Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12514
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Digital Forensic Investigates Sexual Harassment on Telegram using Naïve Bayes

Meyti Eka Apriyani[1)*], Rahmad Alfian Maskuri[2)], Muhammad Hasyim Ratsanjani[3)], Agung Nugroho Pramudhita[4)], Rawansyah[5)]
[1,2,3,4,5)]Politeknik Negeri Malang, Indonesia
[1)]meytieka@polinema.ac.id, [2)]alfian@gmail.com, [3)]hsy@polinema.ac.id, [4)] agung.pramudhita@polinema.ac.id , [5)]rawansyah@email.com

Submitted : Jun 5, 2023 | **Accepted** : Jun 21, 2023 | **Published** : Jul 1, 2023

Abstract: The widespread use of Telegram in Indonesia has had both positive and negative effects. While the app offers strong security features, it has also become a platform for digital crimes, including sexual harassment. This study aims to address the need for effective forensic analysis and classification methods by employing the National Institute of Justice (NIJ) methodology and Naïve Bayes classifier to analyze conversations on Telegram. The research evaluates the performance of digital forensic tools and the effectiveness of the Naïve Bayes method in identifying instances of sexual harassment conversation. The data analyzed is about conversations on the telegram application that contain sexual harassment. Data collection involves extracting relevant conversations and subjecting them to forensic analysis using MOBIL edit Forensic Express and FTK Imager. Based on the test results, the naïve Bayes algorithm can be used to classify conversations into positive and negative about sexual harassment. The value obtained from naïve Bayes testing is the accuracy value of 91.3%, Precision 100%, and Recall 90%.

Keywords: Forensic, Investigation, Method, Naïve Bayes, Telegram

INTRODUCTION

Sexual harassment on digital platforms, such as Telegram, has become a pervasive issue, requiring effective strategies to address and prevent such misconduct. In this context, digital forensic investigations play a crucial role in uncovering evidence and identifying perpetrators. This paper aims to explore the application of the Naïve Bayes algorithm in digital forensic investigations of sexual harassment on Telegram, and its significance in contributing to previous research in the field. The importance of this research lies in its potential to provide valuable insights and methodologies to enhance previous studies. While existing research has shed light on the prevalence and impact of online sexual harassment, the specific utilization of the Naïve Bayes algorithm in digital forensic investigations remains an area that requires further investigation and exploration.

Digital forensic investigations of sexual harassment on Telegram are essential for several reasons. Firstly, these investigations aim to provide justice and support to the victims who have experienced harassment in the digital space. By gathering digital evidence and identifying the offenders, digital forensic investigators play a vital role in holding them accountable for their actions. This not only provides closure and support to the victims but also acts as a deterrent for potential offenders, creating a safer online environment. (Smith, 2022). Secondly, such investigations provide an opportunity to gain a deeper understanding of the patterns and dynamics of sexual harassment on Telegram. By analyzing message content, metadata, and other digital artifacts, investigators can identify crucial patterns, linguistic cues, and characteristics associated with harassment. This knowledge can inform

*name of corresponding author

the development of preventive measures, policies, and educational campaigns to combat and minimize instances of sexual harassment on messaging platforms.

The application of the Naïve Bayes algorithm in digital forensic investigations offers a promising approach to the field. Naïve Bayes has proven effectiveness in various text classification tasks, making it a suitable choice for identifying and categorizing instances of sexual harassment on Telegram. By training the algorithm on labeled datasets of harassing and non-harassing messages, investigators can develop models that automate the classification process. This facilitates efficient analysis of large volumes of data and expedites the identification of potential cases of sexual harassment, thereby enhancing the overall effectiveness and efficiency of the investigative process. Furthermore, this research aims to build upon and contribute to previous studies in the field of digital forensic investigations. While prior research has explored different aspects of sexual harassment, the integration of the Naïve Bayes algorithm specifically in investigating such incidents on Telegram remains an underexplored area. By delving into this aspect, this study has the potential to provide novel findings and insights that can contribute to the existing body of knowledge and methodologies in digital forensic investigations. These contributions can serve as valuable resources for future investigations, potentially inspiring further research into the application of machine learning algorithms in digital forensics.

In conclusion, digital forensic investigations are crucial in addressing sexual harassment on messaging platforms like Telegram. This research aims to contribute to previous studies by examining the application of the Naïve Bayes algorithm in detecting and categorizing instances of harassment. By shedding light on this aspect of digital forensics, this study has the potential to provide valuable insights and methodologies that can assist investigators in combating sexual harassment on Telegram effectively.

LITERATURE REVIEW

Analysis of sexual harassment tweet sentiment on twitter in Indonesia using naïve bayes method through national institute of standard an technology digital forensic acquisition approach", the study used the Naïve Bayes method because it produced a valid sentiment classification model and a better overall test value compared to other classification methods. The Naïve Bayes method gets an accuracy value of 83%, precision 57%, and recall 25% (Budiman et al., 2020). The use of naive bayes in other studies has concluded that the Naïve Bayes method can predict sentiment by getting an accuracy value of 75%. The data used in the study amounted to 1000 tweets (800 tweets for training data and 200 for test data). In addition, adding training data and test data can make accuracy even better (Afrizal et al., 2020). For Classification of Government Sentiment Towards Handling Covid-19 Using Twitter Data", this study concluded that the system with the Multinomial Naïve Bayes method can categorise text sentiment in positive, negative, and neutral classes. The Multinomial Naïve Bayes method can produce accuracy with a value of 74%, precision 74%, and recall of 74%. With these results, an AUC value of 0.74 can be obtained. So it can be concluded that this algorithm has a moderate or fairly good diagnostic value (Yuyun et al., 2021). Digital forensics is science and technology in the interest of proving the law, with the aim of proving computer crimes by obtaining digital evidence used against the perpetrators of the crime. by obtaining digital evidence used against the perpetrator. In essence, this field of science can obtain digital evidence that may be stored on drives, internal storage, and other storage. Digital forensics is needed because mobile-based services are increasing and more and more users, with the increasing popularity of mobile computing and mobile commerce, the need for mobile transactions is also getting higher. The quality and speed of mobile service providers must be proportional to the number of mobile transactions taking place. The challenge of mobile transactions lies in the large number of mobile service providers with high speed and secure networks. Online transactions conducted using mobile devices must have high security and protect users from misuse by irresponsible people (Riadi et al., 2017).

Research conducted by (Hidayat & Rizqi, 2020), namely Classification of News Documents Using the Enhaced Confix Stripping Stemmer Algorithm and Naïve Bayes Classifier using a dataset from the www.jawapos.com portal as many as 600 news documents, and using 40 data to be tested. The classification results obtained an average accuracy value for each category of 95%.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i3.12514 p-ISSN : 2541-044X

METHOD

At the stage of collecting data using a literature study, the author looks for references that are relevant to the object to be studied. Reference searches are carried out in libraries, bookstores, and online using the internet. The information obtained can be used in compiling the theoretical basis, and research methodology, determining the application to perform simulations, and how to perform simulations. This study uses a classification method that consists of 5 stages consisting the following is identification stage is an activity of sorting the evidence found and sorting the data that supports the investigation process. This stage requires tools and materials used by investigators in carrying out the forensic investigation process. The next stage is a collection of researchers who propose a solution that aims to solve problems from the information from the identification stage. Furthermore, at this stage, the researcher examines the data collected forensically either manually or automatically and ensures the authenticity of the data obtained by what was obtained at the scene of the crime. The forensic tools used in the Examination process are MOBIL edit Forensic Express and FTK Imager. After going through several stages that have been carried out, the next stage is the analysis stage. In the analysis stage, researchers use the Naïve Bayes method to analyze forensic results on the conversation data obtained. Last The reporting stage is the stage of making a report that is carried out after digital evidence is obtained from the examination process and the analysis process. At this stage, reporting the results of the analysis is carried out which includes a description of the case that occurred, a description of the actions taken, the forensic techniques and tools used, and other supporting aspects in the digital forensic action process.

Figure 1 below also explains the design of the system built with naïve bayes. 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.

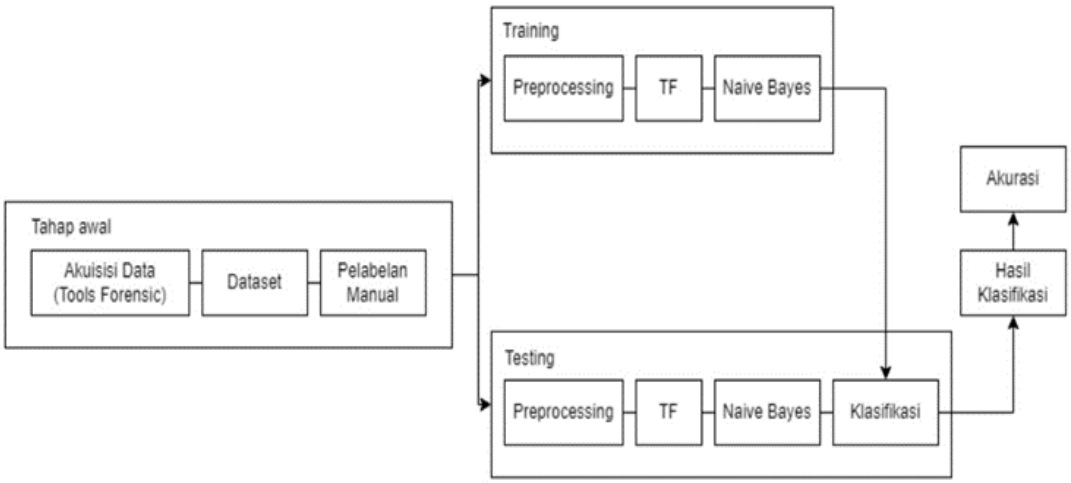

Fig 1. Desain System

This stage includes case folding, tokenizing, stop word removal, and stemming. After pre-processing the dataset, the system then calculates TF which calculates the probability of words in each conversation so that it can be an input for calculation into Naïve Bayes. The TF value can be used as a calculation method and produces categories for each training and testing data. Training data and training data and testing data are classified after obtaining their respective values in the previous process and become a reference for the classification results in the system. In this system, training data and testing data are randomized by the system with a ratio of 50:50. Conversation data amounted to 80

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12514
e-ISSN : 2541-2019
p-ISSN : 2541-044X

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. In the test, several examples of conversations sent between the perpetrator and the victim were used.

RESULT

Result

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 analysed 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, The results of finding evidence in cases 1 and 2 are in Table 1 and Table 2.

Table 1 Digital Evidence Discovery Results Case 1

		Forensic Tools			
No	Digital Evidence	MOBILedit Forensic Expres		FTK Imager	
		Case 1			
		Smartphone 1	Smartphone 2	Smartphone 1	Smartphone 2
1	Chat	0	0	80	0
2	Image	0	0	1	0

Table 2 Digital Evidence Discovery Results Case 2

		Forensic Tools			
No	Digital Evidence	MOBILedit Forensic Expres		FTK Imager	
		Case 1			
		Smartphone 1	Smartphone 2	Smartphone 1	Smartphone 2
1	Chat	0	0	45	0
2	Image	0	0	0	0

Tables 1 and 2 describe the discovery of evidence and the results of searching or analyzing data on the Telegram Messenger application using MOBIL edit Forensic Express and FTK Imager tools. MOBIL edit Forensic Express did not succeed in finding chat or image evidence in case 1, while FTK Imager managed to find 80 conversations and 1 image in case 1 in Table 1 and 45 conversations in case 2 in Table 2.

In this study, researchers collected data by simulating searching and analyzing forensic data using an Android-based smartphone with version 4.4.2 (KitKat) which has the Telegram application installed and uses a fake account, where the data from this simulation will be used by researchers as research analysis material. Simulation scenarios must be carried out to obtain digital evidence in the forensic process. The victim reported the incident to the authorities and the victim's smartphone was used as evidence. After a complaint from the victim, the perpetrator was summoned by the police, and the evidence, namely the perpetrator's smartphone, was secured by the party concerned. All data in the form of conversations that have been deleted on the suspect's device from Telegram Messenger will be revealed or reappeared using the help of tools carried out by the Investigator.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12514
e-ISSN : 2541-2019
p-ISSN : 2541-044X

For security and maintaining the authenticity of evidence MOBIL edit Forensic Express performs an imaging process on the Telegram application which the final result is in image format so that it can be used in other forensic tools. The examination process using MOBIL edit Forensic Express can be done by connecting physical evidence to a computer or laptop. The digital evidence sought includes evidence of conversations and images. After the smartphone is connected, the imaging process will be carried out to capture data on the Telegram Messenger application, and the conversation data will be analyzed by the FTK Imager tool. Conversation data resulting from the data acquisition process is still raw data that is not ready to be processed, therefore a text pre-processing stage is carried out to produce data that is ready for use in the next stage. Before entering this stage, the conversation data is automatically labeled by the system based on the occurrence of words that include words of abuse and can be continued in the pre-processing stage.

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 3. The results of preprocessing are then identified by the Naïve Bayes method so that the TF value is obtained as shown in Table 3

Table 3. Case Conversation Pre-processing

Conversation	*Pre-processing*
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']

After the text pre-processing stage is carried out, the data resulting from this stage will be word weighted. In this research, the weighting is obtained from the frequency of a word contained in a sentence or the number of occurrences of terms in one document Term frequency (tf). Next is the probability stage, there is the value of the calculation of the class probability in each sentence whether the sentence belongs to a positive or negative class. Table 4 shows the probability generated by the system. For results that have a high probability value in all test classes, the conversational dataset will be classified as that class.

Table 4. Case Conversation Probability

Conversation	*Positive*	*Negatives*
bayangin ngewe kamu suka	0.466	0.533
normal lah bukti serius pingin cinta	0.588	0.411
perawan	0.474	0.525
selesai temu	0.262	0.737
pingin liat payudara pantat liat	0.572	0.427
aneh	0.474	0.525
udah cantik seksi	0.417	0.582
cabul gila	0.667	0.332
loh sudah sih puput seksi	0.506	0.493
cium	0.474	0.525

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12514
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The results of testing the Naïve Bayes algorithm classification in case 1 using 50 percent of training data and 50 percent of random testing data get an accuracy value of 85 percent, a precision value gets a value of 85.7 percent, and a recall value gets value of 85. The results of testing the Naïve Bayes algorithm classification in case 2 using 50 percent of training data and 50 percent of random testing data get a value of 7 percent. This is due to the number of complete sentences in each conversation tested, the possibility of accuracy can be improved by completing the sentences in each conversation. Completeness of sentences here such as each sentence has a subject, predicate, and object. While the test results in case 2 with the Naïve Bayes algorithm using 50% randomized training and testing data resulted in an accuracy value of 91.3%, a precision value of 100%, and a recall value of 90%. The comparison of the results can be seen in Figure 2

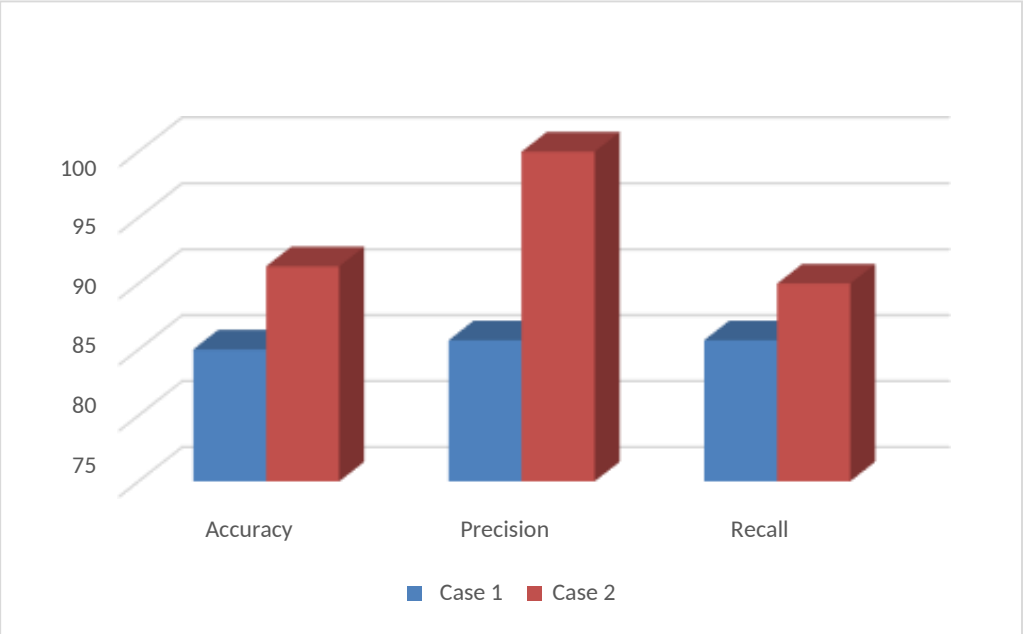

Fig 2. Testing naïve bayes algorithm

The results of digital forensic analysis obtained in the case concluded that the MOBIL edit Forensic Express application could not find digital evidence on both smartphones, this was because MOBIL edit Forensic Express could not extract files from Telegram Messenger. However, in making or doing the imaging process MOBIL edit 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.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, July 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i3.12514 p-ISSN : 2541-044X

DISCUSSIONS

The findings of the study demonstrate the effectiveness of the Naïve Bayes algorithm in classifying conversations related to sexual harassment on Telegram. The algorithm achieved a high accuracy rate of 91.3%, indicating its ability to accurately distinguish between harassing and non-harassing messages. This high accuracy can be attributed to the unique characteristics of the Naïve Bayes algorithm. Naïve Bayes is a probabilistic algorithm that leverages Bayes' theorem and assumes that the features in the data are conditionally independent of each other. This assumption simplifies the calculation of probabilities and makes the algorithm computationally efficient. In the context of conversation classification, Naïve Bayes calculates the probability of a message belonging to a particular class (harassing or non-harassing) based on the probabilities of its features. The algorithm then assigns the message to the class with the highest probability.

The accuracy of the Naïve Bayes algorithm in this study can be attributed to the effective preprocessing of the data. Data preprocessing involves transforming, tokenizing, and filtering the data to remove noise and improve the quality of the input for analysis. By ensuring that the data is clean and relevant, the algorithm can make more accurate predictions. The preprocessing stage plays a crucial role in enhancing the overall performance of the Naïve Bayes algorithm and contributes to the high accuracy achieved in this study. Furthermore, the study also discusses the impact of the forensic tools used in the initial stage of the investigation. The study employed Mobil Edit Forensic Express and FTK Imager applications to recover digital evidence from smartphones. The findings indicate that Mobil Edit Forensic Express had a 0% recovery rate in terms of deleted data or digital evidence, while FTK Imager achieved a 100% recovery rate.

In the preprocessing process, there are still data that produce wrong predictions when classified. Sentences with "neutral" sentiment generally have a wider variety of words and lack typical words as in other sentiment values, making it difficult to recognize (Santoso et al., 2017). Sentiment classification using naïve Bayes resulted in 15 negative conversations and 30 positive conversations with a total data of 45 conversations. This proves that by doing this analysis, crime investigators can find out the types of crimes related to sexual harassment. However, there are still some words that contain elements of sexual harassment but use local languages so that the system cannot detect whether they are included in the positive or negative classification. The tendency is to fall into the neutral classification. Our findings are the results of research conducted by (Tia, 2020). Where these results become one of the factors that strengthen the results of previous research on the types of words that often appear for tweets of hostile work environment types of sexual harassment so that the larger the size of the word in the word cloud, the higher the frequency of the word, meaning that the word is often used by victims of sexual harassment who bravely share their experiences on Twitter.

This discrepancy in performance highlights the importance of selecting appropriate forensic tools for digital investigations. The inability of Mobil Edit Forensic Express to recover deleted data suggests limitations in its capabilities, which may impact the overall forensic results. On the other hand, the successful recovery of conversations and images using FTK Imager demonstrates its effectiveness in extracting relevant evidence. Overall, the findings of this discussion indicate that the Naïve Bayes algorithm, when combined with effective data preprocessing techniques, can achieve high accuracy in classifying conversations related to sexual harassment on Telegram. Additionally, the choice of forensic tools used in the investigation process can significantly impact the recovery of digital evidence. These findings provide valuable insights for future digital forensic investigations, emphasizing the importance of selecting appropriate algorithms and tools to enhance the accuracy and reliability of forensic results.

CONCLUSION

Forensic analysis of sexual harassment in telegram applications based on the NIJ method with several stages and tools produces different accuracy. The use of this method is used to obtain digital evidence and the Naïve Bayes method to classify conversation data included in sexual harassment. The results obtained in this study show that sentence patterns can affect the classification and testing results carried out by the naïve Bayes method.

*name of corresponding author

REFERENCES

Anshori, K., Setya Putri, E., & Ghoni, U. (2020). Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ. *IT Jurnal Riset dan Pengembangan*, 5(2), 118-134. doi: 10.25299/itjrd.2021.vol5 (2).4664.

Asyaky, M. S. (2019). Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. *Jurnal Penelitian Teknik Informatika*, 3(1), 220–231.

Azizah, S., Ramadhona, S. A., & Gustitio, K. W. (2020). Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST. *Journal of Repos*, 2(10), 1400–1405. doi: 10.22219/repository. v2i10.1066.

Ariyanti, D., Iswardani, K., & Rafidah, S. (2020). Klasifikasi Penanganan Keluhan Masyarakat Kota Probolinggo Menggunakan Algoritma Naive Bayes. *J-SAKTI (Jurnal Sains dan Teknologi Indonesia)*, 4(September), 424-433.

Bulan, B., Tahun, T., Yudhana, A., Umar, R., & Ahmadi, A. (2022). Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *Jurnal CoreIT*, X(X), 8-13.

Fikri, M. I., Sabrila, T. S., & Azhar, Y. (2020). Perbandingan Metode Naïve Bayes dan Support Vector Machine pada Analisis Sentimen Twitter. *Smatika Jurnal*, 10(02), 71–76. doi:10.32664/smatika. v10i02.455

Imam, R., Anton, Y., & Muhammad, C. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (NIJ). *Jurnal Teknik Informatika dan Sistem Informasi (JUTISI*), 4, 219-227.

Imam, R., Sunardi, S., & Arizona, F. (2017). Forensic Investigation Technique on Android's Blackberry Messenger Using NIST Framework. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 4, 198-205.

K. Budiman, N. Zaatsiyah, U. Niswah, F. Muhanna, & N. Faizi. (2020). 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. *Journal of Advanced Information Systems and Technology*, 2(2), 21-30.

Leonardo, A., & Indrayani, R. (2021). The Comparison Performance of Digital Forensic Tools Using Additional Root Access Options. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 7(3), 512-521. http://dx.doi.org/10.26555/jiteki.v7i3.2238

Lestandy, M., Abdurrahim, A., & Syafa'ah, L. (2021). Analisis Sentimen Tweet Vaksin COVID-19 Menggunakan Recurrent Neural Network dan Naïve Bayes. *Jurnal Rekayasa Sistem dan Teknologi Informasi (RESTI*), 5(4), 802–808. doi:10.29207/resti. v5i4.3308

Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI*), 4(01), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, 5(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

Randhika, M. N., Young, J. C., Suryadibrata, A., & Mandala, H. (2021). Implementasi Algoritma Complement dan Multinomial Naïve Bayes Classifier Pada Klasifikasi Kategori Berita Media Online. Ultima *Jurnal Teknik Informatika*, 13(1), 19–25. doi:10.31937/ti. v13i1.1921

Riadi, I., Sunardi, &, Sahiruddin. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 7(1), 197-204. doi:10.25126/jtiik.202071921

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analysis Forensic Digital Pada Frozen Solid-State Drive Dengan Metode National Institute of Justice (NIJ). *Elinvo (Electronics, Informatics, Vocational Education*), 3(1), 70-82. doi:10.21831/elinvo.v3i1.19308

Riadi, I., Yudhana, A., & Putra, M. C. F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (NIJ*). Jurnal Teknik Informatika Dan Sistem Informasi*, 4(2), 219–227.

*name of corresponding author

Santoso, V. I., Virginia, G., & Lukito, Y. (2017). Penerapan Sentiment Analysis Pada Hasil Evaluasi Dosen Dengan Metode Support Vector Machine. *Jurnal Transformatika*, 14(2), 72–76. https://doi.org/10.26623/transformatika.v14i2.439

Sari, R., & Hayuningtyas, R. Y. (2019). Penerapan Algoritma Naive Bayes Untuk Analisis Sentimen Pada Wisata TMII Berbasis Website. *Indonesian Journal of Software Engineering*, 5(2), 51–60. doi: 10.31294/ijse. v5i2.6957.

Sahiruddin, R., Imam, R., & Sunardi, S. (2018). Data Recovery Dengan Keamanan Fingerprint Pada Smartphone Android. *Proceedings of the Semantics, Engineering, and Digital Information Conference* (SENDI-U).

Smith, J., & Johnson, A. (2022). Investigating Sexual Harassment on Social Media Platforms: A Digital Forensic Approach. *Journal of Digital Forensics, Security and Law*, 10(2), 35-48.

Putri, T. A. M., Enri, U., & Sari, B. N. (2020). Analisis Algoritma Naive Bayes Classifier untuk Klasifikasi Tweet Pelecehan Seksual dengan #MeToo. *Indonesian Journal on Computer and Information Technology*.

Wiratama, I. P., Suharso, A., & Rozikin, C. (2021). Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA. *Jurnal Sains Komputer & Informatika* (J-SAKTI), 5(2), 712–726.

Yudhana, A., Riadi, I., & Ridho, F. (2018). DDoS classification using neural network and naïve Bayes methods for network forensics. *International Journal of Advanced Computer Science and Applications*, 9(11), 177-183

*name of corresponding author