

Browser Forensics on Web-based Tiktok Applications using Digital Forensic Research Workshop Method

Fakhira Annisatul Zahrah
Department of Informatics
Universitas Ahmad Dahlan,
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan,
Yogyakarta of Indonesia

ABSTRACT

The rapid development of the current age of information technology has brought many advantages and disadvantages, one of which is TikTok. However, it still often happens that people misuse this TikTok videos where the content harms certain decent things for public consumption. TikTok also affects society today as a place to spread hoax content. This research aims to obtain digital evidence of cybercrime cases using the current method, namely the Digital Forensic Research Workshop (DFRWS). The method used in this research uses the Digital Forensic Research Workshop (DFRWS) which has 6 stages of research, namely identification, maintenance, collection, examination, analysis, and presentation. The tools used in this research are FTK Imager, Browser History Examiner, Browser History Capture, and Video Cache View. The results of this study are that the FTK Imager obtained results in the form of usernames and Passwords The Browser History Examiner tool obtains evidence in the form of the date and time of uploading the tiktok video. Tools Browser History Viewer obtained 1 proof of the TikTok video thumbnail and the perpetrator's profile photo. Video Cache View tools get 1 proof that deleted videos can be extracted back into a complete video.

Keywords

Cybercrime, Forensik Digital, Digital Forensic Research Workshop (DFRWS), Tiktok.

1. INTRODUCTION

The rapid progress of the current information technology age has brought various positive and negative aspects. A positive influence that can be achieved through the development of information technology is the easier it is for people to obtain and use information and communicate with other people in any part of the world [1][2]. One of the social networking applications that are currently frequent discussed by people in Indonesia is Tiktok [3]. is a social networking application and music video platform where users can create, edit, and share short video clips complete with filters and accompanied by music as support [4].

However, there are still frequent misuses of this TikTok video where the content harms certain decent things for public consumption. TikTok also affects society today as a place to spread hoax content. Hoax content is false or misleading news disseminated in a community environment. Hoax content that applies can come from individuals or organizations that deliberately seek profit and harm other parties [5].

This technological development is followed by software such as social media; now, many social media services are Instagram, Facebook, Twitter and Tiktok. Almost everyone in all walks of life has a social media application because social media is used for various needs such as sharing information,

sales and entertainment facilities [6]. Digital Forensics Research Workshop (DFRWS) is used for the digital forensic analysis stage. This approach facilitates a centralized mechanism for obtaining evidence and recording collected information [7]. In addition, there are other methods available for digital forensics, including the National Institute of Standards and Technology (NIST), the National Institute of Justice (NIJ), Live Forensic, and the Association of Chief Police Officers (ACPO) [8].

This research will use the Digital Forensic Research Workshop (DFRWS) approach because each action taken can provide a complete explanation based on the case being processed and contribute to establishing a system for obtaining evidence and records collected for centralized mechanism information [9]. This research aims to use the Digital Forensics Research Workshop (DFRWS) method to conduct a cyber forensic investigation process on network devices to obtain evidence.

Which can reveal cybercrime cases in the Tiktok application. Hopefully, this research can provide additional education to the public to be more careful about cybercrime in their environment.

2. LITERATURE STUDY

2.1 Digital Forensics

Forensics is an activity consisting of the discovery and ascertainment of facts relating to criminal events and other legal matters. Digital forensics is a branch of forensic science that involves the discovery and examination of materials (data) found on digital devices (computers, cell phones, tablets, PDAs (personal digital assistants), network devices, storage, etc [10] [11].

Digital forensics has a number of sub-fields associated with: Examining different types of devices, media or artifacts, including: Others: Computer forensics, Mobile device forensics, Network forensics, Database forensics [12].

2.2 Web Browser

A web browser is a program or application that provides services containing a collection of plain text or complex text program code commonly known as html, similar in the form of text, graphics, or multimedia vehicles [13].

2.3 Digital Evidence

Digital evidence is an issue that is stored or transmitted in binary form that can be trusted in court [14]. Evidence can be found on computer hard drives, cell phones, personal digital assistants (PDAs), digital camera CDs and flash cards, among other places. Digital evidence is often associated with digital or electronic crimes, such as pornography, prostitution, theft of characteristics, fraud, credit card or ATM fraud. However,

digital evidence is now used to prosecute all types of crimes, not just digital crimes [15]. Digital evidence is complicated to maintain its purity if not handled efficiently [16]. The inclusion of purity in digital evidence can be as useful or useless evidence or conclusions [17].

2.4 TikTok

Tik tok is the most famous and most popular application in the world. Users can create videos for up to 3 minutes with music and effects, and even now, there is such a thing as a tiktoshop for selling online [18]. This application was created by the Chinese company ByteDance which first released an application with a short name called Douyin. In one year, Douyin had 100 million users and an average of 1 billion video views per day [19]. Douyin's popularity has expanded outside of China as Tik Tok. According to a statement by Sensor Tower, the app was downloaded 700 million times in 2019. TikTok will likely surpass some of the apps sponsored by Facebook Inc. This TikTok app is in second place, while Whatsapp has 1.5 billion downloads, TikTok has 1.46 billion active users [20].

2.5 Cybercrime

Cybercrime is a type of crime related to the use of information and communication technologies without borders and with strong technological engineering characteristics that rely on a high level of security of information transmitted and accessed by internet users [21]. Cybercrime can also be said to be the use by cyber criminals of computers for criminal purposes. Misuse of high technology and cybercrime can be described as All non-criminal services/illegal acts based on computer technology The complexity of the development of internet technology [22]. Meanwhile, cybercriminals commit unlawful acts with criminal intent or crimes within the scope of cybercrime [23].

3. METHODOLOGY

This research uses the digital forensics method created by the Digital Forensics Research Workshop (DFRWS). The DFRWS method facilitates access to evidence and a centralized mechanism for documenting the information collected [24].

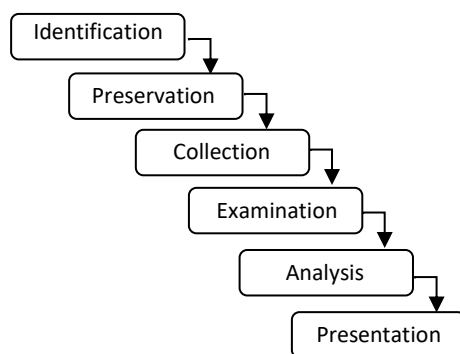


Figure 1. Digital Forensic Research Workshop Method

Figure 1 shows the stages of the Digital Forensic Research Workshop method. The identification stage determines the need for investigation and evidence retrieval. The preservation stage preserves digital evidence to ensure its authenticity and refute claims that it has been tampered with or sabotaged. The collection stage identifies data sources. The examination stage performs a predetermined data filtering step on certain parts of

the data source. The analysis stage examines where the data was generated, by whom it was generated, how it was generated, and why it was generated. The presentation stage makes a presentation by displaying the information generated from the analysis stage [25].

4. RESULT AND DISCUSSION

This research applies the DFRWS method to the Tiktok web application on the Mozilla Firefox browser. The case example used in this research is the spread of videos containing defamation through content uploaded on the social media TikTok web. This research can provide information in text, photos and videos that can be used as digital evidence. The simulation can be seen in Figure 2.

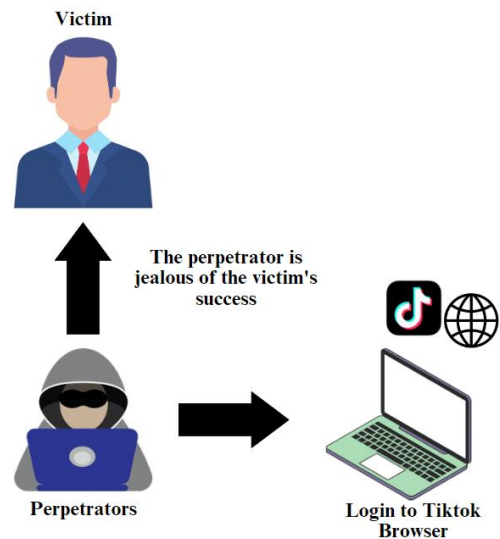


Figure 2. Pre-Incident of Defamation Case

Figure 2 The perpetrator is jealous of the victim's video, which looks successful. He stitches the video by saying that the perpetrator is successful because he practices a shaman tradition.

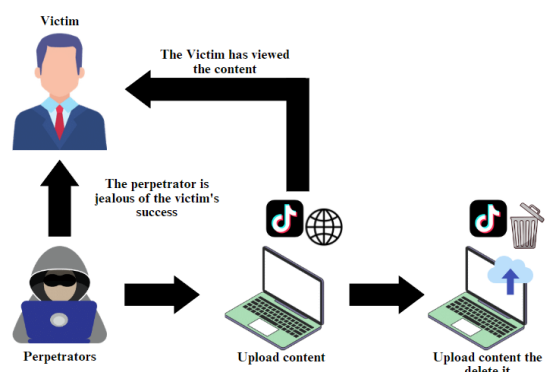


Figure 3. Incidents of Defamation Cases

Figure 3 the victim saw the obscene content that the perpetrator had made, which made the victim angry because the perpetrator's actions were very annoying. The video was a harmful act and a hoax because the victim never carried out the tradition that the perpetrator referred to. Then the victim reported the video to the police because the video content made by the perpetrator was a hoax. When the trial was imminent,

the post was deleted, and the suspect ran away, so the evidence was from laptops and smartphones. Which used remains exists.

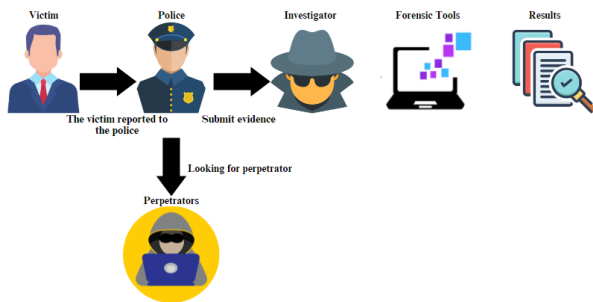


Figure 4. Post-Defamation Incident

Figure 4 the image of the laptop used by the suspect becomes digital evidence using a forensic application, which is then investigated by the investigator using digital forensic software. The initial data created in this case simulation is a Tiktok account and a post. The forensic process is carried out using the DFRWS method. It uses forensic tools such as FTK Imager, Belkasoft Evidence Center, browser capture history, browser capture viewer and video cache view.

4.1 Identification

Identification is the first stage that investigators will use. At this stage the investigator will determine the target of the evidence to be sought. Determination of this target is based on the chronology that can be seen in the research simulation section which has explained how the suspect posted video content to his Tiktok account and was deleted by the suspect when someone felt harmed or harassed. The process of collecting information or digital evidence is carried out with several forensic stages. Figure 5 is evidence of the scenario provided by the victim.

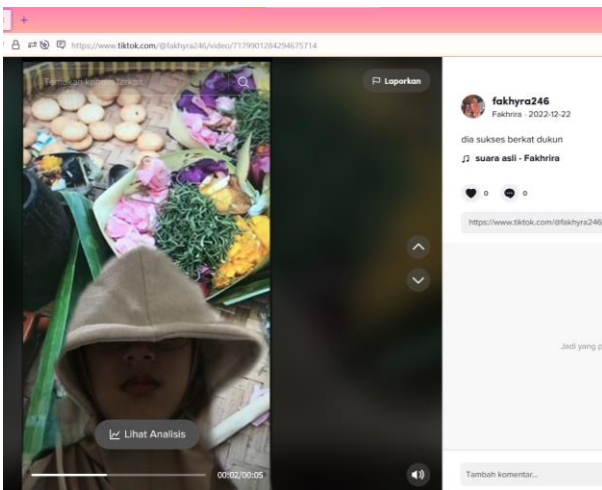


Figure 5. Evidence from the Victim

4.2 Preservation

This stage involves securing the evidence, validating the evidence, and denying that the evidence was sabotaged. Ensuring with physical evidence isolation techniques is carried out to maintain the integrity and destruction of evidence (obstruction of justice). Physical evidence can be seen in Figure 6.



Figure 6. Isolation of Evidence

4.3 Collection

The Collection is the process of collecting evidence suspected of containing electronic evidence that can be used as evidence in the legal process. This process is used to determine the needs and look for what will be needed or used for the next stage according to the evidence in the used for the next stage according to the evidence obtained. This stage is the stage carried out by the investigator to search for, collect and process documentation of evidence contained at the scene of the crime. The evidence used in this scenario is a laptop used by the suspect. In table 4.1 below is the evidence used is the specification of the evidence as follows:

Table 1. Tools and Materials

No	Tools and Materials	Description
1	Laptop	Prosesor AMD Ryzen 7 4800U with Radeon Graphics 1.80 GHz, RAM : 8 GB SSD : 477 GB, Windows 10 64-bit operating system, x64-based processor
2	Tiktok	Applications that are the object of research
3	FTK Imager	Applications used to lift digital evidence on laptops
4	Browser History Viewer	Applications used to lift digital evidence on laptops
5	Browser History Examiner	Applications used to lift digital evidence on laptops
6	Video Cache View	Applications used to lift digital evidence on laptops

To capture memory, FTK Imager and Browser History Examiner tools are used. To read the RAM capture data used FTK Imager tools, FTK Imager will read the previous RAM capture data which has the format ".mem". the contents of the capture data can be seen in Figure 7.

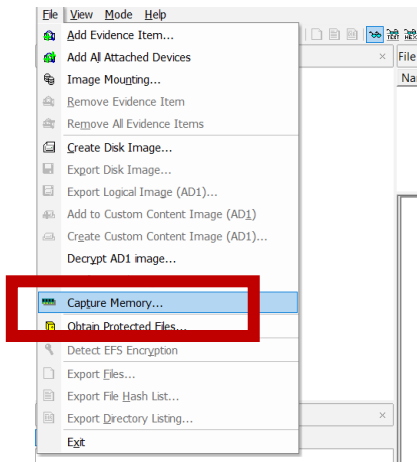


Figure 7. Capture Memory FTK Imager Feature

In the FTK Imager application, data can be collected by capturing a memory. The way to charge is to select the file menu and click on the capture memory feature section. The results will be saved with the file name Evidence. mem



Figure 8. FTK Imager Capture File

Figure 8 During RAM acquisition, there is information about the results that will be obtained based on the RAM of the suspect laptop, which is 8.23 Gigabytes (GB). The stages of the search history capture process use the Browser History Examiner tool. This tool will retrieve data from the Mozilla Firefox web browser.

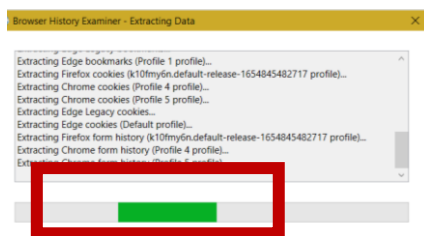


Figure 9. Web Browser History Examiner view when capturing

Browser History Examiner is used to capture web browser browsing history while reading and viewing the captured data. Browser History Examiner can capture, analyze, and report web browser browsing history. The capture results can be seen in Figure 10.

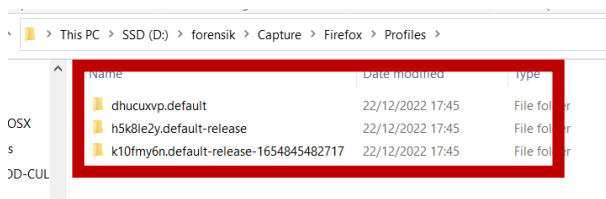


Figure 10. Cache Web Page

4.4 Examination

The examination is a stage carried out after the collection process; at this stage, the process of examining the data that has been obtained previously is carried out. The examination is carried out on the RAM (Random Access Memory) capture data and the capture of the browsing history on the web browser used.

To read the RAM capture data, the FTK Imager tool is used; FTK Imager will read the previous RAM capture data, which has the ".mem" format. The contents of the captured data can be seen in the figure capture process can be seen in Figure 9.

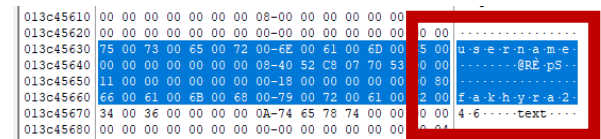


Figure 11. Performer Username

Figure 11 shows the results of searching for the perpetrator's username. It can be seen that the username used by the perpetrator to log into his account is "fakhyra246," and then he search for a password.

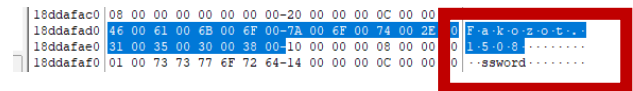


Figure 12. Performer Password

Figure 12 shows the results of searching for the perpetrator's password. It can be seen that the password used by the perpetrator to log into his account is "Fakozot.1508".

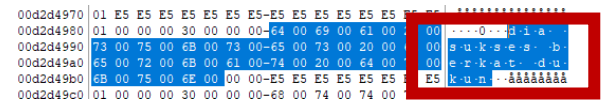


Figure 13 . Posting Performer Caption

Figure 13 shows the results of searching for the perpetrator's caption with the text "he was successful thanks to the shaman," a sentence listed in the caption on the video or content uploaded by the suspect.

To open the results of capturing browsing history on a web browser, the Browser History Examiner tool is used; the Browser History Examiner will display a graph of browsing activities carried out by users, and there are filters to find relevant data faster based on keywords and time/date ranges, and can analyze and extract and analyze various types of data such as websites that have been visited, cookies, cache files, and item downloads.

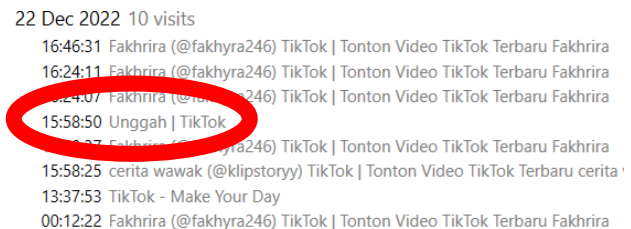


Figure 14 . Tiktok Upload

In Figure 14, it is evident in the browser history examiner tool that the perpetrator uploaded a video at 15:58:50 on December 22, 2022.

Next, we will use the video cache view; Video Cache Viewer is a tool that Du uses to acquire videos from browser applications such as Firefox, Opera, and Chrome.

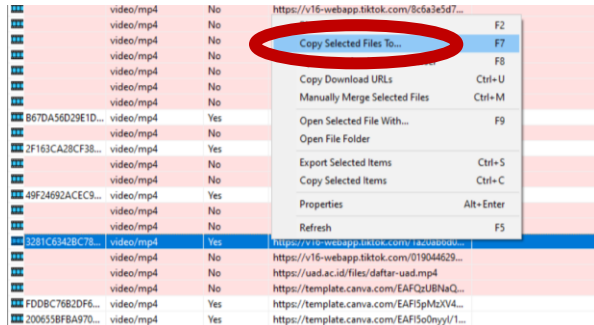


Figure 15 . Video Cache to be extracted.

After that, select all files, then select the chosen copy menu, or you can directly press f7 to save the results of the acquisition data. The results of the saved video can be seen in Figure 15, and the extract results can be seen in Figure 16.

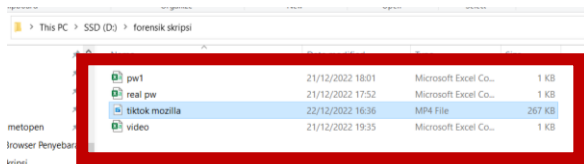


Figure 16 . Results After Extraction

4.5 Analysis

The analysis stage is carried out to see the examination results or examination results in detail. At this stage, the effects of the previous examination process are examined to obtain digital evidence. At the analysis stage, researchers can analyze evidence manually or with the help of the software used. The results of analyzing digital evidence using the four forensic tools are described as follows.

4.4.1 FTK Imager Analysis

Based on the examination results that have been carried out using the FTK Imager tool, evidence was found in the form of usernames, passwords, and captions on the uploaded videos used by the perpetrator to log in to his Instagram account. The username and password can be seen in Table 2.

Table 2 . FTK Imager Tools Results

Information	Results	Note
Username	Fakhrya246	Found
Password	Fakozot.a508	Found
Caption	“Dia sukses berkat dukun”	Found

4.4.2 Analisis Browser History Examiner

Based on the results of the checks that have been carried out, the Browser History Examiner tool can find evidence in the form of website visit histories, such as date and time.

TikTok access is on 22/12/2022. The perpetrator uploaded a video, and the web browser used by the perpetrator is mozilla firefox

22 Dec 2022 10 visits

- 16:46:31 Fakhrya (@fakhrya246) TikTok | Tonton Video TikTok Terbaru Fakhrya
- 16:24:11 Fakhrya (@fakhrya246) TikTok | Tonton Video TikTok Terbaru Fakhrya
- 16:24:07 Fakhrya (@fakhrya246) TikTok | Tonton Video TikTok Terbaru Fakhrya
- 15:58:50 Unggah | TikTok
- 15:58:37 Fakhrya (@fakhrya246) TikTok | Tonton Video TikTok Terbaru Fakhrya



Gambar 17. Video Upload Performers

In Figure 17, it is evident in the browser history examiner tool that the perpetrator uploaded a video at 15:58:50 on December 22, 2022.

4.4.3 Browser History Viewer Analysis

The results of the website viewer with TikTok parameters to find the evidence needed results obtained are seen on the date of the incident. Namely 22/12/22. There are results, namely two photos: the perpetrator's profile photos and thumbnails of the video content uploaded. These photos are sourced from TikTok, which can be seen from the URL of each image. The results of profile photos and video thumbnails can be seen in Table 3.

Table 3 . Browser History Viewer Results

Information	Results
Profile Photo	
Video Thumbnail	

4.4.4 Video Cache View Analysis

Video Cache Viewer is a tool for collecting and saving videos from the videos played in the browser. The video is a video that can be saved according to their respective sources. When this video can be obtained, save it to storage and open it manually with a video player application. After a manual search, it was found that the video was searched. Because videos from social media can be stored in the Browser cache itself, as shown in the picture.

No	https://v16-webapp.tiktok.com/2fba53405c...	Chrome	Web Browser	19/12/2022 09:05:54	17/12/2022 07:52:02	0
No	https://v16-webapp.tiktok.com/25a840109...	Chrome	Web Browser	21/12/2022 09:01:45	20/12/2022 19:36:05	0
Yes	https://v16-webapp.tiktok.com/219ae561c...	Mozilla/Firefox	Web Browser	22/12/2022 16:24:38	22/12/2022 16:24:38	11
No	https://v16-webapp.tiktok.com/1ffc0a4f3...	Chrome	Web Browser	21/12/2022 18:55:34	21/12/2022 18:50:56	0
Yes	https://v16-webapp.tiktok.com/1a20ab680...	Mozilla/Firefox	Web Browser	22/12/2022 16:24:28	22/12/2022 16:24:28	27
No	https://uad.ac.id/files/daftar-uad.mp4	Chrome	Web Browser	19/12/2022 15:27:36	15/04/2020 11:37:55	0
No	https://template.canva.com/EAFQzUBNaQ...	Chrome	Web Browser	22/12/2022 08:26:04	05/11/2022 09:37:02	0

Figure 18. Video Cache View

In Figure 18, it can be seen that the video from TikTok is stored in the Mozilla Firefox browser cache, so the footage that has been saved from this tool into the device storage can save the video sourced from TikTok and can be extracted back into a complete video.

4.6 Presentation

Reporting The final stage is to present the results of the analysis and draw conclusions from the results of the investigation from the initial stage to the final stage. The data that has been obtained from this research is a complete report along with acquisition data from forensic tools FTK Imager obtained results in the form of usernames and passwords used by the perpetrator to log into his tiktok account. Browser History Examiner tools obtain evidence in the form of date and time tiktok video upload. Tools Browser History Viewer obtains evidence of tiktok video thumbnails and profile photos of the perpetrator. Video Cache View tools obtain evidence that deleted videos can be extracted back into a complete video. The information from the device from this research is a Windows 10-based laptop with details in Table 4.

Table 4 . Hardware Evidence

Brand	Lenovo ideapad5 LAPTOP-E8UDG2AV
Processor	AMD Ryzen 7 4800U with Radeon Graphics
Graphics	Radeon Graphics 8 Cores
Memory	8GB Memory DDR4
Harddisk	477 GB SSD
Monitor	15.6" FHD (1920×1080) IPS 300 nits Anti-glare, 45% NTSC.

The application or software that is forensically analyzed is Mozilla Firefox with a web, namely Tiktok web. By following several examination procedures, the evidence is diagnosed with several tools with their own functions and features from the social media TikTok web analysis. Then the results focus on several things related to the suspect and social media TikTok web; more details can be seen in Table 5.

Table 5. Tiktok Web Browser Mozilla Firefox results

No	Digital Evidence	Software Forensics			
		FTK Imager	Browser History Examiner	Browser History Viewer	Video Cache View
1	Foto	0	0	2	0
2	Video	0	0	1 (Thumbnail)	1
3	Caption	1	0	0	0
4	Username	1	1	1	0
5	Link	0	1	1	1

Table 5 is the result of the discovery of evidence on the TikTok website that runs on the Mozilla web browser Firefox. The FTK Imager tool got proof of username, password and text from the post caption uploaded by the suspect; the suspect's user name is @fakhyra246. The photos and videos (Thumbnails) are obtained from the Browser History Examiner and Viewer tools; the results are in the form of prose photos of the suspect's account. Results were obtained in the form of a profile photo of

the suspect's history, a video (Thumbnail) of the video content uploaded by the suspect and the suspect's username. There are links and usernames from the suspect when logging in and uploading the crime content. The results obtained from the video cache viewer are only link links from videos on TikTok social media, for video successfully received because the footage from Tiktok web can be stored in the browser cache. In the browser cache.

5. CONCLUSION

Based on the results of research that has been carried out with the title "Forensik Browser On Web-Based Tiktok Application Using Digital Forensic Research Workshop Methods" which areruns in the Mozilla Firefox browser application on Windows 10 then obtaining forensic evidence is collected by capturing ram and cache stages using several tools that support the data collection process such as the tools used in this study, namely FTK Imager, Browser History Examiner, Browser History Capture and Video Cache View. FTK Imager obtained the results in the form of a username and password used by the perpetrator to log into his tiktok account. The Browser History Examiner tool obtains evidence in the form of the date and time of uploading the tiktok video. Tools Browser History Viewer obtains evidence of tiktok video thumbnails and profile photos of the perpetrator. Video Cache View tools obtain evidence that deleted videos can be extracted back into intact videos. Based on the tools used in this study, it was successful in obtaining 100% of the goods.

6. REFERENCES

- [1] G. Fanani, I. Riadi, and A. Yudhana, "Journal Media Informatika Budidarma Analysis Michat Application Forensics Using Digital Forensics Research Workshop Methods," vol. 6, no. 2, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.
- [2] H. P. S Nawawi, C. Carudin, and D. Yusup, "Analysis of Digital Evidence Discovery Through Voice Recording Using Praat with Audio Forensic Methods," *JUSTINDO (Journal of Systems and Technol.*, vol. 7, no. 1, pp. 10–19, 2022, doi: 10.32528/justindo.v7i1.5368.
- [3] I. A. N. S. Dayuoman, "Self-Actualization and Social Media (Dramaturgy of Millennials in Tiktok Social Media)," *Widya Duta J. Ilm. Religious Sciences and Social Sciences. Culture*, vol. 17, no. 2, pp. 89–98, 2022, doi: 10.25078/wd.v17i2.1655.
- [4] Muhammad Abdul Aziz, Wicaksono Yuli Sulistyono, and Sri Rahayu Astari3, "Comparative Anti Forensics of Web-Based Instant Messaging Applications Using the Association of Chief Police Officers (ACPO) Method," *JURISTIK (Journal of Ris. Technol. Inf. and Computer)*, *JURISTIK (Jurnal Ris. Teknol. Inf. dan Komputer)*, vol. 1, no. 01, pp. 8–15, 2021, doi: 10.53863/juristik.v1i01.341.
- [5] S. M. Dusu and I. Riadi, "Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method," *Int. J. Comput. Appl.*, vol. 183, no. 33, pp. 9–15, 2021, doi: 10.5120/ijca2021921716.
- [6] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," *Int. J. Comput. Appl.*, vol. 175, no. 34, pp. 47–52, Dec. 2020, doi: 10.5120/ijca2020920897.
- [7] F. Anggraini and A. Yudhana, "Forensic Analysis of TikTok Application on Android Smartphone Using Association of Chief Police Officers Framework," vol. 9,

- no. 4, pp. 1117–1127, 2022, doi: 10.30865/jurikom.v9i4.4738.
- [8] M. I. Syahib, I. Riadi, and R. Umar, "Viber Application Digital Evidence Acquisition Using the National Institute of Standards Technology (NIST) Method," *J-SAKTI (Journal of Comput. and Inform. Science)*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196.
- [9] Sunardi, I. Riadi, and M. H. Akbar, "Application of Static Forensics Method for Steganography File Extraction on Digital Evidence Using DFRWS Framework," *J. RESTI (Engineering Systems and Technol. Information)*, vol. 4, no. 3, pp. 576–583, 2020.
- [10] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Digital Forensic Analysis of Instant Messaging Applications in Android-Based Smartphones for Digital Evidence," *J. Technol. Inf.*, vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.
- [11] S. RACHMIE, "The Role of Digital Forensic Science in the Investigation of Website Hacking Cases," *Litigation*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.
- [12] G. B. Satrya and A. A. Nasrullah, "Android Forensic Analysis: Artifacts in Box Cloud Storage Application," *J. Technol. Inf. and Comput. Science.*, vol. 7, no. 3, p. 521, 2020, doi: 10.25126/jtiik.2020732220.
- [13] I. R. Muddin and S. Muryanto, "Utilization of Website Media as a Sales Promotion of Fishing Rods during the Covid-19 Pandemic in Kiringan RT 01 / RW 06 Boyolali," *Senyum Boyolali*, vol. 2, no. 1, pp. 26–32, 2021, doi: 10.36596/sb.v2i1.530.
- [14] S. Putu, F. Wira, I. G. Ngurah, A. Cahyadi, and M. Akbar, "Digital Forensic Analysis of Twitter Applications on Android as Digital Evidence in Handling Online Prostitution Cases," vol. 10, no. 3, pp. 271–278, 2022.
- [15] D. P. R. Adawiyah, "The Effect of Tiktok Application Use on Teenagers' Self-Confidence at Sampang Regency," *J. Komun.*, vol. 14, no. 2, pp. 135–148, 2020, doi: 10.21107/ilkom.v14i2.7504.
- [16] M. B. Pakarti, "Digital Evidence Management to Improve the Accessibility of Digital Forensics Laboratory," 2020, [Online]. Available: https://dspace.uui.ac.id/handle/123456789/28258%0Ahttps://dspace.uui.ac.id/bitstream/handle/123456789/28258/15917217_Moch_Bagoes_Pakarti.pdf?sequence=1&isAllowed=y
- [17] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity and Digit Forensics.*, vol. 3, no. 2, pp. 12–21, 2020.
- [18] V.A.R.Barao, R.C.Coata, J.A.Shibli, M.Bertolini, and J.G.S.Souza, "Covariance Structure Analysis of Health-Related Indices for the Elderly at Home, Focusing on Subjective Feelings of Health," *Braz Dent J.*, vol. 33, no. 1, pp. 1–12, 2022.
- [19] P. R. Kertayasa, "Analysis of Video Likes to Video Views Ratio Tiktok on 5 Tiktok Artists with the Most Followers in 2021," 2021.
- [20] T. Zahirah, "P Development of TIKTOK-Based Biology Learning Media on Excretory System Material for Class XI at MAN 1 Langsa," *Unpublished*, 2021.
- [21] F. A. Saharani, "Data Analysis of Increased Use of TikTok Social Media," 2022.
- [22] M. R. Habibi and I. Liviani, "Information Technology Crime (Cyber Crime) and Its Countermeasures in the Indonesia Legal System," *Al-Qanun J. Pemikir. dan Pembaharuan Huk. Islam*, vol. 23, no. 2, pp. 400–426, 2020, [Online]. Available: <http://jurnalfsh.uinsby.ac.id/index.php/qanun/article/view/1132>
- [23] M. Rifauddin and A. N. Halida, "Cybercrime Alert and Hoax Information on Facebook Social Media," *Khizanah al-Hikmah J. Library, Information, and Archival Science*, vol. 6, no. 2, p. 98, 2018, doi: 10.24252/kah.v6i2a2.
- [24] M. N. Fadillah *et al.*, "Forensic Analysis of Digital Wallet Applications on Android Smartphones Using the Dfrws Method," vol. 09, no. 02, pp. 265–278, 2022.
- [25] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Uncovering and Testing the Authenticity of Digital Evidence in Cybercrime Crimes with the Digital Forensic Research Workshop Method," *J. Appl. Technol. Inf. and Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.