Police Regulation Number 6 of 2017, Attachment XVIII, the Head of Sub-Directorate I is responsible to the Director of Cyber Crime and the Head of Criminal Investigation of the Police as the legal superior. In addition, the Head of Sub-Directorate I is in charge of carrying out investigations and investigations of special crimes related to cyber crimes, information crimes and electronic transactions, telecommunications crimes including transnational crimes related to cyber crimes and formulating policies in the context of investigating and investigating cyber crimes.
3.	Question	What is the Vision and Mission of the Directorate of Cyber Crime, Bareskrim Polri?
	Answer	The vision of the Directorate of Cyber Crime at the National Police Criminal Investigation Unit is to become the foremost unit in carrying out the task of investigating and investigating crimes that occur in electronic devices and / or crimes committed through misuse of information technology, as well as in providing technical support for investigations and investigations for the unit. Other Polri. Missions: 1. Increase the ability of personnel and equipment in supporting the carrying out of investigative, investigative and examination

		tasks on digital evidence related to crimes against electronic devices and / or misuse of information technology; 2. Empowering collaboration with stakeholders, both inside and outside the National Police, Government and private sector organizations engaged in information technology; 3. Develop digital forensic service methods and other technical support to requesting agencies in a professional, transparent and accountable manner without discrimination; 4. Maintain equipment and infrastructure within the Directorate of Cyber Crime with full responsibility; 5. Improve the capacity of planning and budget functions, including planning for human resource needs, equipment, facilities and infrastructure, as well as planning for financial needs that is transparent and accountable.
4.	Question	How has cyber crime been handled?
	Answer	Handling cyber cases is not as easy as dealing with conventional crimes, because there are theories of locus (place of incident) and tempus (time of incident). In conventional crimes it is clear the time and place of the crime, while in cybercrime the scene and time of the incident must adjust to the internet time and the place where the perpetrator uploads / downloads The indicator for the completion of cyber crime handling is crime clearance or case settlement, we can show in the following statistics the total crime data and crime clearance for the period 2015 to 2019:
5.	Question	What about online pornography crimes?
	Answer	Online pornography crime has experienced an increasing trend every year, since 2015 there were 135 cases, in 2016 there were

NO	JENIS KEJAHATAN	2015			2016			2017			2018	
		CT	CC	%	CT	CC	%	CT	CC	%	CT	CC
1	BERITA BOHONG / BERITA PALSU	0	0	0	0	0	0	15	8	53,3	60	2
2	PORNOGRAFI	135	46	34,1	155	55	35,5	180	97	53,9	266	12
3	PERJUDIAN	16	14	87,5	26	19	73,1	24	12	50,0	35	2
4	PENCEMARAN NAMA BAIK	588	146	24,8	848	232	27,4	886	375	42,3	1258	59
5	PEMERASAN	18	11	61,1	17	3	17,6	22	6	27,3	36	1
6	PENIPUAN	1494	347	23,2	1570	465	29,6	1430	802	56,1	1781	103
7	UJARAN KEBENCIAN / SARA	37	3	8,1	91	14	15,4	124	74	59,7	238	10
8	PENGANCAMAN	90	13	14,4	108	28	25,9	132	60	45,5	168	8
9	AKSES ILEGAL	107	17	15,9	147	34	23,1	153	73	47,7	263	13
10	PENCURIAN DATA / IDENTITAS	49	14	28,6	20	3	15,0	47	27	57,4	88	4
11	PERETASAN SISTEM ELEKTRONIK	0	0	0,0	0	0	0,0	35	21	60,0	43	2
12	INTERSEPSI ILEGAL	7	2	28,6	15	5	33,3	10	6	60,0	5	
13	PENGUBAHAN TAMPILAN SITUS	27	6	22,2	42	10	23,8	5	0	0,0	5	
14	GANGGUAN SISTEM / DDOS	41	5	12,2	71	40	56,3	13	3	23,1	1	
15	MANIPULASI DATA	0	0	0,0	0	0	0,0	33	46	139,4	113	6
TOTAL		2609	624	23,9	3110	908	29,2	3109	1610	51,8	4360	227

<table>
<tr><td></td><td></td><td>155 cases, in 2017 there were 180 cases, in 2018 there were 266 cases, and in 2019 there were 364 cases.
In fighting the crime of online pornography, we collaborate with stakeholders for online pornography cases, at the international level NCMEC (National Center of Missing Exploited Children), Interpol, while at the national level including ECPAT (End Child Prostitution, Child Pornography, and Traficking) Indonesia, KPAI (Indonesian Child Protection Commission), as well as the Ministry of Women and Child Empowerment.
Then based on the NCMEC report we received, social media became a gathering place for pedophiles and carried out their actions, even throughout 2019 we received many reports of pedophile accounts, but we were constrained by the condition of the account that had been suspended so we could not collect real-time evidence. Because based on Article 184 of the Criminal Code, there are 5 valid evidence with due regard to the locus delictie and tempus delictie. Following are the details of the 2019 NCMEC report
<table>
<tr><th>Social Media Platform</th><th>Number of Pedophile Accounts</th></tr>
<tr><td>Facebook</td><td>1703</td></tr>
<tr><td>Instagram</td><td>1542</td></tr>
<tr><td>Twitter</td><td>3051</td></tr>
</table>
</td></tr>
<tr><td>6.</td><td>Question</td><td>What about victims of online pornography crimes?</td></tr>
<tr><td></td><td>Answer</td><td>In online pornography crimes, there are two types of victims, namely Adults and Children. Then we also categorized the perpetrators of online pornography crimes based on the incidents we had disclosed, for example:
Human trafficking: offenders peddling themselves as objects of pornography then posting vital parts of their bodies as triggers to find consumers, or pimps peddling naughty women, usually they used to act on the roadside / nightclub now switch to using the internet (Perpetrator = adult, victim = adults);
Pedophile: the perpetrator is an adult who has deviant behavior, that is, sexual orientation towards children in the disguise of</td></tr>
</table>

		being a teacher to trick the victim, who is a vulnerable group. Usually the perpetrators of this type have carried out social engineering to find their victims. (Perpetrators = adults, victims = children). Spam Pornography: perpetrators offer pornography services through phishing / email attachments to generate other crimes such as malware. Usually this type of perpetrator is already targeting potential victims. (Perpetrator = adult, victim = adult).
7.	Question	What are the details of the crime with the type of pedophile offender?
	Answer	Some cases of pedophilia that have occurred in Indonesia and which have attracted the attention of the public at large include: 6. In 2014, a pedophile perpetrator was arrested by the Criminal Investigation Unit of the Police in Surabaya, for distributing ten thousand pornographic photos of minors, through the Facebook media under the guise of a teenager reproductive health doctor then asking the victim to take a picture fully clothed naked, even the victim was asked to masturbate with taken a picture. The number of child victims who were identified was 12 children. 7. In 2017, eight pedophiles were arrested by Polda Metro Jaya in Jakarta for distributing child pornographic content on the loly candy facebook group and twitter. The number of child victims who were identified was 13 children. 8. In 2018, a pedophile perpetrator was arrested by the Tangerang Police, for spreading child pornography content on Twitter and Facebook. The number of child victims who were identified was 41 children. 9. In 2018, a pedophile perpetrator was arrested by the Jambi Regional Police in Jambi for distributing child pornography content on Instagram and Twitter. The number of child victims who were identified was 87 children. 10. In 2019, a pedophile perpetrator was arrested by the Criminal Investigation Unit of the National Police at the Madura Pamekasan prison for distributing child

<table>
<tr>
<td></td>
<td></td>
<td>pornographic content on google plus media, facebook, and twitter under the guise of a school teacher. The number of child victims who were identified was 50 children.
Throughout 2019, we handled 364 pornography cases. Of the 364 cases, 79 children were identified and the number of pedophile perpetrators were:
<table>
<tr><th>NO</th><th>NO LP</th><th>PERSONNEL</th><th>WITNESS</th><th>VICTIM</th><th>KET</th></tr>
<tr><td>1</td><td>Police Report Number: LP / A / 0XXX</td><td>1 (ADULT)</td><td>6 (ADULT)</td><td>2 (CHILD)</td><td>STEP II</td></tr>
<tr><td>2</td><td>Police Report Number: LP / A / 01XXX</td><td>1 (ADULT)</td><td>13 (ADULT)</td><td>56 (CHILD)</td><td>STEP II</td></tr>
<tr><td>3</td><td>Police Report Number: LP / B / 3XXX</td><td>1 (ADULT)</td><td>4 (ADULT)</td><td>1 (CHILD)</td><td>STEP II</td></tr>
<tr><td>4</td><td>Police Report Number: LP / B / 07XXX</td><td>2 (ADULT)</td><td>10 (ADULT)</td><td>2 (CHILD)</td><td>STEP II</td></tr>
<tr><td>5</td><td>Police Report Number: LP / B / 08XXX</td><td>1 (ADULT)</td><td>2 (ADULT)</td><td>1 (CHILD)</td><td>STEP II</td></tr>
<tr><td>6</td><td>Police Report Number: LP / B / 08XXX</td><td>1 (ADULT)</td><td>4 (ADULT)</td><td>3 (CHILD)</td><td>STEP II</td></tr>
<tr><td>7</td><td>Police Report Number: LP / B / 09XXX</td><td>1 (ADULT)</td><td>3 (ADULT)</td><td>4 (CHILD)</td><td>STEP II</td></tr>
<tr><td>8</td><td>Police Report Number: LP / B / 1XXX</td><td>1 (ADULT)</td><td>5 (ADULT)</td><td>2 (CHILD)</td><td>STEP II</td></tr>
<tr><td>9</td><td>Police Report Number: LP / B / 1XXX</td><td>1 (ADULT)</td><td>5 (ADULT)</td><td>5 (CHILD)</td><td>STEP II</td></tr>
<tr><td>10</td><td>Police Report Number: LP / B / 1XXX</td><td>1 (ADULT)</td><td>6 (ADULT)</td><td>3 (CHILD)</td><td>STEP II</td></tr>
</table>
Of the 10 Police Reports in 2019, 11 were pedophile perpetrators with 79 victims being children. We mark completion of the case with the term Phase II.</td>
</tr>
<tr>
<td>8.</td>
<td>Question</td>
<td>Can you explain the social media that pedophile perpetrators often use, and what do you think about the social media that pedophile perpetrators like the most?</td>
</tr>
<tr>
<td></td>
<td>Answer</td>
<td>In general, it does not rule out the possibility that on all social media there are opportunities for pedophiles to launch their actions. Based on the data we have, namely the 2019 NCMEC report data, there are 360 reports containing 6,000 pedophile accounts from social media twitter.</td>
</tr>
</table>

		In my opinion, the most popular social media for pedophile actors is twitter, because there are many pornographic images and videos. Then many children today who like to play social media, one of which is Twitter.
9.	Question	How do you reduce the number of pedophile offenders in online pornography and are there any obstacles in handling pedophile cases?
	Answer	The actions of law enforcement officials, especially the Police Criminal Investigation Unit, are repressive measures, namely prosecution characterized by forced attempts in the form of arrest, detention, confiscation and search. Along with the government's program to combat online pornography crimes and pedophiles, In 2019 we built an online pornography database with the help of the twitter API. However, the output or action from the analysis on the database has not been optimal so that case disclosure is still minimal, it can be seen in the case resolution indicators in 2019, namely from 364 cases only 144 cases were resolved. The obstacles we face are the lack of resources to analyze the mountains of pornographic data, and the absence of technology for automatic account detection of pedophile offenders.
10	Question	What about penalties for online pornography crimes, especially for pedophiles?
	Answer	Pornography in general according to Law Number 44 of 2008 concerning Pornography (hereinafter in my answer is short the Pornography Law), is pictures, sketches, illustrations, photos, writings, sounds, sounds, moving pictures, animation, cartoons, conversations, motion bodies, or other forms of messages through various forms of communication media and / or public performances, which contain obscenity or sexual exploitation that violates the norms of decency in society. Pornography, briefly is: a. Message (in the form of text, visual and / or audio);

		b. Through various forms of communication media and / or public performances; c. Which includes obscenity or sexual exploitation; d. d. That violates the norms of decency in society. Pornography Products Article 4 paragraph (1) contains: • Intercourse, including sex that is deviant, which includes intercourse or other sexual activity with corpses, animals, oral sex, anal sex, lesbian and homosexuals; • Sexual violence, including sexual intercourse preceded by acts of violence (maltreatment) or forced molestation or rape; • Masturbate or masturbate; • Nudity or the appearance of nudity, which is a condition of a person wearing a body covering but still showing explicit genitals; • Genitals; or • Child pornography, which is all forms of pornography that involve children or that involve adults who act or act like children. Pornography object or model is a person who does or is ordered to do a pornographic condition, position or scene in a pornographic product or service. Article 37 reads: Anyone who involves children in activities and / or as objects as referred to in Article 11 shall be punished with the same penalties as those referred to in Article 29, Article 30, Article 31, Article 32, Article 34, Article 35, and Article 36, plus 1/3 (one third) of the maximum penalty threat. In my opinion, the main elements of Article 37 of the Pornography Law are: a. Everyone, namely individuals or corporations, both legal entities and non-legal entities.

		b. Child, namely someone who is not yet 18 (eighteen) years old. c. Involving, in the context of the form of participation, namely involvement as a maker of help (medeplichtige), maker of advocate (uitlokker), maker of participants (medepleger) or maker of executor (pleger). d. The object (or model) of pornography is a person who does or is instructed to do a pornographic condition, position or scene in a pornographic product or service. e. Pornography crimes, namely pornography crimes as referred to in Article 29 to Article 38 of the Pornography Law. f. Criminal Restriction, namely the addition of 1/3 (one third) of the maximum criminal penalty Article 38 reads: Invite, persuade, take advantage of, condone, abuse power, or force children to use pornographic products or services. Penalties for pedophile offenders are very severe if the person concerned fulfills all the elements, namely: disseminating, offering, selling and buying child pornographic content. maximum criminal limit, namely the threat of life imprisonment and a minimum of 6 years.
11.	Question	What are your hopes for improving case handling for pedophiles?
	Answer	As the leader, of course we want to do our best for the unit of the Dittipidsiber Bareskrim Polri, supported by law enforcement in a fair and transparent manner. We also hope that there will be technology that can automatically detect the accounts of pedophiles on social media platforms, especially Twitter, because at this time we received reports from NCMEC data but the collection of accounts has been suspended, making it difficult for investigators to carry out legal construction for the perpetrators. an example is realtime proof of account existence.

Interview documentation followed by experts on the task force of child pornography at Dittipidsiber.