ABSTRACT
Tiktok application is an application that is being used a lot, so it causes many criminal acts such as defamation, cybercrime, and cyberbullying. This study uses a forensic method as a standard in the research phase to reveal evidence of pollution crimes that occur in the TikTok web browser application. The method used in this research is the National Institute of Standard Technology (NIST). This method has 4 stages used for reference in the analysis of evidence, namely analysis, collection, examination, and reporting. This research uses a laptop which is used as experimental material in the scenario. This case uses a Chrome web browser in public mode where a laptop is logged into Tiktok with the Chrome browser used to post videos. This research uses tools, forensically named FTK Imager, Browser History Capture / Viewer, Video Cache Viewer. The results obtained from this study are data or evidence from a post that has been deleted in the TikTok web browser application. The results obtained from the process of this research stage are in the form of text, username, photos / videos, and links from posts that the suspect has deleted. Based on the tools used in this study, 80% managed to get butik goods and 20% failed, namely video. The evidence found can then be used to report and assist in the trial process.

Keywords
Forensics, Tiktok, Web, Browser, NIST.

1. INTRODUCTION
Progress of science and technology has a very big influence in various fields of human life [1]. The internet is becoming a new digital space that creates a cultural space [2]. The rapid development of this technology is followed by the development of software such as social media, now many social media services are Instagram, Facebook, Twitter and Tiktok. Social media has changed the world a lot. Pervert a lot of thoughts and theories that are owned. The level or level of communication merges in one container called social networking / social media [3]. Almost everyone from all walks of life has a social media application, because social media is used for various needs, such as sharing information, selling, and entertainment. Personal freedom in conveying ideas, criticism, suggestions and even "blasphemy" is often encountered every hour and day through various variants of the media used [4]. Social media itself has services such as text messages, video posts and photos. TikTok is a social media platform created by a Chinese company in September 2016. TikTok is the international version of the Chinese mobile short video platform Douyin. It is owned by Chinese tech giant Bytedance. Continued growth from 2019 to 2020, surpassing 2 billion downloads in April 2020 amid the ongoing global health crisis [5]. Tiktok is a platform that allows users to create videos up to 1 minute long with a number of features. Tiktok users can follow the accounts they like, give hearts, comment, and share videos on other platforms. Videos, hashtags, sounds and effects can be added to the Favorites section of the user account. The level of convenience provided by the Tiktok application in making videos and editing videos, this creates the potential for cyber bullying and even defamation. Legal provisions for criminal acts of defamation and insult are regulated in Law Number 32 of 2002 concerning Broadcasting, Law Number 11 of 2008 concerning Electronic Information and Transactions, and several other sectoral or special laws [6]. Defamation cases can be revealed on social media with the help of digital forensics using the NIST (National Institute of Standard Technology).

1.1 Literature Study
1.1.1 Previous Research
The literature study stage was carried out to provide a reference to increase knowledge in conducting research. Fadillah, Umar, and Yudhana (2018) explains the process of applying forensic cases to an Android-based mobile payment application using a research method that refers to guidelines mobile device forensics created by the National Institute of Standards and Technology (NIST). In the process of lifting digital evidence for smartphones that have been installed with the mobile payment application, rooting is required for Android smartphones, and there are many tools that can be used in the process of lifting digital evidence that runs on the Windows platform [7].

Yudhana, Riadi, and Anshori (2018) with a study entitled "Facebook Messenger Digital Evidence Analysis Using the NIST Method" in this study discusses the process of obtaining evidence on an android smartphone using Oxigen forensic forensic software on the Facebook Messenger application. With the conclusion, namely: The results that have been obtained are conversational text, images and audio [9].

Prasongko, Yudhana, and Fadil (2018) which has a research title, "Forensic Analysis of Kakaotalk Applications Using the National Institute of Standards and Technology Method" which has a discussion of digital forensic analysis on KakaoTalk for handling cybercrime. With the conclusion: Digital evidence expected from the process of forensic removal and analysis can help the process of investigating a digital crime [10].

Kunang and Khristian (2016) with the title "Implementation of Forensic Procedures for Analysis of Whatsapp Artifacts on Android Phones". The conclusion is that using the stages of
the WhatsApp application forensic procedure on the platform used in this study produces several conclusions and suggestions that can be used as a standard procedure reference for conducting forensic investigations on the use of WhatsApp Messenger on an Android smartphone in real situations or as a reference for related research.[11.

1.1.2 Digital Forensics
Forensics is an activity to investigate and establish facts relating to criminal activities and other legal issues. Forensics is a part of science that covers the discovery and investigation of data found on digital devices (computers, cellphones / smartphones, tablets, storage and the like), in this case digital forensics can be divided into computer-related forensics (host, server), networks, applications (including 12 databases), and devices (digital devices). Each of them has its own depth[12].

1.1.3 Web Browser
Web browser is an application for accessing web sites via the internet. Web browsers allow users to search for information, read e-mails, communicate via instant messages or social networks, use internet banking and shop through web sites e-commerce [13]. A web browser is a software application for retrieving, presenting, and traversing information sources on the internet or the world wide web (WWW). The source of information is identified by a Uniform Resource Identifier (URL) and may be a web page, image, video, or other piece of content[14]. The web browser itself stores a large amount of data about user activity during browsing, including cache files, Uniform Resource Identifier (URL), keywords, cookies.

1.1.4 Digital Evidence
Methodology evidence is information stored or transmitted in binary form that can be relied on in court. Evidence can be found on computer hard drives, cell phones, personal digital assistants (PDAs), CDs, and digital camera flash cards, among other places. Digital evidence is generally related to digital or electronic crimes, such as pornography, prostitution, identity theft, phishing, credit card or ATM fraud. However, digital evidence is now being used to prosecute all types of criminals, not just digital crimes[15]. Digital evidence is divided into 15 types, namely logical files, deleted files, encrypted audio files, video files, images files, emails, user id / password, etc.

1.1.5 TikTok
TikTok is one of the fastest growing social media platforms in the world. TikTok allows users to create short 15-second videos with music, filters, and several other creative features. In September 2016, the Chinese company ByteDance launched a short video application called Douyin. Within 1 year, Douyin had 100 million users and 1 billion daily video views. Just like most social media platforms, TikTok is also big because users are creating their own content. TikTok is considered a social media platform because like Twitter and Instagram, its users have a social group of followers and other users they follow[16].

1.1.6 Cybercrime
Cybercrime according to the United Nations: any illegal behavior committed by means of, the victim of a computer system or system or network, including crimes such as illegal possession, offering or distributing information through computer systems or networks. There are many different categories to explore what is meant by cybercrime, one of which is to divide cybercrime into two major groups, namely: Violent / potentially violent, and Non-Violent [17].

1.1.7 National Institute of Standard Technology
National Institute of Standard Technology (NIST) has four main areas including biotechnology, nanotechnology, information technology, and modern manufacturing. NIST provides standardized methods that can be used to solve problems and perform analysis of digital evidence or stages to obtain information from digital evidence [18]. The National Institute of Standard and Technology (NIST) stages have 4 stages that will be used to carry out investigations on mobile forensic cases.

2. METHODOLOGY
2.1 Research Scenario
The case study used in this research is the distribution of videos containing defamation through content uploaded on social media, tiktok web. The simulation of this case is a suspect who uses the Chrome web browser to log into Tiktok and then uploads a video and in quite a while the post is deleted. The acquisition process is carried out to secure the data running on the computer at that time so as to minimize the loss of evidence. The results are then backed up or copied, these copies can then be continued for forensics. The laptop used by the suspect is alive after being used to post videos to the Tiktok application, as in Figure 1 a simulation of the case of defamation of Tiktok application running on the Chrome browser by logging in using a username and password, the perpetrator posts the video and then it is deleted again. The simulation can be seen in Figure 1.

![Figure 1. Research Scenario](image)

In Figure 1 describes a scenario about how the suspect posted video content to his Tiktok account and was deleted by the suspect when someone felt harmed or harassed.
2.2 Research Stages
The stages of this research are where the case study simulation process can be carried out in stages to try to find a crime butt from the Tiktok web application based on digital evidence. The research stages can refer to a method, namely the National Institute of Standards and Technology (NIST), which has several steps that can be taken to produce evidence. The National Institute of Standard and Technology (NIST) stages have 4 stages that will be used to carry out investigations on mobile forensic cases. Explanation 4 stages following method as shown in Figure 2:

![Figure 2. NIST Method Stages](image)

mobile forensicStagesNational Institute of Standards Technology (NIST), there are several stages as follows:

1. Collection The collection stage identifies, labels, records, and retrieves data from relevant data sources by following data integrity preservation procedures.
2. Examination The Examination Phase processes the collected data forensically using a combination of various scenarios, both automatic and manual, assessing and releasing data as needed while maintaining data integrity.
3. Analysis The Analysis phase analyzes the results of the examination using technically and legally justified methods to obtain useful information and answer questions that drive collection and examination.
4. Reporting The reporting stage is to report the results of the analysis which includes a description of the actions taken, an explanation of the tools and procedures selected, the determination of other actions that need to be taken (for example, forensic examinations of additional data sources, identified security gaps, or increased security controls), and provide recommendations for improving policies, procedures, equipment, and other aspects of the forensic process[19].

3. RESULT AND DISCUSSION
The scenario of the case of spreading pornographic content on social media Twitter is trying to be revealed by conducting forensics on physical evidence, namely the alleged perpetrator's laptop. The tools and materials needed, among others, can be seen in Table 1.

### Table 1. Tools and Materials

| No | Tools and Materials | Information |
|----|---------------------|-------------|
| 1  | Laptop              | Laptop suspect with the MSI GL62M 7RDX brand, Intel Core i7-7700HQ @ 2.80GHz, RAM: 8GB, HDD: 1TB, Windows 10 x64 |
| 2  | FTK Imager          | To read the capture results from the ram capturer and use it to check the hash value of the ram acquisition results and is used to search for evidence based on the parameters you are looking for |
| 3  | Browser History Viewer | To read the capture results from tool Browser History Capturer |
| 4  | Browser History Capturer | To retrieve history from browser including cached images and web |
| 5  | Cached Video Viewer | To get evidence. |

### Table 2. Physical Evidence

| No | Evidence | Description |
|----|----------|-------------|
| 1  | Laptop with the MSI GL62M 7RDX brand that was found turned on and connected to the internet at the TKP |

Table 2 is documentation of evidence with specifications obtained from the scene of the incident, namely a MSI laptop with type GL62M-7RDX with intel core i7-7700HQ and 8GB RAM and 1TB HDD storage with a Windows 10 OS which was found to be on and still connected to the internal in filling out the Questionnaire.

3.2 Examination
This stage is a major stage in an investigation to acquire data on evidence from a suspect's laptop.

3.2.1 FTK Imager
In the process of collecting data from RAM memory or
Capture memory, can be used a tool forensics such as FTK Imager, the data collection process is as in Figure 3.

**Figure 3. FTK Imager acquisition**

Data collection by means of memory capture. The way to capture is to select the file menu and click on the memory capture feature. The results will be saved with the .mem extension.

### 3.2.2 Browser History Capture

In the Chrome application, data acquisition will be carried out using tool to retrieve data from the browser. Data that can be obtained from browser acquisition include history, cache, and archived history. The stages for acquisition with the tool Browser History Capture can be seen in Figure 4.

**Figure 4. Browser History Capture acquisition**

This application has several advantages and several disadvantages. The advantage itself is that tool this does not need to install on the device so it can speed up the data collection process, the drawback is that tool this can only run on a number of applications, namely on Firefox, Chrome, and Internet Explorer & Edge. In the history folder, there are several files such as Bookmarks, Cookies, Current Session, History, Last session, Login Data, Preferences, Top sites, and Web data. The above files will be analyzed using the Browser History Viewer tool.

#### 3.3.2 Video Cache View

Video Cache Viewer is a tool used to acquire videos from browser applications such as Firefox, Opera, and Chrome. The acquisition process involves extracting video files from the video cache in the browser. Automatically all cache from the browser in the form of videos will be read in this tool. The acquisition process can be seen in Figure 5.

**Figure 5. Video Cache View Acquisition**

When tool this is opened, it will immediately carry out the data acquisition process on all browsers on the suspect's laptop according to the type mentioned earlier. When the tool completes the acquisition, you will see all the video results obtained from various sources.

### 3.3 Analysis

The analysis stage is a stage that aims to analyze and see the evidence obtained previously from the Examination stage in detail. The results that have been obtained will later be entered into the table to see the comparison of the results obtained from the various tools used. This analysis uses several tools used by researchers as follows:

#### 3.3.1 Ftk Imager

Analysis Tool FTK Imager are used to analyze the results of examination its before performed using tool TFK Imager also, files that can be seen in Figure 6.

**Figure 6. Results FTK Imager Acquisition**

The acquired files above will then be analyzed. The results obtained from the tiktok keywords that can be used as evidence are as shown in Figure 7.

**Figure 7. Results of the Tiktok keyword**

Shown in Figure 7, the results of the first search can be seen in Figure 7 with the tiktok keywords. The result in the can that link be logged in with a user name "https://www.tiktok.com/foryou?loginType=repeatLogin&lang=en"PTomy Pandella (@tomy_pandella) TikTok.
Figure 8. Results From Keyword Username

Results of Search for the second word in Figure 8, namely the user name of the victim's account which is evidence of a sign of suspicion against the victim, and the results obtained are a user @tmpdl26 which is the victim's user name along with the text "apparently he is" and a hashtag #nakal which is a sentence listed in the caption in the video or content uploaded by the suspect.

3.3.2 Browser History Viewer

The results obtained from the browser acquisition are two folders, namely Chrome and Historical folders. In this study we will retrieve what data in the Chrome folder containing the folder cache and history Folder history contains several files such as Bookmarks, Cookies, Current Session, History, Last session. Login Data, Preferences, Top site, and Web data. above will be analyzed with the tool as Browser History Viewershown in Figure 9.

Figure 9. Results of Browser History Capture

In tool this, the process of extracting files that have been from obtained the tool browser history capture is in the form of a folder capture with the contents the file. The results that have been extracted can be seen in Figure 10.

Table 3. Evidence Specifications

| Brands   | MSI GL62       |
|-----------|----------------|
| Processor | Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz |
| Graphics  | Intel(R) HD Graphics 630 & NVIDIA Geforce GTX1050/2GB DDR5 |
| Memory    | 8GB Memory DDR4 |
| Harddisk  | 1TB 7200RPM |

Applications or software that are forensic or analyzed, namely the Chrome browser with a web, namely Tiktok web. By following several inspection procedures, evidence is analyzed with several tools with their own functions and features, from analysis of the TikTok web social media. So the results that are focused are several things related to the suspect and the Tiktok web social media, for more details, see Table 4.

Table 4. Results of All Methods

| No | Digital Evidence | Operating System | Forensic Software |
|----|------------------|------------------|-------------------|
| 1  | Photo            | Windows 10       | FTK Imager, Browser History Capture/Viewer |
| 2  | Videos           | Windows 10       | FTK Imager, Browser History Capture/Viewer |
| 3  | Text             | Windows 10       | FTK Imager, Browser History Capture/Viewer |
| 4  | User Name        | Windows 10       | FTK Imager, Browser History Capture/Viewer |
| 5  | Links            | Windows 10       | FTK Imager, Browser History Capture/Viewer |

Table 4 is the result of the discovery of evidence on the TikTok web site running on the Chrome web browser. In the tool FTK Imager successfully obtained evidence in the form of text from the post caption uploaded by the suspect, the suspect's user name (@tomypandella) who logged into TikTok and the victim's user name (@tmpdl26) which was marked in the suspect's content caption, and the suspect's link.
when logging in upload content and other activities on tiktok social media. The results of photos and videos (Thummail) were obtained from the tool Browser History Capture / Viewer, the results obtained were in the form of photos of the suspect's account, video (Thummail) of the video content uploaded by the suspect and there was a link and username of the suspect when logging in and uploading the content of the ruthlessness.

3.5 Result
The keywords used to find evidence are photos, videos, text, usernames, and links posts. The results of Tiktok forensics on the Chrome web browser can be seen in table 5.

| Information | FTK Imager | BHC/BHV | VCV |
|-------------|------------|---------|-----|
| Photo       | -          | ✓       | -   |
| Video       | -          | -       | -   |
| Text        | ✓          | -       | -   |
| Username    | ✓          | ✓       | -   |
| Link        | ✓          | ✓       | ✓   |

Based on table 5, the results of this study almost get all the results from the keywords used by 80% and 20% fail, namely video posts.

4. CONCLUSION
Based on the results of research that has been running on the Chrome browser application on Windows 10 with the title “Browser Forensics in Web-Based Tiktok Applications”, collecting forensic evidence by capturing ram and cache using several tools that support the data collection process, such as the FTK Imager tool, browser history capture, and video cache display. To search for evidence yourself using the same tools as FTK Imager, browser history viewer, and video cache view. The results of the evidence generated by several tools are used, then analyzed to find digital evidence in the form of text, caption content, username of suspect and victim, profile photo of suspect and victim, video photo Thummail and source link from Tiktok that the suspect accessed. Based on the tools used in this study, 80% of items were successfully obtained and 20% failed, namely videos.

5. REFERENCES
[1] A. Muhson, “Pengembangan Media Pembelajaran Berbasis Teknologi Informatika,” J. Pendidik. Akunt. Indones., vol. 8, no. 2, 2010.
[2] T. R. Afriluyanto, “Fenomena Remaja Menggunakan Media Sosial dalam Membentuk Identitas,” KOMUNIKA J. Dakwah dan Komun., vol. 11, no. 2, pp. 184–197, 2018.
[3] E. D. S. Watie, “Komunikasi dan Media Sosial (Communications and Social Media),” J. Messenger, vol. 3, no. 2, p. 69, 2016.
[4] A. S. Cahyono, “Pengaruh media sosial terhadap perubahan sosial masyarakat di Indonesia,” J. ilmu Sos. ilmu Polit. diterbitkan oleh Fak. Ilmu Sos. Polit. Univ. Tulungagung, vol. 9, no. 1, pp. 140–157, 2016.
[5] D. B. V. Kaye, X. Chen, and J. Zeng, “The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok,” Mob. Media Commun., 2020.
[6] F. R. Muthia and R. Arifin, “Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara(Cybercrime) Dalam Perkara Pencemaran Namaku Di Indonesia,” Resan J. Hok., vol. 5, no. April, pp. 21–39, 2019.
[7] M. N. Fadillah, R. Umar, and A. Yudhmana, “Rancangan Metode Nist Untuk Forensik Aplikasi,” Semin. Nas. Inform. 2018 (semasiaIP 2018) UPN “Veteran” Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328, vol. 2018, no. November, pp. 115–119, 2018.
[8] R. N. Fitriyaha, B. Diklat, and K. Semarang, “Prosideng SENDI_ U 2019 ISBN : 978-979-3649-99-3 Prosiding SENDI_ U 2019 ISBN : 978-979-3649-99-3,” no. 1, pp. 978–979, 2019.
[9] A. Yudhmana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” It J. Res. Dev., vol. 3, no. 1, pp. 13, 2018.
[10] R. Y. Prasongko, A. Yudhmana, and A. Fadil, “Analisa forensik aplikasi kakaotalk menggunakan metode national institute standard technology,” Semin. Nas. Inform. 2018 (semasiaIP 2018) UPN “Veteran” Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328, vol. 2018, no. November, pp. 129–133, 2018.
[11] Y. N. Kunang and A. Khristian, “Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android,” vol. 2, no. 1, pp. 59–68, 2016.
[12] B. Raharjo, “Sekilas Mengenai Forensik Digital,” J. Sosioteknologi, vol. 12, no. 29, pp. 384–387, 2013.
[13] D. GDharanD and N. Meenan A R, “Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser,” Int. J. Comput. Appl., vol. 91, no. 4, pp. 32–35, 2014.
[14] T. Rochmadi, I. Riadi, and Y. Prayudi, “Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser,” Int. J. Comput. Appl., vol. 164, no. 8, pp. 31–37, 2017.
[15] I. S. Wijaya, H. Riadi, “Analisis Forensik Digital Aplikasi Telegram,” Semantikom, pp. 95–98, 2017.
[16] J. C. Medina Serrano, O. Papakryiakopoulos, and S. Hegelich, “Dancing to the Partisan Beat: A First Analysis of Political Communication on TikTok,” WebSci 2020 - Proc. 12th ACM Conf. Web Sci., pp. 157–166, 2020.
[17] A. Fauzan, I. Riadi, and A. Fadil, “Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime,” Ann. Res. Semin., vol. 2, no. 1, pp. 159–163, 2017.
[18] H. D. Karen Kent, Suzanne Chevalier, Tim Grance, “Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86),” NIST Spec. Publ., no. August, pp. 800–886, 2006.
[19] I. Riadi, A. Yudhmana, M. Caesar, and F. Putra, “Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode Nist,” Semin. Nas. Teknol. Inf. dan Komun. - Semant., pp. 161–166, 2017.