Ceddi Journal of Information System and Technology (JST)
Vol. 2 No. 2 December (2023)
https://doi.org/10.56134/jst.v2i2.45

ISSN: 2829-808X (print)
ISSN: 2829-6575 (online)

Digital Forensic Evidence Analysis in Revealing Defamation on Social Media (Twitter) Using the Static Forensics Method

Reski Badillah[1*], Andi Yulia Muniar[2], Abd. Rahman[3], Febri Hidayat Saputra[4], Mansyur[5], Supriadi Sahibu[6]

[1-4]*Department of Informatics, Universitas Teknologi Akba Makassar, Makassar, Indonesia*
[5]*Educational Research and Evaluation, Universitas Negeri Makassar, Makassar, Indonesia*
[6]*Computer System, Universitas Handayani Makassar, Indonesia*

Abstract

This research addresses the persistent challenge of defamation, notably prevalent on the Twitter platform, where the discovery of digital evidence is hampered by robust privacy protections. The study aims to investigate and identify digital evidence in defamation cases on Twitter, focusing on optimizing the evidence discovery process. Employing static forensics to prevent data alterations during acquisition from devices associated with defamation, the research successfully uncovered various digital evidence, including text from deleted comments, usernames, emails, and deleted image files linked to defamation. Out of the initial 28 reported data instances, 22 pieces of evidence were identified, resulting in an impressive 79% accuracy rate. The investigative procedures align with the chain of custody, ensuring the reliability of the collected evidence. This study not only contributes valuable insights into digital evidence discovery in online defamation cases but also highlights the efficacy of static forensics as a method. These findings provide a foundation for robust digital forensic practices, crucial for addressing challenges posed by online defamation on social media platforms.

Keywords: Digital Evidence; Static Forensics; Defamation; Chain of Custody.

Received: 15 August 2023 Revised: 19 October 2023 Accepted: 6 December 2023

Introduction

In the era of information technology development, social media is becoming increasingly popular and continues to evolve (Bimo, 2017; Yusuf, 2023). Social media is an online service that enables communication through the internet (Noorikhsan et al., 2023). One of the popular platforms is Twitter, where users can express their thoughts through images, videos, or text (Guraba, 2021). Unfortunately, the spread of fake news continues to rise, and many people easily believe in it. In facing this issue, digital forensics becomes an effective method to uncover the truth of digital evidence and identify perpetrators in cases of defamation on social media (DSLA, 2023).

There are several methods and applications used in digital forensics to reveal the truth of digital evidence (Priyono et al., 2022). A study (Anggraini et al., 2022) used the static forensics method to uncover the truth of digital evidence on the TikTok application, using the Magnet AXIOM application and achieving an accuracy rate of 77%. In the research by (Ardiningtias et al., 2021), also using static forensics in a Digital investigation case on Facebook Messenger, the MOBILedit Forensics Express application was employed with an accuracy rate of 85.71%. And in the study by (Utami et al., 2021), the live forensic method was used to prove cases of electronic transaction fraud on WhatsApp web using the FTK Imager and Browser History Viewer applications, with an accuracy rate of 45.6% out of a total of 46 messages and 39% out of a total of 46 timestamps on messages (Leonardo & Indrayani, 2021).

The static forensics method has advantages in uncovering information from digital evidence that is inactive or deleted after the incident, while the live forensic method can obtain evidence directly from a running system quickly (Nurhairani & Riadi, 2019), (Sulianta, 2013). However, static forensics cannot identify real-time changes on devices, whereas live forensics is limited to active systems and cannot trace or obtain evidence if the system is not in an active state (Hariyadi, 2022).

*Corresponding author.
E-mail address: reskibadillah@gmail.com (Reski Badillah)

Based on previous research, the conclusion that can be drawn is that not all available or investigated evidence in previous studies was successfully obtained (Abdi, 2021), (Pedapudi & Vadlamani, 2023). Although digital forensics continues to evolve, there are still limitations in collecting evidence from specific devices or platforms, such as strong privacy protection, including the issue of defamation that is currently prevalent (Casey et al., 2022). This research aims to investigate the collection and preservation of activity traces or digital evidence related to defamation on Twitter (Efendi et al., 2020), (Yudhana et al., 2019). The main focus is to measure the accuracy of discovering digital evidence related to the prevalent issue of defamation (Kusbiyanto, 2022). The static forensics method is used to identify and collect relevant evidence from Twitter accounts (Casey, 2009). Analysis tools such as Belkasoft Evidence Center X, Belkasoft Remote Acquisition, and Paraben's E3 Universal are applied in this study, with the hope of further uncovering cases of defamation on Twitter (Mukti, 2017).

Method

The primary goal of static forensics is to identify, collect, and analyze digital evidence that can be used in legal investigations (Rafique & Khan, 2013). This method can assist in uncovering criminal activities (Sachdeva et al., 2020), cybercrimes, or other illegal activities that occur through digital devices or media (Salamh et al., 2021). In practice, static forensics involves analyzing various types of files and data within image forensics, such as text files, image files, audio files, video files, log files, system files, and metadata (Yaacoub et al., 2021).

The method used in this research is static forensics (Waseem et al., 2021), which consists of several stages:

a. Identification
   In this identification stage, preparing equipment for the investigation process is based on the created case scenario. This includes determining what is needed to find digital evidence.
b. Data Collection
   Collecting data or gathering evidence, in the form of the target investigative smartphone. The evidence is the Samsung Galaxy J7 smartphone, as seen in Table 1.

Table 1. Smartphone Specifications

Samsung Galaxy J7 Smartphone Specifications	
Specifications	Type
Model	SM-J700F
Android Version	6.0.1
IMEI 1	352846072333925
IMEI 2	352847072333923
SIM Card	Yes

c. Analysis
   Copying data from the target device using applications like Belkasoft Evidence Center X (Delija et al., 2022), Belkasoft Remote Acquisition, and Paraben's E3 Universal (Perumal & others, 2022). The data acquisition process from the smartphone or target device to the laptop is done using a data cable. The acquisition process takes a considerable amount of time depending on the storage capacity of the smartphone. After completing the data acquisition process, an examination of metadata information is conducted, searching for evidence such as image files, text messages, comments, account information, or Twitter IDs related to the initial data. The data search process also takes time, depending on the number of files acquired and the amount of data or evidence that needs to be found.
d. Reporting
   This stage involves displaying the data resulting from the analysis, followed by data matching or accuracy calculation using the percentage formula between the initial data (victim) and the data resulting from the analysis (perpetrator). The percentage calculation results determine the accuracy level of discovering digital evidence between the initial data and the analysis results. After accuracy calculation, the suspect is identified, and then a report on the investigation results of the defamation case on the Twitter application is presented. The investigation report takes the form of a chain of custody report.

The design method of Digital Forensic Evidence Analysis in Revealing Defamation on Social Media (Twitter) Using the Static Forensics Method is as follows:

1. Case Scenario Design
   This research creates a scenario in which the perpetrator posts negative content about the victim using a fake account. The purpose of running this scenario is to facilitate the investigation of social media Twitter defamation cases. The scenario unfolds as follows, figure 1.

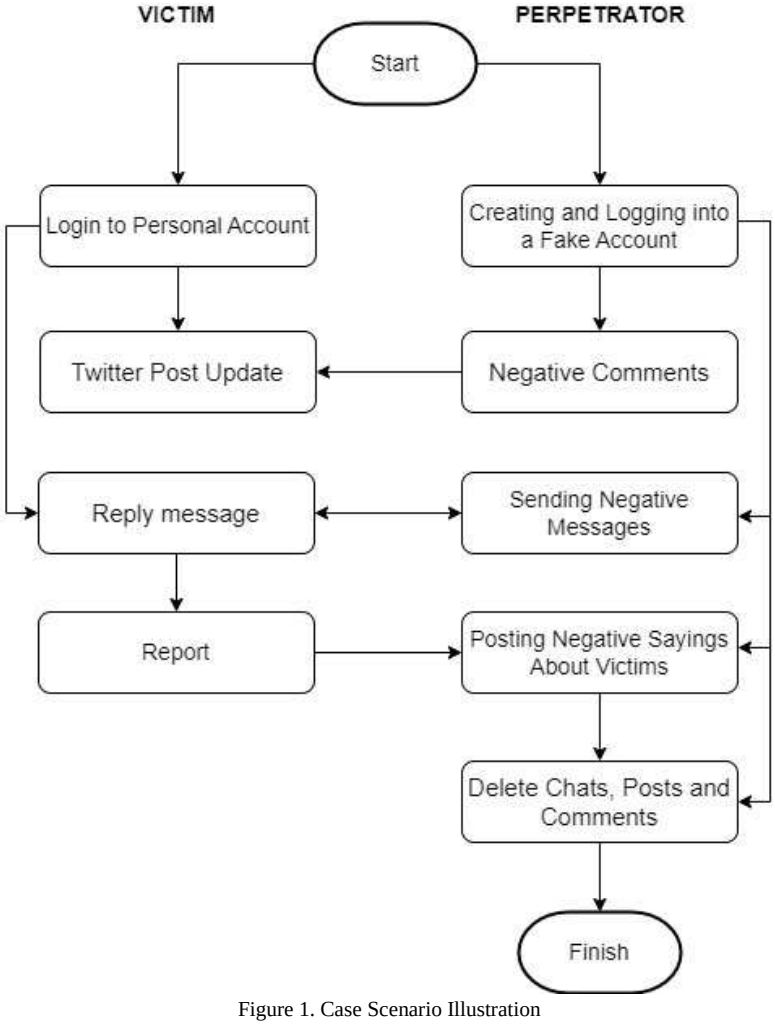


Figure 1. Case Scenario Illustration

Initially, the perpetrator creates a fake account on the Twitter application and uses it to comment on one of the victim's posts. Subsequently, the perpetrator uses the fake account to send messages to the victim. After not receiving a response from the victim, the perpetrator sends messages containing negative or demeaning words. The perpetrator also resumes commenting on the victim's posts with defamatory remarks (Javed et al., 2022). The victim, responding to these messages, tries to identify the perpetrator's identity. Next, the perpetrator posts false information about the victim. After making posts, and comments, and sending negative messages, the perpetrator promptly deletes the text messages and comments. Feeling disturbed by the negative messages and comments, the victim reports the suspected perpetrator to the authorities for investigation. In this study, it is assumed that the perpetrator is a coworker who initially showed interest in the victim.

However, after being rejected, the perpetrator did not accept the rejection, leading to the decision to engage in defamation against the victim.

2. Investigation Flow

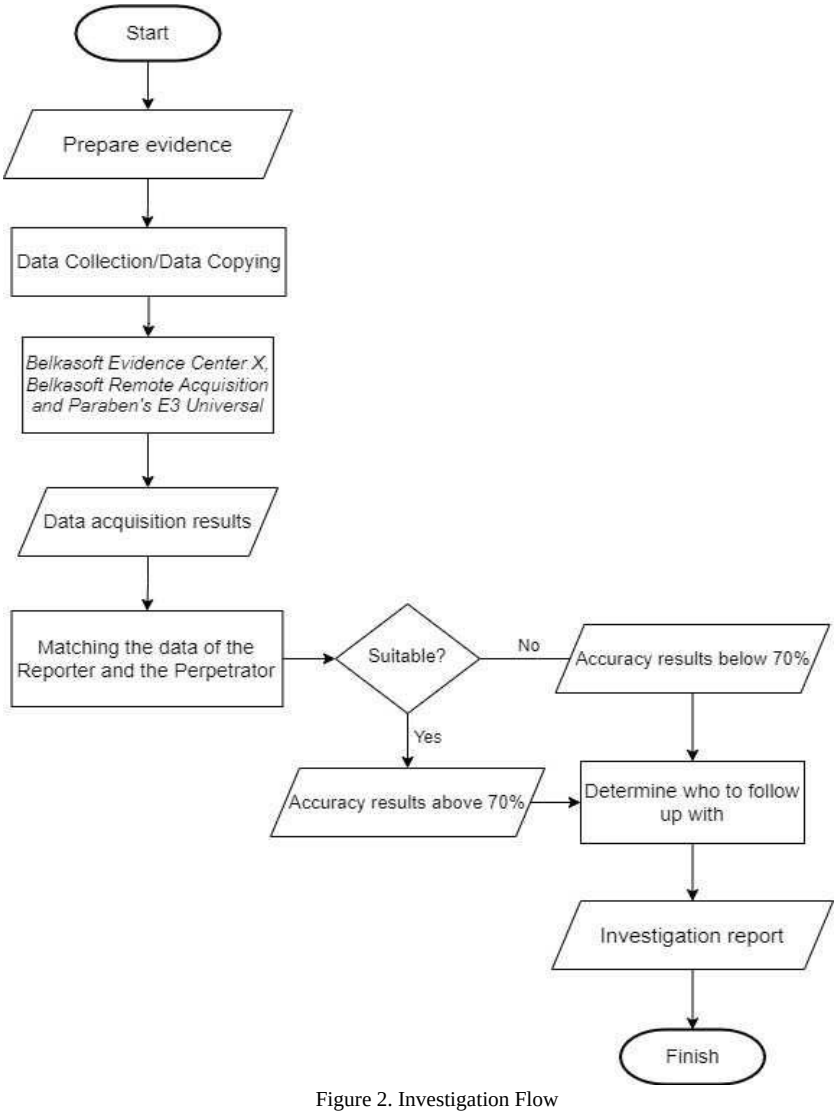


Figure 2. Investigation Flow

The investigation process in Figure 2, begins with data collection or preparing evidence for examination. This involves copying or retrieving data from the target device using applications such as Belkasoft Evidence Center X, Belkasoft Remote Acquisition, and Paraben's E3 Universal. After acquiring or retrieving data, the next step is to examine the data, searching for evidence such as image files, text messages, comments, posts, account information, or Twitter IDs related to the initial data (Khweiled & Jazzar, 2021). Following the examination of relevant data or evidence, the next step is to match the evidence between the initial data and the results of the analysis by calculating the accuracy level to determine the validity of the evidence. Subsequently, identifying who needs further action, the investigation results are presented in a report handed over to the appropriate authorities.

Results and Discussion

Result

Through the application of the static forensics method, this study successfully identified key defamatory elements embedded within social media posts on Twitter. The method proved instrumental in extracting and analyzing textual content, images, and associated metadata, offering a comprehensive understanding of the context and nature of defamatory material. The results of the study from Digital Forensic Evidence Analysis in Revealing Defamation on Social Media (Twitter) Using the Static Forensics Method are as follows:

1. Case Scenario
   In this research, utilizing the static forensics method, a scenario is outlined within a Twitter scene, involving the victim's Twitter account named @DillaLyla and the perpetrator's Twitter account named @Velakhu. Initially, the perpetrator merely commented on one of the victim's posts, greeting the victim, and also sent a message to which the victim did not respond to. Subsequently, the perpetrator began commenting on the victim's posts with unpleasant words. Moreover, on the perpetrator's Twitter account, derogatory comments accompanied by the victim's photo were posted. Feeling disturbed by the perpetrator, the victim reported the case to the authorities, citing violations of the ITE Law Article 27 Paragraph (4) on defamation and/or character assassination through electronic media. Upon learning of the report, the perpetrator then deleted chats, and posts, and changed the Twitter ID and name that were previously associated with the victim.
2. Identification
   To carry out the investigative process to find digital evidence, careful preparation of all necessary equipment is essential, including computers, forensic software, and required cables throughout the investigation.

Table 2. Research Materials and Tools

Tool's Name	Description	Information
Laptop	Lenovo ThinkPad X260, RAM 8,00 GB, Windows 10 Pro	Hardware
Smartphone	Samsung Galaxy J7	Hardware
USB Cable	USB Micro	Smartphone Connector
Belkasoft Evidence Center X	V.2.0.132777	Software
Belkasoft Remote Acquisition	V.1.2.12161	Software
Paraben's E3 Universal	V. 3.7.16206.20452	Software

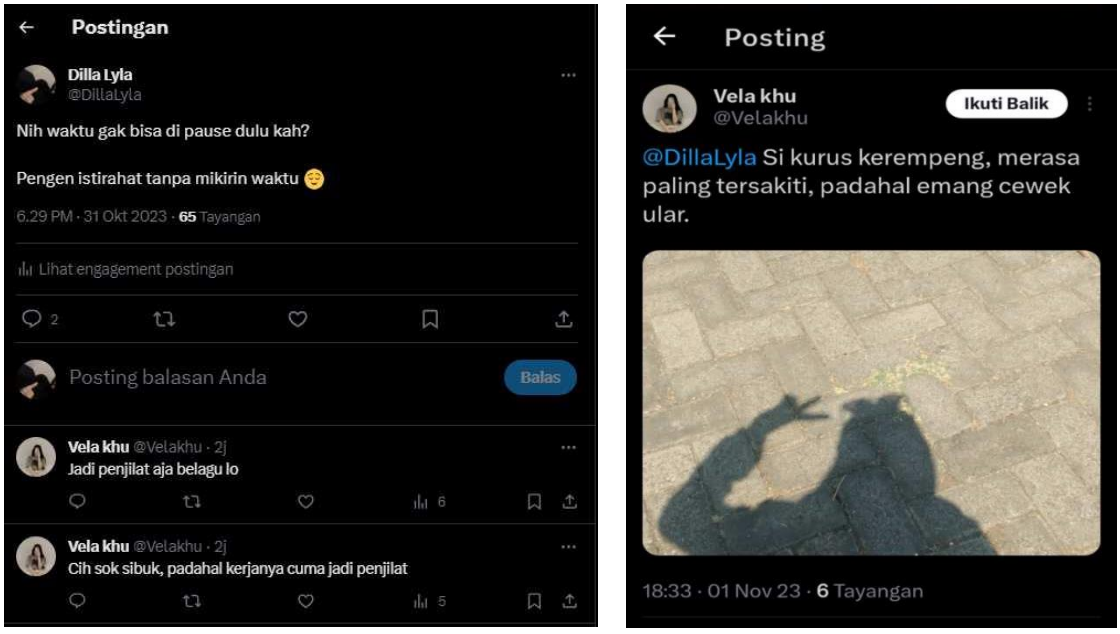
3. Collection of Evidence
   After receiving a report related to the violation of the Electronic Information and Transactions Law (ITE Law), the investigative team promptly took action by securing items suspected to be evidence in the defamation case on the Twitter platform. During the investigation at the perpetrator's residence, the investigative team found a Samsung Galaxy J7 smartphone suspected to be used in the commission of the alleged crime.

Table 3. Evidence

Name of Evidence	Picture	Description	Information
Samsung Galaxy J7		Version Number MMB29K.J700FXXU4BVH1 6.0.1 IMEI (1) 352846072333925	Hardware

4. Device-related Case
   The perpetrator in this issue is faced with a case involving the use of their mobile device in acts of defamation and derogatory remarks against the victim. This case is related to applicable laws, and in the submitted report, the victim attached screenshots documenting the criminal actions performed by the perpetrator. This serves as tangible evidence supporting the charges against the perpetrator in the context of this case.

Figure 3. Defamation and Hate Speech



(a) (b)

Figure 4. (a) Perpetrator's Comments (Hate Speech) and (b) Perpetrator's Post (Insulting Victim)

In the image, a compelling narrative unfolds as it captures the perpetrator's actions. Initially, the wrongdoer downloads a picture from the victim's account, setting the stage for an act of digital transgression. Subsequently, the perpetrator takes a step further by posting the victim's photo on a public platform, accompanied by an unpleasant caption. This deliberate attempt to tarnish the victim's image is intensified by the inclusion of a tagged mention to the victim's Twitter account. The act of tagging not only amplifies the visibility of the defamatory content but also directly involves the victim, ensuring their notification and potential exposure to the harmful post. This image encapsulates a critical moment in the perpetration of online

defamation, serving as digital evidence that can be instrumental in legal proceedings and investigations to hold the perpetrator accountable for their actions.

Article 27 paragraph (3) of the ITE Law also regulates defamation. Perpetrators charged under this article may face imprisonment for up to 4 years and/or a maximum fine of IDR 750,000,000.00 (seven hundred fifty million Indonesian Rupiah). Furthermore, in the revision of Law No. 19 of 2016, it is explained that the provision in Article 27 paragraph (3) constitutes a criminal complaint. Spreading information to incite hatred or hostility towards individuals and/or specific groups based on ethnicity, religion, race, and inter-group (SARA) is also prohibited under Article 28 paragraph (2) of the ITE Law. The punishment for perpetrators of hate speech as described in Article 28 paragraph (2) is imprisonment for a maximum of 6 years and/or a fine of up to IDR 1,000,000,000.00 (one billion Indonesian Rupiah).

Discussion

The temporal analysis conducted through static forensics emerges as a valuable tool for unraveling the chronological evolution of defamatory content on Twitter. This temporal perspective provides a holistic view of the lifecycle of such content, aiding in the identification of patterns, modifications, and dissemination dynamics over time. This stage, begins with the acquisition of data on the Samsung Galaxy J7 device using tools such as Belkasoft Evidence Center X, Belkasoft Remote Acquisition, and Paraben's E3 Universal (Lwin et al., 2020).

Acquisition using Belkasoft Remote Acquisition:

1. After logging into Belkasoft Remote Acquisition, to initiate the acquisition, connect the Samsung Galaxy J7 device using a USB cable. Once connected, click the Acquire button > Mobile > ADB Backup > Click the folder for storing the acquisition results > Start. Then, wait for the acquisition process to complete. The duration of the acquisition process depends on the amount of data on the Samsung Galaxy J7 device.
2. Searching for evidence in Belkasoft Evidence Center X

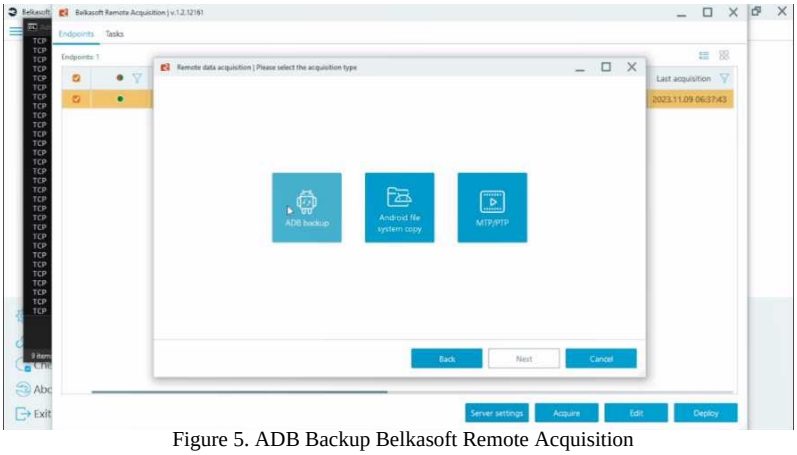


Figure 5. ADB Backup Belkasoft Remote Acquisition

Open Belkasoft Evidence Center X > Add Data Source > Add Existing > Mobile Image > Then select the acquisition result file from Belkasoft Remote Acquisition.

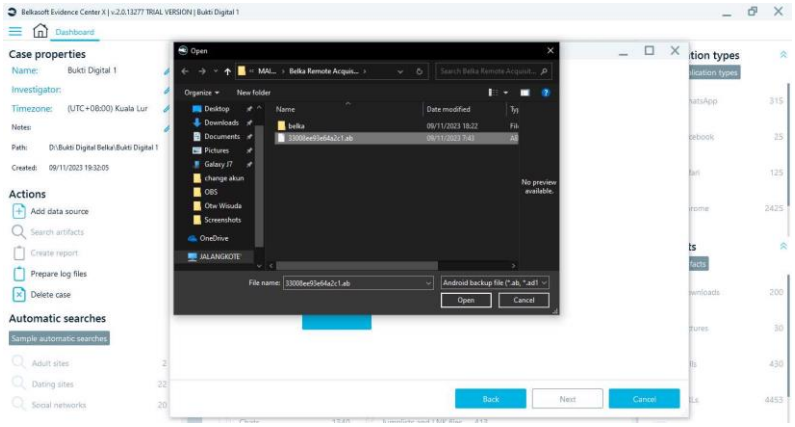


Figure 6. Acquisition files from Belkasoft Remoter Acqusition

The digital evidence successfully found includes image files, the perpetrator's accounts @Velakhu and @tershangKha, where the @Velakhu account was changed to @tershangKha. Additionally, there are ongoing tweet posts with the caption, "Assalamualaikum dunia," created on October 8th. Acquisition using Belkasoft Remote Acquisition Paraben's E3 Universal:

1. After accessing Paraben's E3 Universal > Create New Case > Enter the Case name "Digital Evidence" > choose the Case storage location. Connect the Samsung Galaxy J7 device using a USB cable, then click Start Acquisition > Android > Custom Logical Acquisition > Continue > Start Acquisition > Wait for the acquisition process to complete.

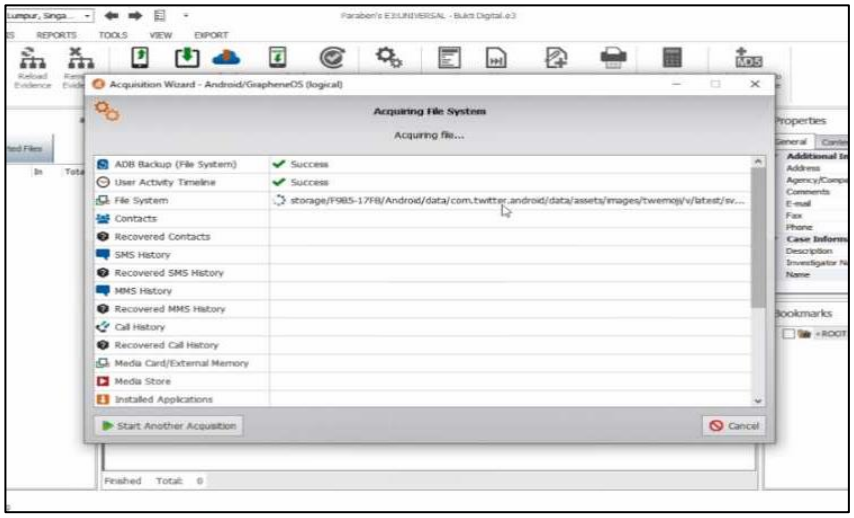


Figure 7. Paraben's E3 Universal Acquisition Process

2. Searching for digital evidence
   The obtained digital evidence includes deleted text comments and posts, image files, emails, as well as the username of the perpetrator.

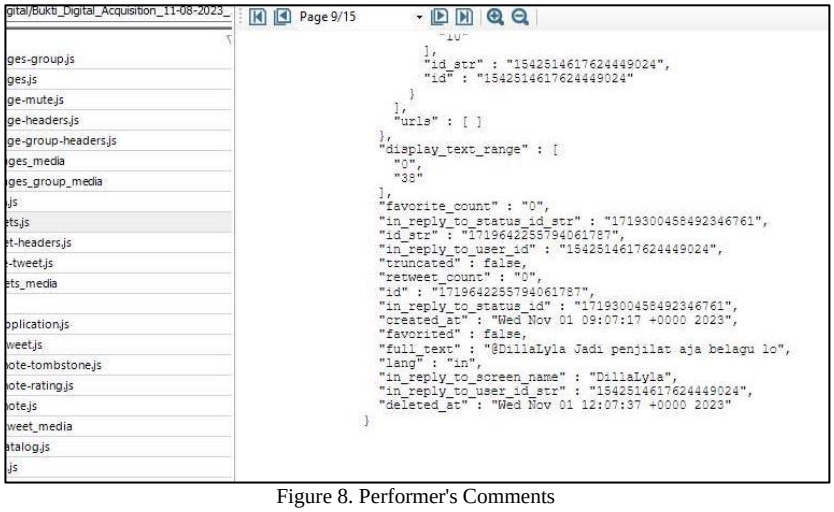
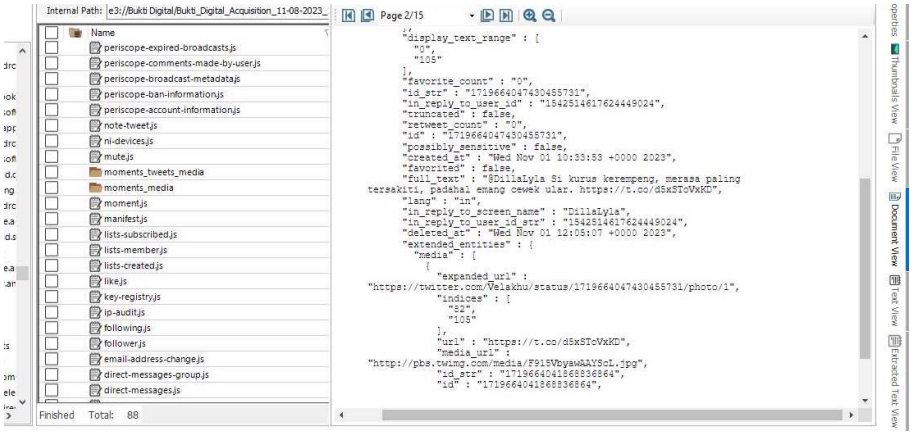


Figure 8. Performer's Comments

One of the deleted posts by the perpetrator had the caption, '@DillaLyla "*Si kurus kerempeng, merasa paling tersakiti, padahal emang cewek ular*," accompanied by a photo of the perpetrator.



(a)

(b)

Figure 9. (a), (b) Deleted Posts

Twitter ID, the perpetrator's username @Velakhu, which was changed to @tershangKha.

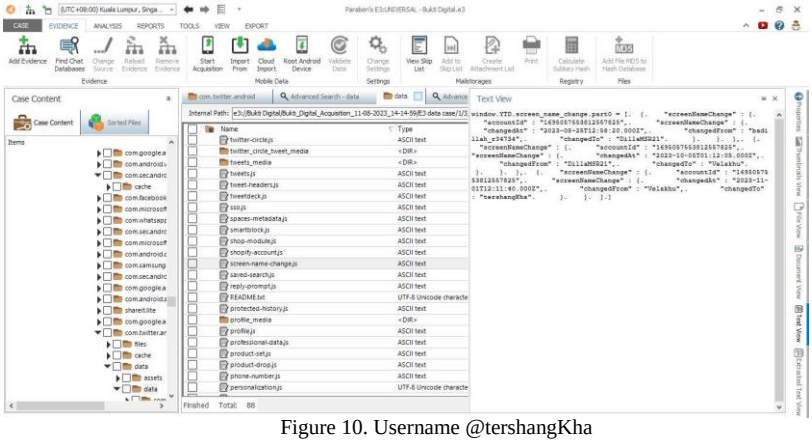


Figure 10. Username @tershangKha


```
  "screenNameChange" : {
 "accountId" : "1695057553812557825",
 "screenNameChange" : {
  "changedAt" : "2023-11-01T12:11:40.000Z",
  "changedFrom" : "Velakhu",
  "changedTo" : "tershangKha"
```


Table 4. Successful evidence found

Tipe Data	Jumlah	*Belkasoft Evidence Center X*	Paraben's E3 Universal
Email	2	1	1
Username / Id	4	2	✓
Deleted Image Files	2	✕	✓
Profile Image File	1	✓	✓
Deleted Comment	10	✕	✓
Deleted Post	2	✕	✓
Chat	6	✕	✕
Ongoing Posts	1	✓	✓
Total	28	5	21
Total data found		22	

The results of the acquisition process and the search for digital evidence are attached in the table. The initial data reported by the victim amounted to 27, and the data successfully found through analysis amounted to 21. The percentage is calculated as follows:

$$\begin{aligned} \text{Percentage} &= \frac{\text{Partial Value}}{\text{Total Value}} \times 100\% \\ &= \frac{22}{28} \times 100\% \\ &= 0{,}7857 \times 100\% \\ &= 78{,}57\ \% \end{aligned}$$

The success rate in uncovering digital evidence reaches an impressive 79%. The investigation procedure stipulates that once the accuracy rate surpasses the 70% threshold, legal authorities are mandated to initiate follow-up actions against the perpetrator. Specifically, these actions fall under the defamation case outlined in Article 27 paragraph (3) of the ITE Law. This stringent criterion emphasizes the gravity of online defamation and the importance of meeting a substantial evidentiary standard before legal measures are taken. The procedural framework for conducting this investigation is meticulously governed by the order and comprehensive report detailing the chain of custody investigation results. This approach ensures a systematic and accountable process in handling cases of digital defamation, providing a robust foundation for law enforcement to pursue decisive and just actions by the stipulations of the law.

Conclusions and Suggestions

Conclusions

After analyzing the discovery of digital evidence in the case of defamation on the social media platform Twitter, the following conclusions can be drawn. The research results indicate that out of the initial 28 data (victim's reporting data), 22 data were successfully found through analysis. The investigation procedure aligns with the order and the report of the chain of custody investigation, ensuring the preservation chain of data or evidence in the defamation case. The investigation report revealed successfully found data, including emails, usernames/IDs, deleted comments and posts by the perpetrator, the perpetrator's profile picture, and images deleted along with two posts by the perpetrator. The evidence also showed that the perpetrator changed their username after committing the crime. The success rate of finding digital evidence in this investigation is 79%. Based on the investigation process, if the accuracy rate is above 70%, the authorities will proceed with taking action against the perpetrator under Article 27 paragraph (3) of the ITE Law.

Suggestions

Based on the research on defamation on the Twitter social media platform, the following recommendations are proposed for further development. Utilize the latest and most advanced tools in the data collection process. By using these advanced tools, it is expected that data searches with keywords will become more efficient, saving time, and facilitating the identification of digital evidence without the need to search each acquisition data individually. And consider adding superior tools to find deleted data such as chat records to achieve a better accuracy rate in the discovery of digital evidence.

Acknowledgments: Thank God Almighty for the blessings given in completing this research.

References

Abdi, H. (2021). Pengertian Analisis menurut para ahli, Kenali fungsi, tujuan, dan jenisnya. *Diambil Kembali Dari Pengertian Analisis: Https://M. Liputan6. Com/Hot/Read/4569178/Pengertian-Analisis-Menurut-Para-Ahlikenali-Fungsi-Tujuan-Dan-Jenisnya*.

Anggraini, F., Herman, H., & Yudhana, A. (2022). Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers. *JURIKOM (Jurnal Riset Komputer)*, *9*(4), 1117–1127.

Ardiningtias, S. R. A., Sunardi, S., & Herman, H. (2021). Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice. *Jurnal Informatika Polinema*, *7*(4), 19–26.

Bimo. (2017). *Perkembangan Media Sosial di Indonesia*. PakarKomunikasi.Com. https://pakarkomunikasi.com/perkembangan-media-sosial-di-indonesia

Casey, E. (2009). *Handbook of digital forensics and investigation*. Academic Press.

Casey, E., Nguyen, L., Mates, J., & Lalliss, S. (2022). Crowdsourcing forensics: Creating a curated catalog of digital forensic artifacts. *Journal of Forensic Sciences*, *67*(5), 1846–1857.

Delija, D., Sudec, D., Sirovatka, G., & Žagar, M. (2022). How to do a forensic analysis of Android 11 artifacts. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1042–1047.

DSLA, A. (2023). *Apa Saja yang Termasuk Pencemaran Nama Baik ? - DSLA (Daud Silalahi & Lawencon Associates)*. Dslalawfirm. https://www.dslalawfirm.com/id/perbuatan-yang-termasuk-pencemaran-nama-baik/

Efendi, T. F., Rahmadi, R., & Prayudi, Y. (2020). Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital. *J. Teknol. Dan Manaj. Inform*, *6*(2), 53–63.

Guraba. (2021). *Praktik Chains of Custody dalam Penanganan Alat Bukti Elektronik - TIMES Indonesia*. Timesindonesia. https://timesindonesia.co.id/kopi-times/387090/praktik-chains-of-custody-dalam-penanganan-alat-bukti-elektronik

Hariyadi, D. (2022). *Buku Panduan Dasar Forensik Digital*. CV Baskara Media. https://www.researchgate.net/publication/365993681_Buku_Panduan_Dasar_Forensik_Digital

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089.

Khweiled, R., & Jazzar, M. (2021). An Improved Framework For cyberbullying Investigation Process on WhatsApp application. *J. Xi'an Univ. Archit. Technol.*, *13*(9), 238–246.

Kusbiyanto, A. (2022). *Fakultas Kedokteran UNS | Pentingnya Ahli Forensik dalam Sistem Peradilan Pidana Indonesia*. Uns. https://fk.uns.ac.id/index.php/berita/detail/662/pentingnya-ahli-forensik-dalam-sistem-peradilan-pidana-indonesia

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.

Lwin, H. H., Aung, W. P., & Lin, K. K. (2020). Comparative analysis of Android mobile forensics tools. *2020 IEEE Conference on Computer Applications (ICCA)*, 1–6.

Mukti, W. A. (2017). *Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android* [{B.S.} thesis]. Fakultas Sains Dan Teknologi Universitas Islam Negeri Syarif Hidayatullah~….

Noorikhsan, F. F., Ramdhani, H., Sirait, B. C., & Khoerunisa, N. (2023). Dinamika Internet, Media Sosial, dan Politik di Era Kontemporer: Tinjauan Relasi Negara-Masyarakat. *Journal of Political Issues*, *5*(1), 95–109.

Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. *International Journal of Computer Applications*, *177*(27), 35–42.

Pedapudi, S. M., & Vadlamani, N. (2023). Digital forensics approach for handling audio and video files. *Measurement: Sensors*, *29*, 100860.

Perumal, V., & others. (2022). *A Comprehensive Survey and Analysis on Multi-Domain Digital Forensic Tools, Techniques and Issues*.

Priyono, P., Wahid, B. A., Priatno, P., Iskandar, R., Akbar, A., & Putra, A. S. (2022). Investigations Using The Whatsapp Application By Analyzing Evidence of Crime In Conversation Data. *IJISTECH (International Journal of Information System and Technology)*, *6*(1), 152–158.

Rafique, M., & Khan, M. N. A. (2013). Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific \& Engineering Research*, *4*(10), 1048–1056.

Sachdeva, S., Raina, B. L., & Sharma, A. (2020). Analysis of digital forensic tools. *Journal of Computational and Theoretical Nanoscience*, *17*(6), 2459–2467.

Salamh, F. E., Karabiyik, U., Rogers, M. K., & Matson, E. T. (2021). A comparative uav forensic analysis: Static and live digital evidence traceability challenges. *Drones*, *5*(2), 42.

Sulianta, F. (2013). *Komputer Forensik*. Elex Media Komputindo.

Utami, S. D., Carudin, C., & Ridha, A. A. (2021). Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik. *Cyber Security Dan Forensik Digital*, *4*(1), 24–32.

Waseem, Q., Alshamrani, S. S., Nisar, K., Wan Din, W. I. S., & Alghamdi, A. S. (2021). Future technology: Software-defined network (SDN) forensic. *Symmetry*, *13*(5), 767.

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. *ArXiv Preprint ArXiv:2103.17028*.

Yudhana, A., Riadi, I., & Zuhriyanto, I. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS). *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, *20*(2), 125–130.

Yusuf, M. (2023). *Tren Penggunaan Internet dan Media Sosial dalam Era Konvergensi Media - Kompasiana.com*. Kompasiana. https://www.kompasiana.com/muhammad99498/653b18cc110fce5247396822/tren-penggunaan-internet-dan-media-sosial-dalam-era-konvergensi-media