Mobile and Forensics
Vol. 5, No. 2, September 2023, pp. 21-30
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v5i2.7893

Forensic Digital Analysis of Telegram Applications Using the National Institute of Justice and Naïve Bayes Methods

[1,*]Meyti Eka Apriyani, [2]Rahmad Alfian Maskuri, [3]M.Hasyim Ratsanjani, [4]Agung Pramudhita, [5]Rawansyah
[1,2,3,4,5]State Polytechnic of Malang, Malang, indonesia
[1,*] meytieka@polinema.ac.id , [2] rahmadalfianm23@gmail.com, [3]hsy@polinema.ac.id, [4]agung.pramudhita@polinema.ac.id, [5]rawansyah@polinema.ac.id
*correspondence email

Abstract

Currently, Telegram is an instant messaging application that is often used by the Indonesian people as a means of long-distance communication with other users. Telegram also has good security features to protect all data from its users. However, Telegram has a positive impact on its users. This security feature can be used by several people to protect against digital crimes, especially cases of sexual harassment. To overcome the existing crimes, analysis, and forensic methods are needed to help solve crimes. This research is guided by the investigation process using the National Institute Of Justice (NIJ) method and the Naïve Bayes method to classify the conversations found. It can be concluded that MOBILedit Forensic Express has a poor performance in finding digital evidence in the Telegram application and FTK Imager is very good at finding digital evidence in the Telegram application. In this research, the classification process using the Naïve Bayes method has been able to classify conversations that contain sexual harassment or not. Evaluation of the classification method uses a confusion matrix to determine the best classification model.

Keywords: Digital Forensic, National Institute Of Justice, Naïve Bayes, Telegram, Investigation.

INTRODUCTION

Based on a report in January 2021 announced by Hootsuite and We are social, internet users in Indonesia reached 73% or 203 million people out of 275 million population in Indonesia. In this case, leading companies compete to create applications that use internet media to connect them. Chat or instant messaging applications are the main targets of the company. At this time Telegram application has become an instant messaging application that is often used by the people of Indonesia as a means of long-distance communication with other users [1][2]3/19/24 1:09:00 AM.

In addition to having a function as a means of remote communication, the Telegram application also has good security features to protect all data from Telegram application users. The Telegram application does not store device or user information locally, but Telegram stores it in the device database or the cloud. That way, Telegram has a positive impact on its users. On the other hand, this security also hurts its users. With this feature, user data can be used by several people to protect when a digital crime occurs. Digital crimes that can be found through this application such as online sexual harassment, cyberbullying, and hate speech [3][4][5][6][7].
Sexual harassment is still common in society and harms the victims. The impact felt by victims of sexual harassment crimes by the people around them will traumatize them psychologically and hurt the formation of their personalities. Sexual harassment can be in the form of sexual content, making jokes that lead to sexuality and insults to someone's body parts, and making physical

Article History: *Received March 27, 2023; Revised June 13, 2023; Accepted September 17, 2023*

contact by touching or the like [8]. Of course, the crime of sexual harassment has digital evidence as investigative material used during the court process. The biggest problem in obtaining digital evidence is that criminals hide or delete digital evidence on smartphones to eliminate traces of the perpetrator's evidence [9]. Given these problems, in overcoming existing crimes, analysis and forensic methods are needed to assist the investigation process in finding deleted or deleted digital evidence so that it can be used during court proceedings and is valid in legal fatwas [3].

Several studies have been conducted regarding the retrieval of digital forensic evidence. The first research was conducted by [10] with the research title "Analysis of Digital Evidence for Facebook Messenger Applications on Android Smartphones Using the NIJ Method", using the NIJ method the study obtained the percentage of digital evidence using the MOBILedit Forensic application 100% accounts, 55% chat, and 86% images. AXIOM magnets generate 100% account percentage, 55% chat, and 86% images. And the Oxygen Forensic app generates 100% percentage for accounts, 5% chat, and 86% pictures. Previous studies only carried out the acquisition or removal of digital evidence, therefore in this study, a classification model is needed to make it easier to categorize conversations including sexual harassment or not. Modeling carried out in the form of classification can assist investigators in detecting the quality of conversations so that they can speed up the investigation process. A related study was conducted by [8] entitled "analysis of sexual harassment tweet sentiment on Twitter in Indonesia using nave Bayes method through the national institute of standard and technology digital forensic acquisition approach", the study used the Naïve Bayes method because it produced a sentiment classification model that valid and better overall test scores compared to other classification methods. The Naïve Bayes method gets 83% accuracy, 57% precision, and 25% recall. The contribution of the research assists interested parties to uncover crimes in sexual harassment cases by obtaining accurate digital evidence.

METHODS

The process of searching for digital evidence has been carried out to obtain digital evidence that has been lost or hidden. The research carried out the process of searching for digital evidence using forensic tools, especially MOBILedit Forensic Express and FTK Imager which functioned to find digital evidence and further analysis will be carried out regarding acts of sexual harassment.

2.1. National Institute Of Justice (NIJ)

National Institute Of Justice (NIJ) is a method that describes the stages of conducting forensic analysis. That way, the research flow can be known research flow so that it can be used as a reference in solving existing cases. Conducting a forensic analysis based on the right research flow the possibility of having a high success rate. The stages of the NIJ method can be seen in Figure 1.

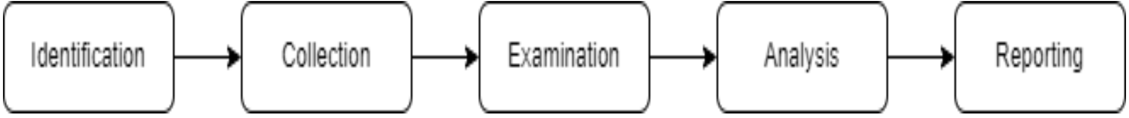

Figure. 1. Stages of the National Institute Of Justice Method

NIJ method has 5 stages among them the Identification stage, which sorts out evidence, the Collection stage collects physical evidence, supporting data, and documentation of physical evidence, the Examination stage conducts data inspection, the Analysis stage performs analysis using legally justified methods, and the reporting stage. Reporting the results of the analysis that has been carried out [11].

Simulation scenarios must be carried out to obtain digital evidence in the forensic process. The simulation was carried out by the perpetrator and the victim as shown in Figure 2. The perpetrator initially sent a normal conversation and continued with a conversation containing sexual harassment content. After physical evidence is obtained, the victim's and perpetrator's smartphones will be acquired for the forensic investigation stage.

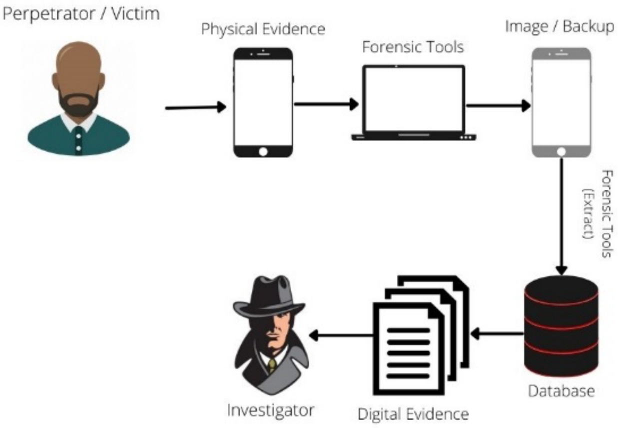

Figure 2. Investigation System

Figure 3 below also explains the design of the system built. The system built in this research is a system for classifying conversational text carried out by investigators or investigators. Classification is done to make it easier for investigators to categorize a text conversation that is used as digital evidence in a digital crime case. The system has several processes, namely the collection of conversational text data obtained through a forensic process using several forensic tools. The next process is the manual labeling of positive and negative conversation categories. The requirement for labeling positive data is if there are words containing sexual harassment. Data is labeled negatively if there are no words containing sexual harassment. The next process is pre-processing the dataset.

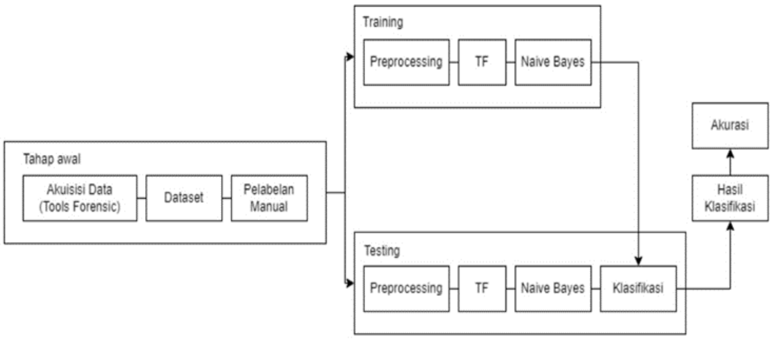

Figure 3. Desain System

This stage includes case folding, tokenizing, stopword removal, stemming. After pre-processing the dataset, the system then performs TF calculations that calculate the probability of each conversation so that it can be input for calculations into Naïve Bayes. The TF value can be used as a method calculation and produce categories in each training and testing data. Training data and testing data are classified after obtaining their respective values in the previous process and become a reference for classification results in the system. In this system, training data and testing data are randomly randomized by the system with a ratio of 50:50

2.2 Dataset

Conversation data amounted to 80 conversations and The data was obtained from the forensic process. From this data, manual labeling was carried out with 2 classification divisions, in case 1

40 positive conversations, and 40 negative conversations, while in case 2 there were 30 positive and 15 negative classifications.
After the conversation data is manually labeled, the next step is to do text preprocessing. Text Preprocessing is the process of converting unstructured textual data into structured data according to the needs of other Text Mining processes [12]. In this case, preprocessing is useful for shortening conversation sentences by getting important words to simplify and speed up the process of identifying cases of sexual harassment. The preprocessing stages can be seen in Figure 4.

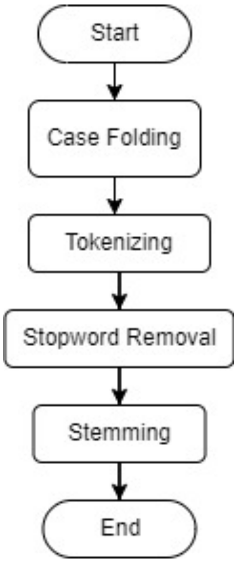

Figure 4. Preprocessing Stage

Figure 3 is the flow of the preprocessing stage which consists of 4 stages. The first stage is case folding, changing all words that use capital letters to lowercase, the tokenizing stage is splitting the character sequence into several parts (words or phrases) called tokens, the stopword removal stage is removing unnecessary words, the stemming stage is making word changes. be the root word [13].

2.3. *Term Frequency*

Term Frequency (TF) itself is the frequency of each word that appears in the document [14]. The important frequency of occurrence of a word in a document is very influential in showing how common that word [15]. TF is symbolized by $tf_{(t,d)}$ which states the number of occurrences of data in each document d. Here is the TF equation.

$$TF_{td} = f_{(t,d)} \tag{1}$$

2.4. *Naïve Bayes Classification*

Naïve Bayes Classification (NBC) is a classification algorithm based on Bayes principle. In classifying Naïve Bayes, including the best method in the process of sentiment analysis. Naïve Bayes applies statistical functions by assuming that certain features are not related to other features. Naïve Bayes has the advantage that it is a simple algorithm but has high accuracy. This method is a classification method by calculating the probability [15]. The probability P calculation can be applied to Equation 2.

$$P(H|X) = \frac{P(H|X)P(H)}{P(X)} \tag{2}$$

Description :
P(H|X) = Probability of hypothesis H based on condition X
X = Represents training data with known class (label)
H = Data dengan kelas (label)
P(H) = Probability of hypothesis X
P(X) = Probability of X observed
P(H|X) = Probability X based on condition H

In the NBC algorithm, each document is characterized by attribute pairs "x1, x2, x3,...,xn" where a1 is the first word, a2 is the second word, and so on, and V is the set of categories [10]. In the classification process, this algorithm looks for the highest probability value from all categories tested (Vmap). To find the highest probability value can use Equation 3.

$$V_{MAP} = \underset{v\ j\ e\ v}{\arg max} \prod_{i=1}^{n} P(x_i|v_j)P(v_j) \tag{3}$$

Description :
V_j = Conversation category
$P(X_i|V_j)$ = Probability of occurrence of Xi in category Vj
$P(V_j)$ = Probability of occurrence of documents that have category j

Further, calculating the probability of each class j can be formulated as follows:

$$P(V_j) = \frac{|docs_j|}{|\text{data } training|} \tag{4}$$

Description :
$P(V_j)$ = Probability of occurrence of documents in category j
$|docs_j|$ = Number of documents in each category j
|data *training*| = Number of documents in all categories

And lastly, calculate the probability of the word xi on the testing data against the test data for each class j, by:

$$P(X_i|V_j) = \frac{n_k + 1}{n + |vocab|} \tag{5}$$

Description:
$P(X_i|V_j)$ = Probability of occurrence of Xi in category Vj
$n_{k=}$ Number of occurrences of each term
n = Number of occurrences of each term in each category
|*vocab*| = Sum of all terms from all categories

2.5 *Confusion Matrix*

A confusion Matrix is a technique for measuring model performance. The Confusion Matrix table shows the results of the classification of true test data and false test data [16]. Calculating the classification performance requires several parameters, namely accuracy, precision, and recall. Accuracy is the ratio of the correctly estimated performance of the total observations. To calculate the accuracy formulated in Equation 6.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

Precision is the ratio of correctly estimated positive observations to the total predicted positive observations. To calculate the precision formulated in Equation 7.

$$precision = \frac{TP}{TP + FP} \tag{7}$$

For recall, it can be said that sensitivity is the number of positive observations that are correctly estimated for all observations in the actual class. To calculate the recall value can use Equation 8.

$$recall = \frac{TP}{TP + FN} \tag{8}$$

RESULT AND DISCUSSIONS

At this stage, a summary of the smartphone used and the forensic process carried out as well as a comparison of the forensic tools used is carried out. The smartphone information used will be reported as physical evidence in the form of 2 units of Android-based smartphones. The application that is analyzed for digital evidence is Telegram Messenger which is installed on each smartphone. In the case simulation, data is created in the case with 80 conversations and 1 picture. The analysis process using FTK Imager is carried out by reading or extracting image files that have been obtained from the physical image creation process in the previous stage. Figure 5 is the process of adding evidence or extracting the image file obtained in the previous stage.

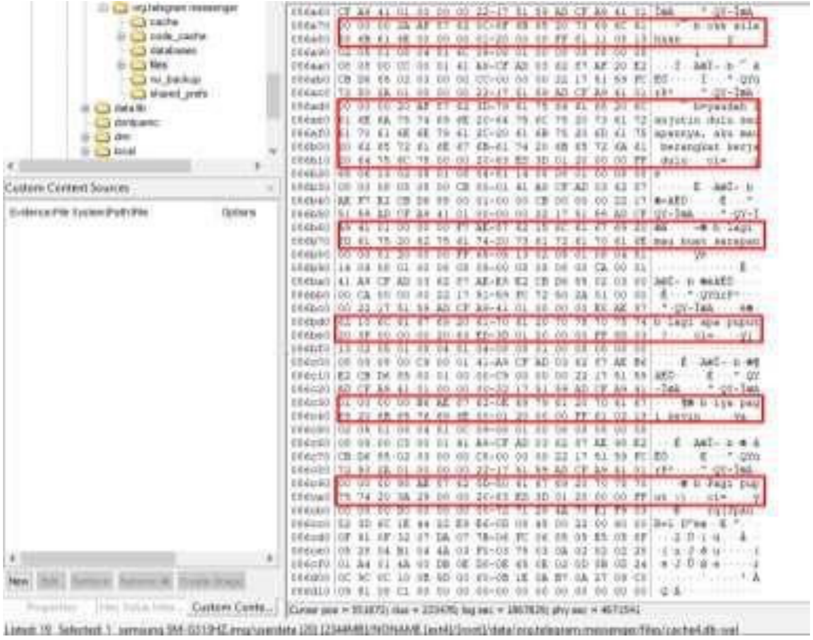

Figure 5. Finding Evidence of Conversations in Telegram Messenger

Figure 5 is the result of searching for digital evidence of conversations conducted on Telegram Messenger. At this stage, FTK Imager can find evidence of 80 conversations between perpetrators and victims as the result of searching for digital evidence of conversations conducted on Telegram Messenger. At this stage, FTK Imager can find evidence of 45 conversations between perpetrators and victims

At this stage, data processing will be carried out using the National Institute of Justice (NIJ) method to obtain digital evidence and the Naïve Bayes method to classify the conversation data of perpetrators and victims whether included in sexual harassment or not. At the beginning of data processing, problem identification is carried out, collecting all information and analyzing the needs of systems and devices needed in the investigation process. The first change occurs at the time of collecting the data, after which the data is examined, and extracted so that the format can be processed by forensic tools. Furthermore, the data that has been obtained is classified to be good information. Ultimately, the data becomes evidence of analogy with applying knowledge into action through information generated by analysis and classification in one or several ways during the reporting phase.

The procedure for examining the evidence found is as follows :

1. The signal is removed by activating airplane mode on smartphones 1 and smartphones 2.
2. The cloning process or creating a physical image is carried out with the MOBILedit Forensic Express application which is connected to an Acer e5-475G brand laptop, Windows 10 64-bit OS, and 500GB storage capacity.
3. Extraction and analysis of digital evidence are carried out by the MOBILedit Forensic Express and FTK Imager applications. The results of the examination are as follows:
   a. On a smartphone that has been rooted, it is found that the application used is Telegram Messenger, while on a smartphone that has not been rooted, the application users cannot be found.
   b. The analysis carried out found evidence of chat and images.
   c. Forensic tools in the form of software used in the digital evidence retrieval process consist of 2 types with various features and capabilities.

The document will be uploaded to the system to find out sexual harassment content with positive labels that include sexual harassment and negative labels that do not include sexual harassment. The next step will be preprocessing the data before identifying sexual harassment using the Naïve Bayes method. The results of preprocessing can be seen in Table 4. The results of preprocessing are then identified by the Naïve Bayes method so that the TF value is obtained as shown in Table 1.

Table 1. Case Conversation Preprocessing

Conversation	***Preprocessing***
bayangin aku lagi ngewe kamu, kamu pasti suka juga	['bayangin', 'ngewe', 'kamu', 'suka']
aku normal lah, buktinya aku serius pingin bercinta sama kamu	['normal', 'lah', 'bukti', 'serius', 'pingin', 'cinta']
kamu masih perawan?	['perawan']
udah selesai pertemuan nya?	['udah', 'selesai', 'temu', 'nya']
aku pingin liat payudaramu, pantatmu, liat semuanya	['pingin', 'liat', 'payudara', 'pantat', 'liat']
Aneh	['aneh']
udah cantik, seksi lagi	['udah', 'cantik', 'seksi']
cabul gila	['cabul', 'gila']
loh kok sudahan sih puput yang seksi	['loh', 'sudah', 'sih', 'puput', 'seksi']
Cium dulu dong	['cium']

The TF that has been obtained in the conversation will be written in Table 1 and Table 2 in the term column using formula (1). TF results will be used to calculate the maximum value of class probability to determine positive and negative classes in each conversation using the formula (3).

Table 2. TF Case Conversation

Term	**TF**
Aja	4
Aneh	1
Apa	1
Ayo	1
banget	5
bareng	1
bayangin	1
beneran	1
bentar	1
berangkat	2

Table 3 shows the probability generated by the system which is calculated using formula (3). For results that have a high probability value in all test classes, the conversational dataset will be classified as that class.

Table 3 Case Conversation Probability

Conversation	***Positif***	***Negatives***
bayangin ngewe kamu suka	0.46687613218611584	0.5331238678138839
normal lah bukti serius pingin cinta	0.5888741233672548	0.41112587663274547
perawan	0.4749999999999999	0.525
selesai temu	0.26253518138563103	0.7374648186143685
pingin liat payudara pantat liat	0.5728245732652713	0.42717542673472864
aneh	0.4749999999999999	0.525
udah cantik seksi	0.4179290683196437	0.5820709316803566
cabul gila	0.6679753840808182	0.33202461591918186
loh sudah sih puput seksi	0.5061002894875762	0.49389971051242415
cium	0.4749999999999999	0.525

Figure 6 shows the test results on the classification of the Naïve Bayes algorithm in case 1 using 50 percent of the training data and 50 percent of random testing data getting an accuracy value of 85 percent, a precision value getting value of 85.7 percent, and a recall value getting a value of 85. 7 percent. This is because of the number of complete sentences in each conversation that is tested, the possibility of accuracy can be increased by completing sentences in each conversation. The completeness of the sentence here is like every sentence has a subject, predicate, and object.

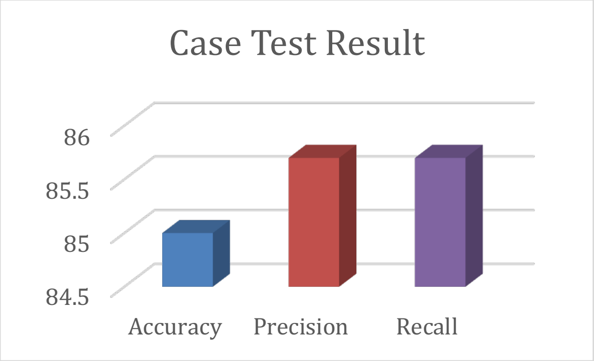

Fig 6. Case Test Results

The results of digital forensic analysis obtained in case concluded that the MOBILedit Forensic Express application could not find digital evidence on both smartphones, this was because MOBILedit Forensic Express could not extract files from Telegram Messenger. However, in making or doing the imaging process MOBILedit Forensic Express is very good and easy to do, but the condition for the imaging process is that the smartphone must be in a rooted condition. As for the performance of FTK Imager, it is very good at finding digital evidence only on smartphone 1, this is because smartphone 2 has not been rooted and cannot create imaging files so it cannot search for digital evidence.

The total dataset used in testing the classification accuracy regarding the performance of the Naïve Bayes method on conversational classification contains 80 sentences of sexual harassment context in cases Manual labeling is done by means the data will be given a positive label if, in the conversation sentence, there are words that contain sexual harassment. If the data does not contain the word sexual harassment, then the sentence will be given a negative label. After testing in the case, the results of the highest accuracy, precision, and recall were obtained in the case, this was because the distribution of training data and testing data was carried out randomly. From the results of the comparison of the data between the label and the prediction results, the data will be true if the prediction results have the same results as the label.

The results of the classification accuracy test produced in the case using 50 percent training data and random testing data are 85%, Precision 85.7%, and Recall 85.7%. This shows that the completeness of the pattern in the sentences affects the results of the classification and testing of each sentence. The results of the comparison of data between the label and the prediction result, then the data will be true if the prediction result has the same result as the label

CONCLUSIONS

Based on the analysis, design, and testing conducted, the following conclusions are evident: firstly, rooted smartphones possess broader data access compared to non-rooted ones during data acquisition; secondly, MOBILedit Forensic Express application showed 0% performance in data recovery on both smartphones 1 and 2, while FTK Imager exhibited 100% performance; and thirdly, the Naïve Bayes algorithm proved effective in classifying conversations into positive and negative categories regarding sexual harassment.

REFERENCES

[1] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *JR*, vol. 2, no. 10, pp. 1400–1405, Sep. 2020, doi: 10.22219/repositor.v2i10.1066.

[2] I. Riadi, R. Umar, and M. A. Aziz, "Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO)," *MF*, vol. 1, no. 1, p. 30, Sep. 2019, doi: 10.12928/mf.v1i1.705.

[3] M. S. Asyaky, N. Widiyasono, and R. Gunawan, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger pada Android," *SinkrOn*, vol. 3, no. 1, pp. 220–231, Sep. 2018.

[4] F. N. Rosyidah and M. F. Nurdin, "Media Sosial: Ruang Baru dalam Tindak Pelecehan Seksual Remaja,"*j.sosioglobal*, vol. 2, no. 2, p. 38, Jul. 2018, doi: 10.24198/jsg.v2i2.17200.

[5] N. Tarmizi, S. Saee, and D. H. Abang Ibrahim, "Detecting the Usage of Vulgar Words in Cyberbully Activities from Twitter," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 3, pp. 1117–1122, Jun. 2020, doi: 10.18517/ijaseit.10.3.10645.

[6] A. Raza and M. Bilal Hassan, "Digital Forensic Analysis of Telegram Messenger App in Android Virtual Environment," *mob.forensics.j*, vol. 4, no. 1, pp. 31–43, Mar. 2022, doi: 10.12928/mf.v4i1.5537.

[7] R. Octora, "PROBLEMATIKA PENGATURAN CYBERSTALKING (PENGUNTITAN DI DUNIA MAYA) DENGAN MENGGUNAKAN ANNONYMOUS ACCOUNT PADA SOSIAL MEDIA," *dialogia*, vol. 11, no. 1, pp. 77–96, Nov. 2019, doi: 10.28932/di.v11i1.1902.

[8] K. Budiman, N. Zaatsiyah, U. Niswah, and F. M. N. Faizi, "Analysis of Sexual Harassment Tweet Sentiment on Twitter in Indonesia using Naïve Bayes Method through National Institute of Standard and Technology Digital Forensic Acquisition Approach".

[9] I. Riadi, "PERBANDINGAN TOOL FORENSIK DATA RECOVERY BERBASIS ANDROID MENGGUNAKAN METODE NIST".

[10] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," *ITJRD*, vol. 5, no. 2, pp. 118–134, Aug. 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[11] I. Riadi, R. Umar, and I. M. Nasrulloh, "ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *ELINVO*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

[12] M. N. Randhika, J. C. Young, A. Suryadibrata, and H. Mandala, "Implementasi Algoritma Complement dan Multinomial Naïve Bayes Classifier Pada Klasifikasi Kategori Berita Media Online," *Ultimatics*, vol. 13, no. 1, pp. 19–25, Jun. 2021, doi: 10.31937/ti.v13i1.1921.

[13] M. N. Randhika, J. C. Young, A. Suryadibrata, and H. Mandala, "Implementasi Algoritma Complement dan Multinomial Naïve Bayes Classifier Pada Klasifikasi Kategori Berita Media Online," *Ultimatics : Jurnal Teknik Informatika*, vol. 13, no. 1, pp. 19–25, 2021, doi: 10.31937/ti.v13i1.1921.

[14] M. I. Fikri, T. S. Sabrila, and Y. Azhar, "Perbandingan Metode Naïve Bayes dan Support Vector Machine pada Analisis Sentimen Twitter," *Smatika Jurnal*, vol. 10, no. 02, pp. 71–76, 2020, doi: 10.32664/smatika.v10i02.455.

[15] Merinda Lestandy, Abdurrahim Abdurrahim, and Lailis Syafa'ah, "Analisis Sentimen Tweet Vaksin COVID-19 Menggunakan Recurrent Neural Network dan Naïve Bayes," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 4, pp. 802–808, 2021, doi: 10.29207/resti.v5i4.3308.

[16] R. Sari and R. Y. Hayuningtyas, "Penerapan Algoritma Naive Bayes Untuk Analisis Sentimen Pada Wisata TMII Berbasis Website," *Indonesian Journal on Software Engineering (IJSE)*, vol. 5, no. 2, pp. 51–60, 2019, doi: 10.31294/ijse.v5i2.6957.

AUTHORS BIBLIOGRAPHY

	MEYTI EKA APRIYANI received a B.S. degree from the Department of Electrical Engineering, Telcom University, Bandung, Indonesia, in 2009. She received the M.Sc. in 2011. Her research interest includes networking, system information, and the internet of things. She is a regular reviewer for various reputable national journals. She has published several national journal articles in accordance with the internet of things and system information