# Forensic Website Analysis of Movie Piracy on TikTok using the ACPO Framework

Bunga Syahira Najla
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

## ABSTRACT

The development of information technology has increased the use of social media, including TikTok, which is now prone to being used for digital crimes such as movie piracy. The research aims to uncover digital evidence of movie piracy on TikTok Web using digital forensic methods with the Association of Chief Police Officers (ACPO) approach, which consists of four stages: planning, data acquisition, analysis, and presentation of results. The tools used in the investigation are FTK Imager, Browser History Examiner, and VideoCacheView. Results showed that FTK Imager and Browser History Examiner each successfully extracted 5 out of 12 digital evidences (41.7%), while VideoCacheView obtained only 2 evidences (16.7%). These findings emphasize the importance of selecting and combining forensic tools that are appropriate for the type of digital data. This approach proved to be effective in supporting the process of identifying and proving content piracy on the TikTok Web platform.

## Keywords

Digital Evidence, Movie Piracy, TikTok, Association of Chief Police Officers (ACPO).

## 1. INTRODUCTION

The development of information technology has encouraged the emergence of digital media as a means of communication, one of which is social media. Social media allows users to interact, share information, and express themselves [1]. It continues to evolve with various features that attract public interest [2]. One of the most popular platforms today is TikTok, which enables users to upload videos ranging from 15 seconds to 3 minutes, and includes an inbox feature for sending direct messages [3][4]. TikTok is freely accessible and widely used. According to the We Are Social report from October 2023, TikTok had reached 1.22 billion global users, with Indonesia ranking second with 106.51 million users [5].

Along with this user growth, digital crimes (cybercrime) have also become more prevalent, including the spread of hoaxes, hate speech, and movie piracy [6]. Piracy in this context involves uploading movie clips without permission, which directly harms the rights of copyright holders [7]. TikTok is often used to share parts of movies, including newly released content from official platforms [8]. This phenomenon demonstrates the importance of addressing digital crime through digital forensic investigation. Several forensic frameworks have been developed to support such efforts, including those from the National Institute of Justice (NIJ), National Institute of Standards and Technology (NIST), Digital Forensics Research Workshop (DFRWS), and the Association of Chief Police Officers (ACPO) [9][10][11][12][13]. The ACPO framework is adopted in this research to investigate movie piracy cases conducted through the TikTok platform.

## 2. LITERATURE STUDY

### 2.1 Digital Forensics

Digital forensics is a branch of forensic science used to investigate and find evidence on digital devices. The application of digital forensics in the investigation process requires technological expertise as well as legal knowledge relevant to criminal proceedings [14]. Digital forensics involves investigating digital devices to collect, preserve, analyze, and present digital evidence [15].

### 2.2 Digital Evidence

Digital evidence is information obtained from digital devices such as computers, cell phones, or other storage media [16]. This evidence plays an important role in criminal investigations as it can be used to identify, analyze, and track criminal activity, both digital and non-digital in nature [17]. Examples include activity logs, saved files, email trails, or suspect location data. As technology develops, the role of digital evidence in law enforcement is increasingly crucial, demanding digital forensic expertise so that the evidence collected is valid and admissible in court.

### 2.3 TikTok

TikTok is a Chinese social media platform developed by ByteDance, and allows users to create and share 15-second to 3-minute videos with various visual effects, music, and filters. Based on the We Are Social report, as of October 2023 there were approximately 106.51 million TikTok users in Indonesia [5]. In the context of digital forensics, TikTok stores various types of data that can be the object of investigation, such as user data, media content (uploaded, downloaded, or watched videos), and activity logs, including access times and user interactions with content [18]. This information can be analyzed to support investigations into suspicious or unlawful digital activities.

### 2.4 Movie Piracy

Film is a creative work created by professionals as a form of expression of values, art, or culture, and a means to convey messages to the audience. However, the development of technology also raises new challenges such as piracy, which is the activity of duplicating or distributing works illegally via the internet [19]. Movie piracy is included in the category of cybercrime that attacks property rights or against property. This illegal act not only causes financial losses to creators but also undermines the value and appreciation of original content.

### 2.5 Web Browser

Web browsers are used to access information on the internet, and automatically store log files that record user activity, such as a history of pages visited, access times, and other input data [20]. In the context of cybercrime, browser logs can reveal the

sites accessed by suspects, the time and interaction with certain content. The forensic process usually involves retrieving data from multiple browsers at once to ensure that no important information is missed [21]. Thus, web browsers not only serve as information access tools, but also as crucial data sources in digital crime investigations [22][23][24][25].

## 3. RESEARCH METHOD

The case analyzed in this study is a movie piracy incident on the TikTok application. The investigation process followed the Association of Chief Police Officers (ACPO) framework consisting of four stages: planning, data acquisition, analysis, and presentation. The stages of this ACPO method can be seen in Figure 1.

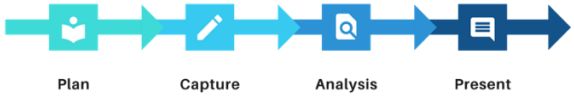


**Figure 1: Stages of the ACPO Method**

Figure 1 shows an overview of the four stages of the Association of Chief Police Officers (ACPO) framework. In the planning stage, the hardware and software were prepared, including an HP Pavilion Aero Laptop 13-be0xxx with Windows 10, FTK Imager 4.7.3.81, Browser History Examiner, and VideoCacheView. Secure storage was also created for evidence preservation, and hash values (MD5/SHA1) were generated to ensure data integrity. In the acquisition stage, FTK Imager was used to perform live memory imaging and capture volatile data. Browser History Examiner extracted browsing history, search queries, and cookies, while VideoCacheView retrieved cached videos and metadata. All evidence was preserved in separate folders with integrity checks before and after acquisition.

During the analysis stage, the memdump.mem file was examined with FTK Imager using keyword and string searches to identify usernames, captions, and deleted video links. Browser History Examiner reconstructed the activity timeline, while VideoCacheView confirmed the presence of cached video files. Finally, in the presentation stage, the findings were summarized in tables and charts to illustrate the number and type of evidence recovered by each tool. The structured workflow provided traceability and ensured the forensic process could be replicated.

## 4. RESULT AND DISCUSSION

The case under investigation is a movie piracy incident on the TikTok application. To obtain valid evidence, the Association of Chief Police Officers (ACPO) framework is used with the help of forensic tools such as FTK Imager, Browser History Examiner, and Video Cache History Viewer. The process was designed to ensure that all evidence was collected and analyzed with appropriate methods. Based on the explanation of the scenario, an illustration of the scenario is made which provides stages consisting of pre-incident, incident, and post-incident. These stages are essential to understand the chronology of the crime, guide the forensic investigation, and ensure that each phase is properly documented. In addition, this structured scenario helps identify key actions taken by perpetrators at each stage.

The first scenario is pre-incident in the figure 2. These stages are important to reconstruct the timeline of the crime, understand the actor's behavior, and identify the key digital traces that support the investigation.

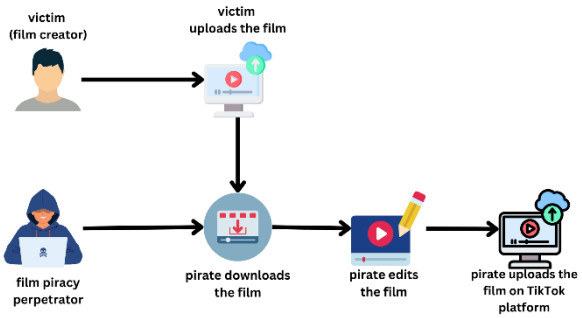


**Figure 2: Pre-incident of movie piracy case**

Figure 2 shows the victim as a movie creator who uploaded the film online. he perpetrator then downloaded the uploaded film, edited it, and re-uploaded the modified film to the TikTok platform. This stage shows the beginning of the piracy case by explaining the initial actions carried out by the perpetrator.

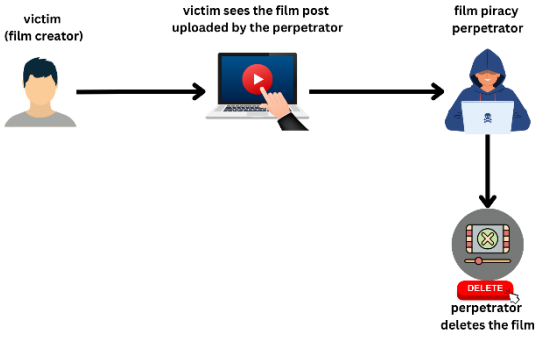


**Figure 3: incident of movie piracy case**

Figure 3 shows the incident stage of the piracy case. The process begins when the victim sees the movie that was uploaded by the perpetrator. The victim sees his work being altered and republished without permission. The victim realizes that the effort and creativity that has been put into making the film is not appreciated. The perpetrator of movie piracy realized that the victim had seen the uploaded and valtered movie video. Realizing this, the perpetrator then deleted the film from his TikTok account.

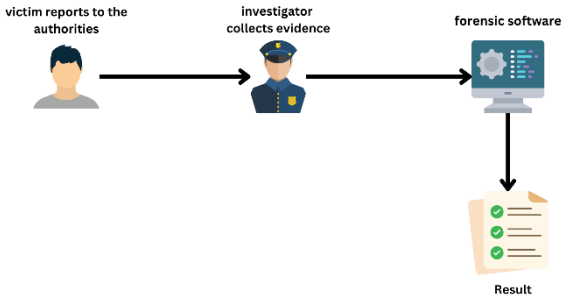


**Figure 4 : Post-incident of Movie Piracy Case**

Figure 4 shows the reporting stage or the final step in the process of collecting digital evidence. To ensure that the evidence is valid, the ACPO framework was applied with the assistance of FTK Imager, Browser History Examiner, and

VideoCacheView. This stage shows the importance of proper documentation and validation of evidence after the piracy incident.

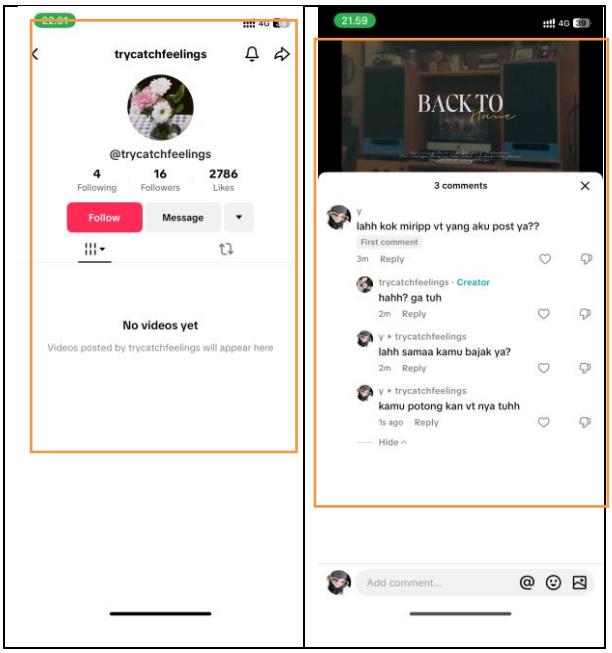


**Figure 5: Evidence in the Victim's Possession**

Figure 5 shows evidence from the victim's TikTok account, @trycatchfeelings, displaying the profile and comments questioning the similarity of the uploaded video. This shows ownership of the content, indicates possible copyright infringement, and provides an initial link to the suspected piracy activity.

## 4.1 Plan

At this stage, the required hardware and software were prepared to support the forensic process. This preparation ensures that all tools are ready to be used systematically and that the evidence collected remains valid. In addition, secure storage and hashing mechanisms were also considered to maintain the authenticity of digital evidence. The hardware and software to be used are presented in Table 1.

**Table 1: List of Hardware and Software**

| Hardware and Software | Description |
|---|---|
| HP Pavilion Aero Laptop 13-be0xxx | Hardware used in the investigation |
| TikTok | Social media of the investigation object |
| FTK Imager 4.7.3.81 | Imaging data and memory capture |
| Browser History Exsaminer | Analyze browser browsing history |
| Video Cache Viewer | Extraction of video evidence from browser cache |

Table 1 shows the hardware and software used in the investigation, including FTK Imager, Browser History Examiner, and VideoCacheView. FTK Imager shows the imaging process and data acquisition, Browser History Examiner shows the analysis of browsing history, and VideoCacheView shows the extraction of videos stored in the browser cache. This shows that different forensic tools were combined to strengthen the investigation process.


**Figure 6: Evidence of the Perpetrator's Laptop**

Figure 6 shows the main evidence in the form of the perpetrator's laptop, which was found in a powered-on condition. This shows the possibility of performing live data acquisition without shutting down the device, allowing volatile data such as login sessions and recent activity to be captured. The imaging process was conducted using FTK Imager, and the results show the basis for further analysis to reveal the perpetrator's activities.

## 4.2 Capture

In the capture stage, data is acquired from the secured device using prepared forensic tools, including memory imaging and cached data from the browser used to access TikTok. This stage ensures that volatile and non-volatile information can be collected properly, providing a reliable basis for the subsequent forensic analysis.

### *4.2.1 FTK Imager*

In the process of collecting data from RAM memory or capturing volatile memory, the forensic tool FTK Imager was used. FTK Imager shows the capability to create a memory image that is saved in a secure directory to preserve evidence integrity. This step is essential to ensure that volatile data such as active sessions and temporary information can be analyzed further during the forensic investigation.

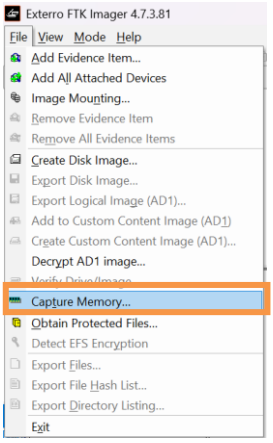


**Figure 7: Capture Memory**

Figure 7 shows the capture memory process on FTK Imager. This shows the display when the memory capture was initiated as part of the forensic acquisition.

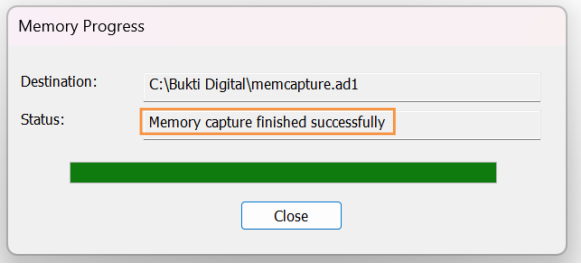


Figure 8 shows the display result after the memory capture process was successfully performed using FTK Imager. The memory acquisition file was saved in the Digital Evidence folder. This shows that the evidence was preserved correctly.

**Figure 8: Successful Memory Capture**

### *4.2.2 Browser History Examiner*

After the memory capture process is successfully carried out using FTK Imager, the next step in the process of digital forensic investigation is to capture the browsing history in the browser using the Browser History Examiner tool. Figure 8 is the capture history feature found in the browser history examiner.

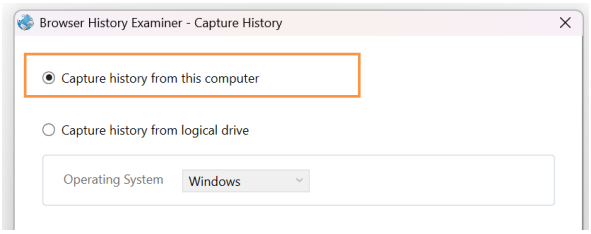


**Figure 9: Capture Memory Browser History Examiner**

Figure 9 shows the folder from Browser History Examiner containing browsing data. This shows that the perpetrator accessed TikTok, and the data was captured to support further analysis.

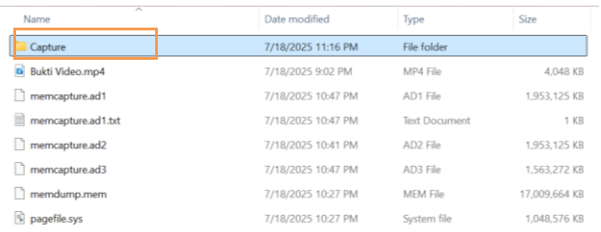


**Figure 10: Capture History Result Folder**

Figure 10 shows the result folder of captured history obtained through Browser History Examiner. This shows a detailed record of browsing activity stored as digital evidence.

### *4.2.3 VideoCacheViewer*

VideoCacheView is capable of displaying detailed information such as the file name, temporary storage location, file size, last access time, and the video's origin URL. After the acquisition process is completed, the tool automatically generates a list of cached video files that were detected in the browser, along with their associated metadata. This allows investigators to not only recover the video file itself but also verify the context of its access, such as when and from where the video was obtained.

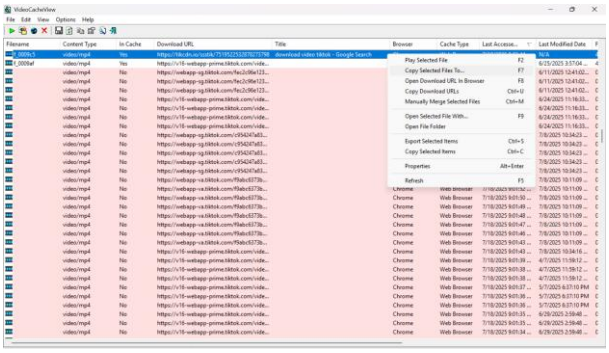

**Figure 11: Video Cache Acquisition**

Figure 11 shows the results of video cache file acquisition using the VideoCacheView tool. Browsing results on Google Chrome show an .mp4 video from ssstik.io, with details like file name, cache status, download URL, browser, title, and last modified time accessed on July 18, 2025 at 09:02:44.

The file Bukti Video.mp4 shows that the video evidence was successfully extracted.

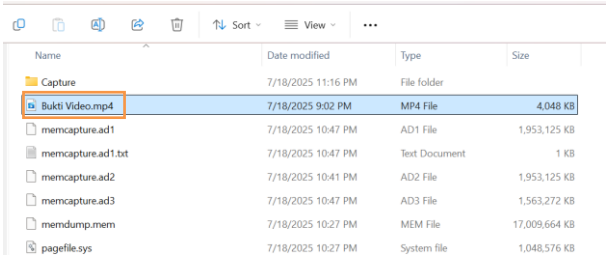


**Figure 12: Results After Extraction**

Figure 12 shows the display of the successfully saved video from the browser cache, which can be used as evidence of the perpetrator's activities.


**Figure 13: Extracted evidence can be opened**

Figure 13 shows that the extracted video can be opened and played like a normal video file. This shows that the video evidence remained intact and available for further forensic analysis.

## 4.3 Analysis

After the capture process is completed, the next step is analysis, which is a process of in-depth examination of the data that has been successfully acquired previously.

### 4.3.1 FTK Imager

At this stage, the memory capture file memdump.mem is analyzed using FTK Imager.

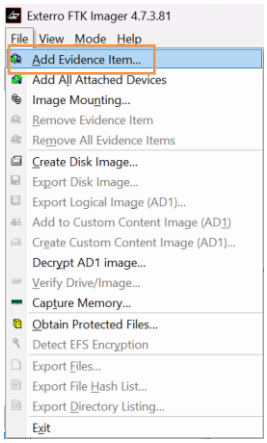


**Figure 14: Add Evidence Item**

Figure 14 shows the initial step in FTK Imager, where the Add Evidence Item option was selected to import the memory capture file for examination. This shows how the process maintains data integrity during analysis.

The next step is to select the memdump.mem file so that further analysis can be performed. In the tool menu, after selecting the Add Evidence Item menu, a pop-up will appear. In the image above, select the Image File section, then enter the evidence file that was obtained earlier with the file type .mem.

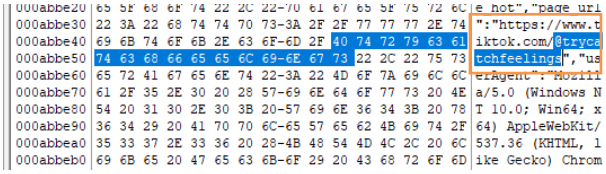


**Figure 15: Searching for the perpetrator's username**

Figure 15 shows a string search in memdump.mem using FTK Imager, which revealed the perpetrator's username: trycatchfeelings. This shows how FTK Imager can uncover user account traces.

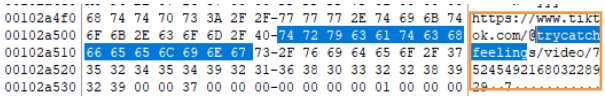


**Figure 16: Piracy Video Link**

Figure 16 shows the result of another string search, revealing a piracy video link that had been deleted by the perpetrator. This shows that the deleted post was no longer available on TikTok, confirming that the perpetrator attempted to remove evidence.

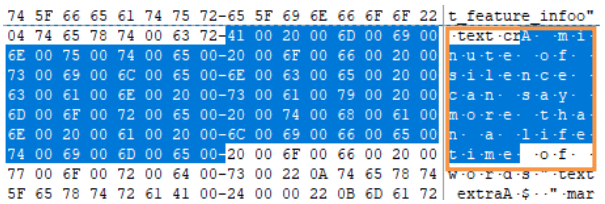


**Figure 17: Offender Caption Search**

Figure 17 shows the caption made by the perpetrator on the video post: “A minute of silence can say more than a lifetime of words.” This shows additional evidence associated with the uploaded pirated content.

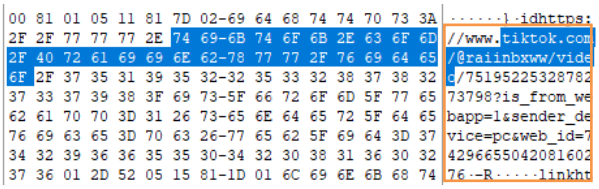


**Figure 18: Victim's Video Link**

Figure 18 shows the results of a text string search that revealed the link of the victim’s original video, copied by the perpetrator. This shows evidence that connects the pirated video with the victim’s content.

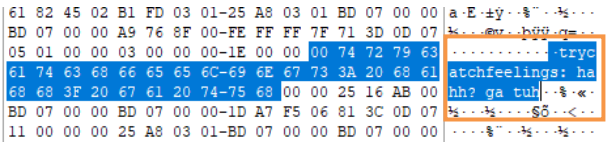


**Figure 19: Offender Comment Search**

Figure 19 shows the search result containing the perpetrator’s comment string “hahh? ga tuh” found in the metadata of the captured file. This shows evidence of the perpetrator’s interaction in the form of comments.

### 4.3.2 Browser History Examiner

Browser History Examiner is used to open and analyze captured browsing history from a web browser. It displays a graph of the user's browsing activity and can extract various types of data. The analysis is done using the Load History feature from the previous memory capture results. This allows investigators to trace digital footprints chronologically. Information such as access time, URL, browser type, and visit duration can serve as evidence of the perpetrator's actions. This data is important for reconstructing the timeline and validating the suspect's behavior. In addition, Browser History Examiner also provides detailed reports that can be exported and preserved as formal documentation for forensic investigation.

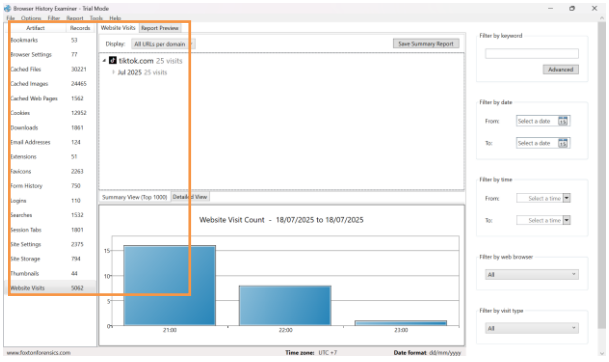


**Figure 20: Folder Capture Extract Result**

Figure 20 shows the results of the captured folder extract, including cache files, cache images, email addresses, favicons, form history, logins, searches, thumbnails, and website visits. This shows the range of evidence obtained through Browser

History Examiner and provides an overview of the browsing activities that can be linked to the piracy case.

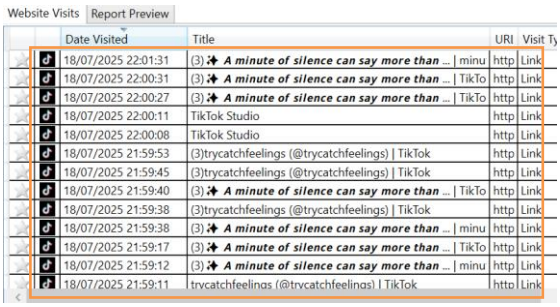


**Figure 21: Evidence of Victim Account Search**

Figure 21 shows the perpetrator's activity on TikTok Web using the Chrome browser on July 18, 2025, around 22:00. This shows the exact time when the perpetrator uploaded the pirated video and confirms the direct connection between the account activity and the piracy incident.

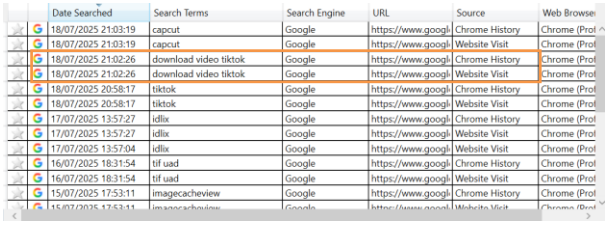


**Figure 22: Evidence of Perpetrator Search Activity**

Figure 22 shows the search results from the Chrome browser, indicating that the perpetrator searched for "download tiktok video." This shows further proof of the perpetrator's intent.


**Figure 23: Cookies Associated with Download Activity**

Figure 23 shows the results of log cookies that were successfully obtained from the offender's browsing activities using the Google Chrome browser. Based on this information, it appears that the perpetrator not only accessed the TikTok site, but also opened the CapCut platform. This data was obtained through a digital forensics process that extracted information from cookies on the perpetrator's system. This activity strengthens the suspicion that the perpetrator edited the hijacked video from the victim's account using CapCut before republishing it.

### *4.3.3 Video Cache Viewers*

Video cache viewer is a tool that collects videos stored in the browser. The video is a video that can be stored based on the source of each - each can be seen in Figure 24 a list of activity history stored in the perpetrator's browser cache.

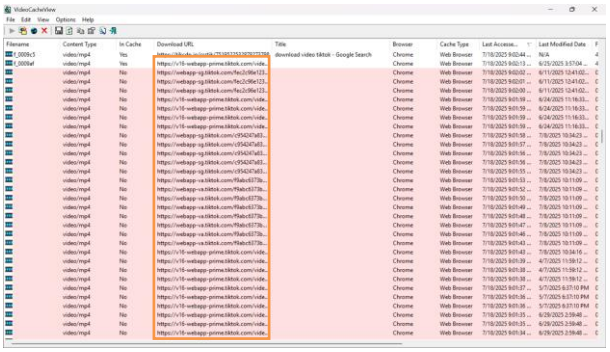

**Figure 24: Video Cache View Results**

Figure 24 shows a video from TikTok stored in the Chrome browser cache. This shows that even though the video was deleted from TikTok, it remained accessible through the cache and could be extracted using VideoCacheView, then replayed as a complete and valid file.

## 4.4 Present

The final stage of this investigation process is to present the results of the analysis and draw conclusions based on all the stages that have been carried out. This research was conducted with the aim of uncovering video piracy that occurred on the TikTok Web platform using a digital forensics approach. The investigation process was carried out through the stages of planning (plan), data acquisition (capture), analysis (analyze), and presentation of results (present). The device used in this research is a Windows 10-based laptop, with the specifications listed in Table 2.

**Table 2 : Laptop Specifications**

| Component | Specifications |
|---|---|
| Brand | HP Pavilion Aero Laptop 13-be0xxx |
| Processor | AMD Ryzen™ 5 5600U |
| Graphics | AMD Radeon™ Graphics |
| Memory | 8 GB DDR4 |
| Storage | 512 GB SSD |
| Component | Specifications |
| Brand | HP Pavilion Aero Laptop 13-be0xxx |

Table 2 shows the specifications of the laptop used by the perpetrator, including brand, processor, graphics, memory, and storage. This shows the technical specifications of the investigation target.

**Table 3: Table of Evidence Found**

| Digital Evidence | FTK | BHE | Video cache |
|---|---|---|---|
| Username (@trycatchfeelings) | 1 | 0 | 0 |
| Piracy video link | 1 | 0 | 0 |
| Caption of the perpetrator's video upload | 1 | 0 | 0 |
| Offender's comment ("hahh? ga tuh") | 1 | 0 | 0 |
| Victim's account link (@raiinbxww) | 1 | 1 | 0 |
| Access history and activity time | 0 | 1 | 0 |
| Search "tiktok video download" | 0 | 1 | 0 |
| Proof of site visit (ssstik.io) | 0 | 1 | 1 |

| | | | |
|---|---|---|---|
| Proof of TikTok and CapCut cookies | 0 | 1 | 0 |
| .mp4 video from browser cache | 0 | 0 | 1 |
| Total Digital Evidence | 5 | 5 | 2 |
| Percentage (%) | 41,7 | 41,7 | 16,7 |

Table 3 shows the digital evidence obtained from FTK Imager, Browser History Examiner, and VideoCacheView. FTK Imager and Browser History Examiner each extracted five pieces of evidence (41.7%), while VideoCacheView extracted two pieces of evidence (16.7%). This shows that memory acquisition and browsing history analysis were more effective than cache-based extraction. To provide a clearer evaluation, an additional comparison is presented in Table 4, which highlights the capabilities and limitations of each tool.

**Table 4 : Tool Comparison**

| Tool | Description |
|---|---|
| FTK Imager 4.7.3.81 | Extracted username, deleted links, captions, and comments. Strong in memory acquisition and string search, but requires manual analysis. |
| Browser History Exsaminer | Extracted browsing history, searches, and cookies. Good for activity timeline reconstruction, but limited to browser data only. |
| Video Cache Viewer | Extracted cached videos and metadata. Can recover playable files, but depends on cache availability. |

Table 4 shows a comparison of the three forensic tools. FTK Imager shows strong memory acquisition and string search capabilities, Browser History Examiner shows effectiveness in analyzing browsing history and cookies, while VideoCacheView shows capability in extracting cached video files. This shows how each tool complements the others in digital forensic investigations. The percentage of evidence extracted by each tool is illustrated in Figure 25.

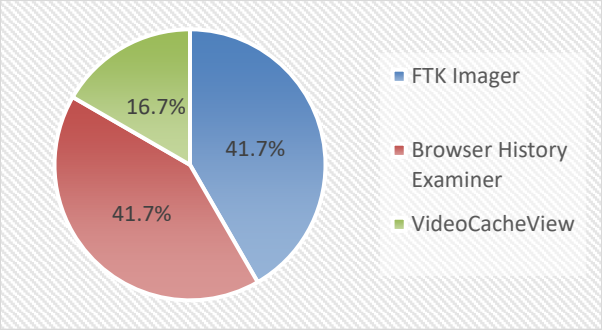


**Figure 25: Percentage of Evidence Extracted by Each Tool**

Figure 25 shows the percentage of evidence obtained by each forensic tool. FTK Imager and Browser History Examiner show higher percentages compared to VideoCacheView. This difference is related to the specific capabilities of each tool in extracting digital evidence. The consistency of the findings strengthens the validity of the evidence and supports the conclusion that the perpetrator was involved in piracy and redistribution of the victim's content on TikTok Web.

## 5. CONCLUSIONS

Based on the research results, it can be concluded that the ACPO framework is effective in conducting forensic investigations of movie piracy on TikTok Web. FTK Imager and Browser History Examiner each managed to extract 5 out of 12 pieces of digital evidence (41.7%), while VideoCacheView obtained 2 evidences (16.7%). These findings demonstrate that memory forensics and browsing history analysis are more effective in recovering diverse types of digital traces compared to cache-based methods. In the future, this approach can be improved by applying the same methodology to other platforms such as Instagram Reels or YouTube Shorts, and by incorporating additional forensic tools such as Autopsy, X-Ways Forensics, or Volatility for deeper analysis. Furthermore, integrating technical findings with legal perspectives will strengthen the admissibility of evidence in judicial processes.

## 6. REFERENCES

[1] A Rafiq, 'Dampak Media Sosial Terhadap Perubahan Sosial Suatu Masyarakat', Jurnal Ilmu Sosial dan Ilmu Politik, vol. 3, no. 1, 2020, doi: https://doi.org/10.33822/gk.v3i1.1704.

[2] Binus University, 'Media Sosial Sebagai Alat Komunikasi', BINUS Higher Education. Accessed: May 05, 2024. [Online]. Available: https://communication.binus.ac.id/2022/12/16/media-sosial-sebagai-alat-komunikasi/

[3] Y. Fitriani, 'Pemanfaatan Media Sosial Sebagai Media Penyajian Konten Edukasi atau Pembelajaran Digital', Journal of Information System, Applied, Management, Accounting and Research, vol. 5, no. 4, pp. 1006–1013, 2021, doi: 10.52362/jisamar.v5i4.609.

[4] Tri Buana and Dwi Maharani, 'Penggunaan Aplikasi TikTok (Versi Terbaru) dan Kreativitas Anak', Jurnal Inovasi, vol. 14, no. 1, Jul. 2020, doi: https://doi.org/10.33557/ji.v14i1.1390.

[5] C. M. Annur, 'Pengguna TikTok di Indonesia Terbanyak Kedua di Dunia per April 2023, Nyaris Salip AS?', databoks. Accessed: May 02, 2024. [Online]. Available: https://databoks.katadata.co.id/datapublish/2023/05/24/pengguna-tiktok-di-indonesia-terbanyak-kedua-di-dunia-per-april-2023-nyaris-salip-as

[6] Y. Fitriani and R. Pakpahan, 'Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace', doi: 10.31294/jc.v19i2.

[7] F. Sulaiman, 'Perlindungan Hukum Terhadap Pencipta Karya Sinematografi Terkait Pembajakan Film pada Situs Online', Jurnal Prosiding (1) Juli, Jul. 2021.

[8] G. Ayu, E. Yuliantari, I. Gede, A. Kurniawan, N. Putu, and D. P. Dewi, 'Perlindungan Hukum Pemegang Hak Cipta Terhadap Pembajakan Potongan Film Pada Aplikasi Tiktok', vol. 9, no. 1, pp. 81–90, 2023, doi: 10.59999/v9i1.1866.

[9] M. Rizki Setyawan and M. Fadli Hasa, 'Analisis Forensik Digital pada Skype Berbasis Windows 10 Menggunakan Framework ACPO', Hasa Jurnal Ilmiah Betrik, vol. 13, no. 02, 2022.

[10] R. Y. Prasongko, A. Yudhana, and I. Riadi, 'Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp', Jurnal Sains

Komputer & Informatika (J-SAKTI, vol. 6, no. 2, pp. 1112–1120, 2022.

[11] F. Anggraini, H. Herman, and A. Yudhana, 'Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers', JURIKOM (Jurnal Riset Komputer), vol. 9, no. 4, p. 1117, Aug. 2022, doi: 10.30865/jurikom.v9i4.4738.

[12] D. Agustian Akbar, F. Salsabila Yursa, M. Rahdian Ega Kurnia, and J. Sidabutar, 'Analisis Aktivitas Cyber Bullying Pengguna Instagram Melalui Browser Chrome dengan Pendekatan Live Forensics', PROSISKO, vol. 11, no. 1, Mar. 2024.

[13] Y. Safitri, I. Riadi, and S. Sunardi, 'Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework', MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, pp. 651–664, Jul. 2023, doi: 10.30812/matrik.v22i3.2987.

[14] S. Rachmie, 'Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website', LITIGASI, no. 21, pp. 104–127, Jul. 2020, doi: 10.23969/litigasi.v21i1.2388.

[15] A. A. Solanke and M. A. Biasiotti, 'Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques', KI - Kunstliche Intelligenz, vol. 36, no. 2, pp. 143–161, Sep. 2022, doi: 10.1007/s13218-022-00763-9.

[16] A. E. Saragih, N. Christian, and P. Khoirunisa, 'Analisis Penggunaan Barang Bukti Digital di Dalam Sistem Hukum di Indonesia (Studi Kasus Putusan Nomor 3 K/PID.SUS/2019)', vol. 2, no. 2, p. 504, 2024, doi: 10.5281/zenodo.12082755.

[17] F. Casino, C. Pina, P. López-Aguilar, E. Batista, A. Solanas, and C. Patsakis, 'SoK: cross-border criminal investigations and digital evidence', 2022, Oxford University Press. doi: 10.1093/cybsec/tyac014.

[18] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, 'Post-mortem digital forensic artifacts of TikTok Android App', in ACM International Conference Proceeding Series, Association for Computing Machinery, Aug. 2020. doi: 10.1145/3407023.3409203.

[19] E. Reviansyah and F. Hana, 'Perlindungan Hukum Pembajakan Film Digital (Studi Perbandingan Hukum Indonesia, Malaysia, dan Korea Selatan)', AJUDIKASI : Jurnal Ilmu Hukum, vol. 6, no. 2, pp. 211–232, 2022, doi: doi.org/10.30656/ajudikasi.v6i2.5469.

[20] H. Adamu, A. Adamu Ahmad, A. Hassan, and ad Barau Gambasha, 'Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis', International Journal of Research and Scientific Innovation, vol. 8, no. 5, May 2021.

[21] Hariani, 'Eksplorasi Web Browser dalam Pencarian Bukti Digital Menggunakan SQLITE', JURNAL INSTEK, vol. 6, no. 1, 2021.

[22] Exterro, 'FTK Forensic Toolkit'. Accessed: Jun. 16, 2024. [Online]. Available: https://www.exterro.com/digital-forensics-software/forensic-toolkit

[23] Foxton FORENSICS, 'Browser History Examiner'. Accessed: Jun. 16, 2024. [Online]. Available: https://www.foxtonforensics.com/browser-history-examiner/

[24] Foxton FORENSICS, 'Video Cache Viewer'. Accessed: Jun. 16, 2024. [Online]. Available: https://www.nirsoft.net/utils/video_cache_view.html

[25] I. Riadi, Sunardi, and Y. Safitri, 'Analisis Forensik Cyberbullying pada Aplikasi IMO Messenger Menggunakan Metode Association of Chief Police Officers', Jurnal Bumigora Information Technology (BITe), vol. 5, no. 1, pp. 1–8, Jun. 2023, doi: 10.30812/bite/v5i1.2977.