Forensic Multimedia Analysis in Film Piracy Cases using National Institute of Justice Method

Fadhilah Widya Putra Mahardika
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The development of digital technology has facilitated the distribution and access to film content, but it has also increased the risk of piracy and illegal modifications that harm the film industry and copyright holders. This research aims to obtain digital evidence and prove the existence of changes in video files in a film piracy scenario using a multimedia forensics approach. The research was conducted through a case simulation with a scenario where the perpetrator modified the film by adding a watermark and subtitles before distributing the modified file. The investigation process uses the National Institute of Justice (NIJ) method, which includes the stages of identification, collection, examination, analysis, and reporting. The tools used include FTK Imager, ExifTool, HashMyFiles, FFmpeg, as well as Python with the OpenCV and Matplotlib libraries. The research results show that the investigation process successfully obtained digital evidence in the form of video files and supporting artifacts for the modification process, totaling 17 files. Metadata analysis and hash value comparison show differences between the original video and the copied video. Additionally, frame analysis of the video using difference image and thresholding successfully identified local tampering in the form of added watermarks and subtitles. Based on these results, it can be concluded that the copied video file is a modification of the original video file, and a multimedia forensics approach can be used to supporting the investigation of film piracy cases.

Keywords
Digital Evidence; Digital Forensics; Multimedia Forensics; NIJ; Film Piracy.

1. INTRODUCTION
The development of information and communication technology has significantly changed the way film content is distributed and consumed. Thru the internet and various digital platforms, the public can now access films more quickly, easily, and efficiently. Film, as a cultural creation, not only serves as a means of mass communication but is also included in the objects of copyright protection, granting exclusive rights to creators to control and distribute their works legally [1]. However, the ease of digital distribution also presents challenges in the form of increased copyright violations, particularly digital film piracy [2].

Digital film piracy has evolved into one of the forms of cybercrime that has a significant impact on the film industry and copyright holders [3]. This practice allows the illegal distribution of film copies thru illegal streaming sites, file-sharing applications, social media, and other distribution media without the permission of the copyright holders [4]. The impact caused is not only the loss of potential income for film creators and distributors but also affects the country's revenue, copyright protection, and the sustainability of the creative industry [5][6]. In addition, users of illegal sites are also at risk of security threats such as malware and personal data theft [7]. Although the government has blocked more than 2,300 illegal streaming sites since 2019 [8], cases of piracy continue to rise. Data shows that Indonesia ranks fifth in the world in terms of visits to pirated movie sites in 2023, with a total of 1.04 billion visits [9]. This condition indicates the need for a more systematic approach in obtaining and managing digital evidence as the basis for proving cases of film piracy [10].

Various previous studies have applied a digital forensics approach in the process of investigating digital evidence. Research by Riadi et al. shows that FTK Imager is capable of recovering deleted data with a higher success rate compared to other tools in the digital investigation process [11]. The research by Idhofi and Muflih applied the National Institute of Justice (NIJ) method for the process of digital data acquisition and recovery [12]. Other studies demonstrate the application of the NIJ method in the recovery process of storage media data and forensic multimedia using various digital investigation tools [13][14][15]. In the field of multimedia authentication, Kustian's research uses hash value analysis, video metadata, and file signatures to determine the authenticity of digital files [16]. Meanwhile, Alwi and Anraeni applied video enhancement techniques using the NIJ method to improve the quality of video recordings as a visual identification tool [17].

Although previous research has discussed digital evidence acquisition, data recovery, metadata analysis, and video quality enhancement, studies specifically examining the proof of video file modification in film piracy cases thru a multimedia forensics approach are still limited. Therefore, this research uses the National Institute of Justice (NIJ) method, which consists of five stages: identification, collection, examination, analysis, and reporting [18]. The research was conducted thru a film piracy simulation scenario using a multimedia forensics approach with FTK Imager, ExifTool, HashMyFiles, FFmpeg, as well as Python-based OpenCV and Matplotlib to obtain digital evidence, compare video file characteristics, and identify localization tampering in the form of added watermarks and subtitles on the modified video files.

2. LITERATURE STUDY
2.1 Film Piracy
Film piracy is an illegal activity involving the distribution, duplication, uploading, downloading, or screening of films without the permission of the copyright holder [6]. This practice is widely carried out over the internet, allowing films to be accessed for free without going thru official services like cinemas or legal streaming platforms [19]. Forms of piracy include recording in cinemas, media duplication, and redistribution from torrent sites [6]. The impact is the loss of

royalties for creators and the weakening of copyright protection [5][1].

2.2 Multimedia Forensics

Multimedia forensics is a branch of digital forensics that focuses on the process of analyzing, authenticating, and reconstructing the history of multimedia content such as images, audio, and video to obtain accountable digital evidence [20]. Multimedia forensics not only aims to detect whether a media has been manipulated but also to trace the history of changes that have occurred to the media thru the analysis of internal characteristics without relying on external information.

2.3 National Institute of Justice

The National Institute of Justice (NIJ) is a digital forensics framework used for systematic investigations thru five stages: identification, collection, examination, analysis, and reporting [15]. This method aims to maintain the integrity of digital evidence so that the investigation results can be scientifically and legally accountable [21].

2.4 FTK Imager

FTK is a software package designed to find, secure, and analyze digital evidence [22]. FTK was originally created by AccessData and has long been a cornerstone in digital forensics work. Currently, under the management of Exterro, FTK has evolved from a regular desktop tool into an investigation platform ready for use by companies [23].

2.5 Exiftool

ExifTool is a standalone Perl library platform that also has a command-line application for reading, writing, and editing meta information in various types of files [24]. ExifTool supports various metadata formats such as EXIF, GPS, IPTC, XMP, JFIF, and others, as well as maker notes from many digital cameras of brands like Apple, Canon, DJI, Nikon, FujiFilm, GoPro, Kodak, Panasonic, and others [25].

2.6 HashMyFiles

HashMyFiles is a simple and free application by Nir Sofer used to calculate hash values such as MD5, SHA1, CRC32, SHA-256, and others from one or multiple files at once. This application is used to verify file integrity, ensuring that there are no changes or damage when the file is downloaded or transferred [26].

2.7 FFmpeg

FFmpeg is a very popular multimedia framework that can decode, encode, transcode, multiplex, demultiplex, stream, filter, and play various types of files created by both humans and machines. FFmpeg supports a wide range of both uncommon old formats and the latest formats [27].

2.8 Python

Python is a programming language used to create websites, software, automate tasks, and analyze data [28]. OpenCV is the main library specifically designed for processing images and videos in real time [29]. Meanwhile, Matplotlib is a Python library used to create data visualizations, graphs, and plots [30].

3. RESEARCH METHOD

The stages in this research refer to the framework from the National Institute of Justice, which has five stages: identification, collection, examination, analysis, and reporting. These stages are shown in Figure 1.

Figure 1: Stages of the NIJ method

Figure 1 shows the stages of the National Institute of Justice (NIJ) method. The identification stage includes the initial process of organizing the data and devices to be analyzed, as well as determining the forensic tools to be used, such as laptops, FTK Imager, Exiftool, Hash My Files, FFmpeg, and Python. The collection stage in this research is conducted to secure physical evidence and gather relevant digital evidence in the case of film piracy, such as original video files, copied video files, editing project files, subtitle files, and watermark files using FTK Imager. The examination stage includes the process of examining the images obtained previously. The examination is focused on evidence relevant to this film piracy case. The analysis stage is the process conducted after the examination stage, aimed at a thorough and in-depth investigation of the findings that have been discovered. This analysis includes metadata analysis, hash comparison, frame extraction, and tampering analysis. The final stage in this method is the reporting stage. Here, all examination results and analyzes of digital evidence are neatly documented in the form of a forensic report.

4. RESULTS AND DISCUSSION

This research analyzes a case of film piracy where the perpetrator obtains the original film file and modifies it, resulting in the creation of a simulation that depicts the entire investigation process divided into three main stages: Pre-Incident, Incident, and Post-Incident. Each stage is explained visually and narratively, with detailed depictions according to the flow and roles performed. This simulation was created to provide a contextual overview of the incident before the digital forensic investigation process is conducted on the found evidence. Thru this simulation, the sequence of the piracy event and the relationships between digital artifacts to be analyzed in the next stages can be understood in a more structured manner. The first simulation, namely the pre-incident phase, can be seen in Figure 2.

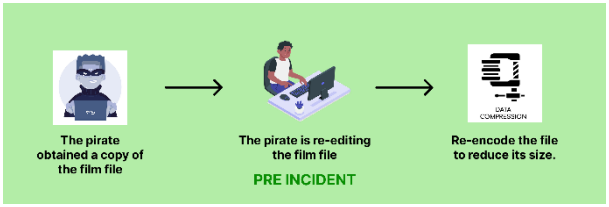


Figure 2: Pre-Incident Stage of the Film Piracy Case

Figure 2 depicts the perpetrator starting their actions after obtaining the original film file. Next, the perpetrator re-edits the film by adding hard subtitles and watermarks, and then re-encodes the film file with the aim of reducing its size.

The second stage of the simulation is the incident stage, which is shown in Figure 3.

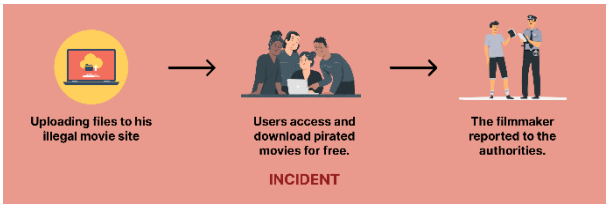


Figure 3: Stage of Incident in the Film Piracy Case

Figure 3 depicts the perpetrator uploading a copied file to their illegal streaming site. So that anyone can access and watch the

film, until the creator of the film discovers that their film has been pirated and is being distributed illegally, the creator immediately reports to the authorities to take action on this film piracy case.

The final stage of this simulation is the post-incident stage, as explained in Figure 4.

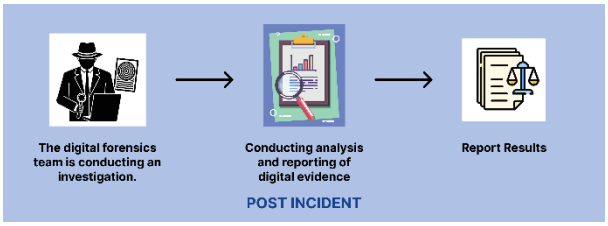


Figure 4: Post-Incident Stage of the Film Piracy Case

Figure 4 depicts the sequence of events post-incident, where the authorities collaborate with the forensic team to investigate the case. As an initial step, the team created a forensic image of the perpetrator's device found during the investigation, and subsequently, the forensic team discovered the original film file and the modified film file (the perpetrator's alteration). In this research, the post-incident process not only focuses on identifying the perpetrator but also on proving the authenticity and integrity of the found multimedia files. Thru metadata analysis, hash verification, and visual comparison between the original file and the modified file, the forensic team can obtain information about the changes that occurred in the film file.

4.1 Identification

The identification stage is the initial phase in the digital investigation process that refers to the National Institute of Justice (NIJ) method. At this stage, an initial classification process is carried out on the data and devices to be analyzed. Documentation of the evidence is displayed in Figure 5.

Figure 5: Laptop Evidence

Figure 5 displays the ASUS VivoBook X515JAB laptop device as evidence in a film piracy case. This process not only involves taking a photo of the device but also includes recording crucial information such as the brand, type of device, and serial number. Complete information about the evidence can be seen in Table 1.

Table 1. Specification of Evidence

No	Specification	Description
1.	Merk	ASUS
2.	Series	VivoBook X515JAB
3.	Processor	Intel® Core™ i3-1005G1 CPU @ 1.20GHz
4.	RAM	4 GB
5.	SSD	512 GB
6.	OS	Windows 11

Table 2. Tools

No	Tool	Type	Description
1.	Laptop	Hardware	ASUS TUF F15 FX506LHB, Intel i5-10300H CPU @2.50Ghz, 8192MB RAM
2.	FTK Imager	Software	Digital evidence acquisition tool
3.	Exiftool	Software	Metadata analysis tool
4.	HashMyFiles	Software	Hash value comparison tool
5.	FFmpeg	Software	Video file extraction tool
6.	Python	Software	Image difference detector tool, and thresholding on the frame

Table 2 shows complete information regarding the hardware and software used in this investigation process. The investigation team used laptops as the main system to run forensic tools. Meanwhile, in terms of software, several forensic tools were used, including FTK Imager, Exiftool, HashMyFiles, FFmpeg, and Python with the OpenCV and Matplotlib libraries.

4.2 Collection

The collection stage in this research is conducted to secure physical evidence and gather relevant digital evidence in the case of film piracy, such as original video files, copied video files, editing project files, subtitle files, and watermark files using FTK Imager. The initial step that needs to be taken is to run the write blocker, which serves as a safeguard to ensure that no changes or damage occur during the acquisition process. The usage display of the write blocker can be seen in figure 6.

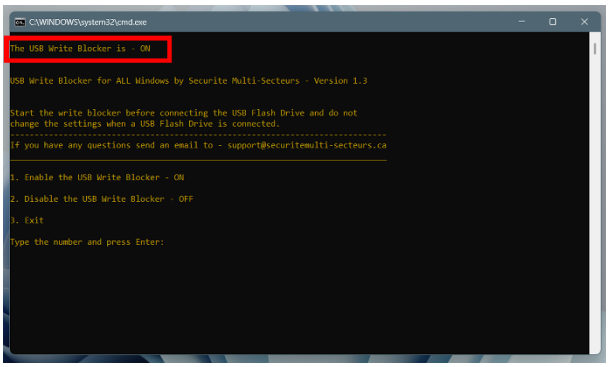


Figure 6: Write blocker Activated

Figure 6 shows the write blocker interface that has been activated. The use of a write blocker ensures that during the process of accessing storage media, no write operations occur that could alter the contents of digital evidence. Thus, the acquisition process supports the application of the chain of custody principle, making it accountable in the digital investigation process. Next, the imaging process can be carried out using the FTK Imager tool, as shown in Figure 7.

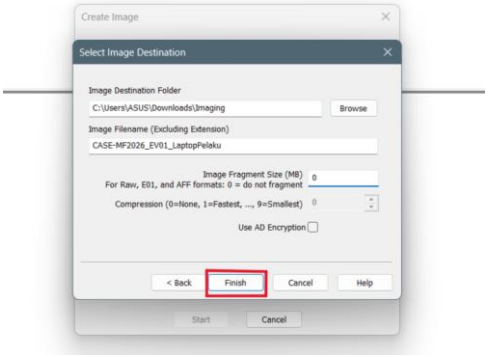


Figure 7: Create Imaging

Figure 7 is the data collection stage conducted using the live acquisition method, as the device was found still in an active condition when secured. The acquisition process was carried out using the FTK Imager tool, which allows for a comprehensive extraction of digital evidence of film piracy activities. After the imaging process is complete, FTK Imager provides a hash verification feature that displays a comparison of the hash from the original file with the image file. The hash value comparison is shown in Figure 8.

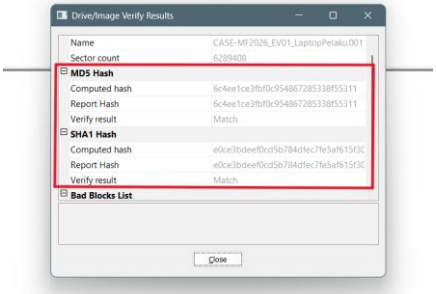


Figure 8: Hash Verification

Figure 8 shows a comparison of the hash from the original file with the image file. The result is that the hash values match for both MD5 and SHA1, meaning there were no changes at all during the image creation process.

4.3 Examination

This stage is the process of examining the previously obtained image results. At this stage, an examination of the directory structure and identification of digital evidence suspected to be related to film piracy activities, such as video files, subtitle files, watermark files, and editing project files, is conducted. To examine the data, a forensic tool called FTK Imager is used, which is capable of reading image capture files in RAW format with a .001 extension. The results of the examination are then used as the basis for the analysis stage to determine any changes or modifications that have occurred in the video file that is the subject of the investigation.

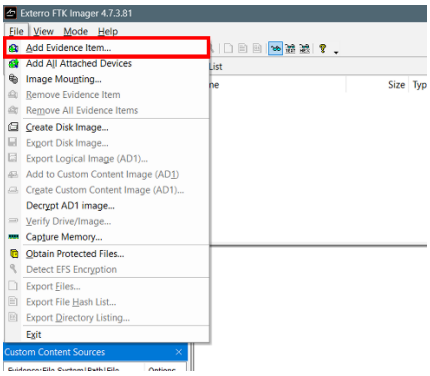


Figure 9: Add Evidence Item

Figure 9 is a feature of FTK Imager that can be used to open and examine the forensic image results obtained from the evidence. Thru the Add Evidence Item feature, investigators can load the acquisition results into the forensic examination environment, allowing for a structured process of searching and analyzing digital artifacts. At this stage, the investigator can browse directories, examine metadata, and identify files related to film piracy activities without altering the data on the original evidence.

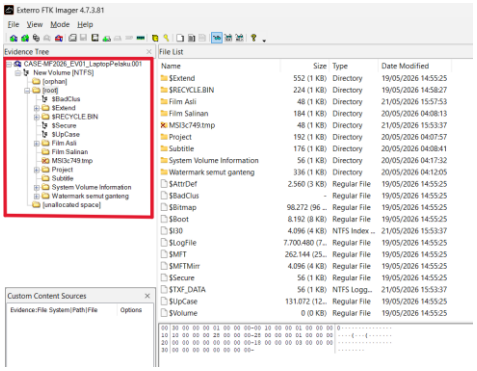


Figure 10: Evidence Directory Structure

Figure 10 displays the directory structure of evidence in the form of video files and other digital artifacts found in the acquisition results. After the examination, a folder related to this case was found. The digital evidence discovered included 1 original video file, 1 copied video file, 2 watermark files, 12 editing project files, and 1 subtitle file.

4.4 Analysis

The analysis stage is a process conducted after the examination stage, aimed at a thorough and in-depth investigation of the findings that have been discovered. This analysis includes metadata analysis, hash comparison, frame extraction, and tampering analysis.

4.4.1 Metadata Analysis

This metadata analysis stage uses Exiftool to analyze the metadata of the original and modified film files. The goal is to obtain technical information from the multimedia file. This stage can be used as evidence that the video has been edited, converted, or altered during the process, as metadata can provide information about the file's history and characteristics.

The metadata analysis process was conducted on two video files, GAK GENAH.mp4 and GAK GENAH semut ganteng.mp4. The acquired video files were placed into the analysis folder along with the ExifTool application, and the command prompt was used to perform the metadata inspection.

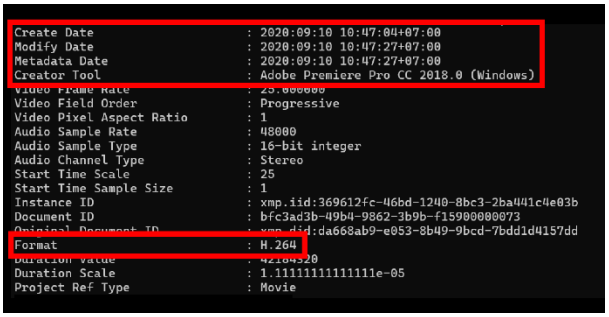


Figure 11: Metadata File Original Film

Figure 11 is the metadata of the original film file, showing some information about the original file named GAK GENAH.mp4. For example, create date 2020:09:10 10:47:04+07:00, modify and metadata date 2020:09:10 10:47:27+07:00, then creator tool Adobe Premiere Pro CC 2018.0 (windows) and has H.264 format.

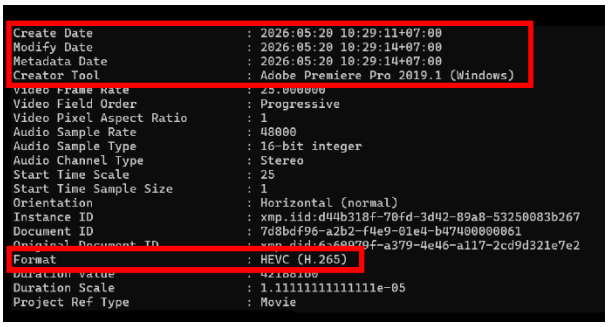


Figure 12: Metadata File Copy Film

Figure 12 shows some information about the copied file named GAK GENAH semut ganteng.mp4. That is, create date 2026:05:20 10:29:11+07:00, modify and metadata date 2026:05:20 10:29:14+07:00, then creator tool Adobe Premiere Pro CC 2019.1 (windows) and has HEVC (H.265) format.

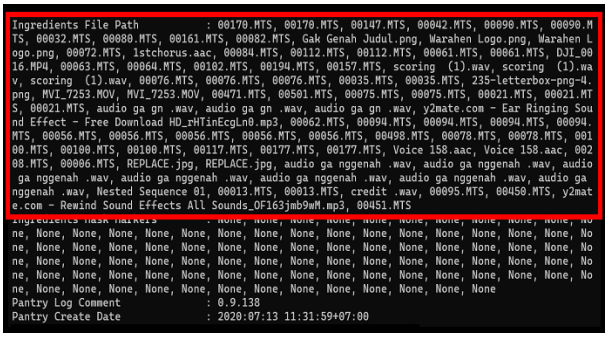


Figure 13: Metadata File Original Film

Figure 13 is the ingredients file path, which is a metadata tag that describes the file or supporting assets embedded within the parent file. In the original film file, it appears to contain the original video file from the camera and several supporting asset files such as logos and audio.

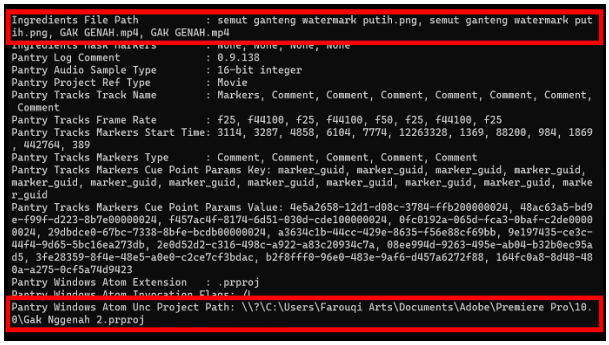


Figure 14: Metadata File Copy Film

Image 14 is the ingredients file path of the copy film file, which only contains the original film file and modified supporting assets such as watermarks and subtitles. Next, there is information about the pantry windows atom unc project path: \\?\C:|Users\Farouqi Arts\Documents\Adobe\Pre miere Pro\10.0\Gak Nggenah 2.prproj, which is the directory belonging to the original film editor.

Figure 15: Metadata File Original Film

Figure 15 shows the metadata from the original film file in the average bitrate section, which is the average amount of data processed per second in the video file and affects the visual quality and file size. In the original film file, the average bitrate value is 13.2 Mbps.

Figure 16: Metadata File Copy Film

Figure 16 shows the average bitrate value of the copied video file at 5.81 Mbps. This indicates a difference in bitrate between the two film files. The change in bitrate is one indication that the film file has undergone re-encoding. The lower bitrate also indicates that the copied video was re-encoded with a different compression setting, which is consistent with the modification scenario described in this investigation.

4.4.2 Hash Value Comparison

This research uses Hashmyfiles to compare the hash values of original video files and copied video files. Hash is a unique digital fingerprint in the form of a sequence of alphanumeric characters generated by a mathematical algorithm. This value represents the contents of a file, where even the smallest change to the file will result in a different hash value.

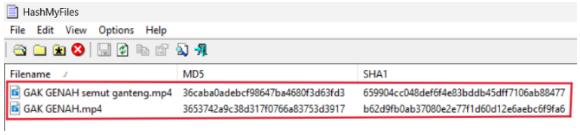


Figure 17: Hash Value Comparison

Figure 17 is a comparison of the hash values of the original video file and the copied video file using the HashMyFiles tool. The results showed that the hash values of the original and copied video files were different. This difference indicates that the two files are not identical at the binary level. Hash comparison therefore provides an initial indication that the copied video has undergone changes compared with the original video. However, the hash result alone cannot identify the type or location of the modification. Therefore, the hash analysis was complemented by metadata and frame-based analysis to determine the characteristics and visual location of the changes.

4.4.3 Frame Extraction

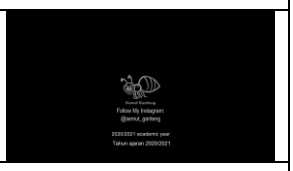
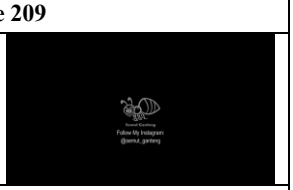
This research uses FFmpeg to perform frame-by-frame extraction from the original and modified video files. The frame extraction process is carried out to obtain each image display from the video. The extraction results in all frames being displayed in image format (.png) arranged sequentially according to their appearance in the video. The result of frame extraction will produce image files such as frame_000001.png, frame_000002.png, and so on, according to the number of frames in the video. This process aims to conduct an in-depth visual comparison of the two video files.

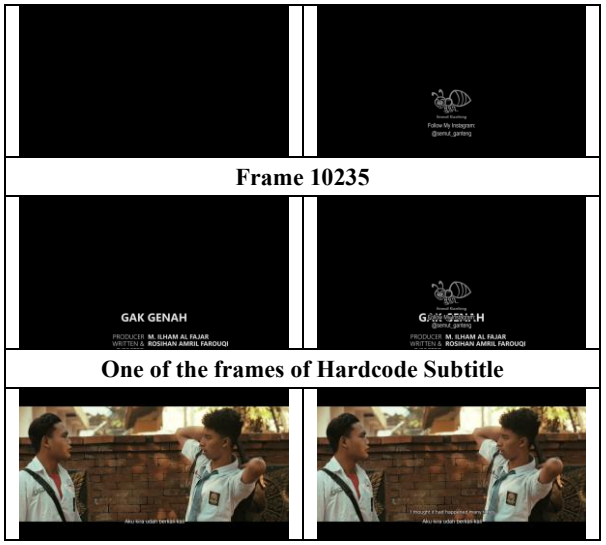
The extraction process of the original film file produced a total of 11,717 frames, while the copy film file produced a total of 11,718 frames. From the frame extraction results of the original film file and the copy film file, there is a difference in the total number of frames produced.

Based on the frame comparison results, it shows that changes have occurred in the visual content of the video after the copying and modification process was carried out. The comparison of frames revealed visual differences between the original film and the copy. A watermark was found to appear at the beginning and end of the video, specifically in frames 102 to 209 and frames 10101 to 10235. Additionally, hardcoded English subtitles were found above the Indonesian subtitles during the conversations. Meanwhile, the original film video does not have those additional visual elements. This difference indicates the occurrence of localization tampering in the form of visual modifications to the multimedia content.

This finding serves as one of the indicators that the copied file is no longer identical to the original file and has undergone a processing that can be proven thru detailed frame analysis. The visual comparison can be seen in Table 3.

Table 3. Visual Frame Comparison

Original Film	Copy Film
Frame 102	
	
Frame 209	
	
Frame 10101	

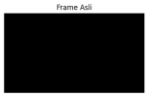
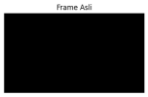


4.4.4 Tampering Analysis

This stage analyzes the difference image and thresholding to detect tampering in the modified video, particularly due to the addition of watermarks and subtitles. The process begins by comparing the original video frame and the copy extracted with FFmpeg, followed by using Python with the OpenCV and Matplotlib libraries. Frames are read using the cv2.imread() function in grayscale mode to facilitate analysis, and the cv2.absdiff() function is used to calculate the absolute pixel value difference between the two frames. The result of the image difference will display areas where pixel changes occur as brighter areas compared to other areas that do not experience changes.

The results of the tampering analysis show differences in the images, and the images detected have been modified. The frames selected for this analysis process are those indicated to have modifications, specifically in frames 102 - 209 where there are modifications to the watermark and English subtitles, then in frames 10101 - 10235 where there are modifications to the watermark, and frame 1910 was chosen as one of the frames with modifications to the English subtitles. The results can be seen in Table 4.

Table 4. Tampering Analysis Results

Frame	Original Frame	Difference Image	Detected Tampering Area
102			
209			
10101			
10235			
1910			

4.5 Reporting

The final stage in the National Institute of Justice (NIJ) digital forensics method is the reporting stage. Here, all examination and analysis results of the digital evidence are neatly documented in the form of a forensic report. The reporting process is carried out by summarizing all the results of the acquisition, examination, and analysis of the original film files and the files obtained from the perpetrator's laptop evidence.

Table 5. Acquisition Results

No	Folder Name	Description	Total Files
1.	Film Asli	Original film folder	1
2.	Film Salinan	Copy film folder	1
3.	Project	Project software editing folder	12
4.	Subtitle	Subtitle folder	1
5.	Watermark semut ganteng	Watermark folder	2
		Total	17

In Table 5, the acquisition results using FTK Imager are displayed, yielding 1 original video file, 1 copied video file, 12 project files, 1 subtitle file, 2 watermark files, with a total of 17 files successfully found. The results of the metadata analysis stage using ExifTool show differences in metadata attributes between the original film video and the modified video, such as file name, file size, average bitrate, creation and modification dates, and software information used in the video processing. The results of the hash comparison stage using HashMyFiles show that the original video and the copied video have different hash values. This difference in hash values indicates that the two files are not identical and have undergone changes in their digital data structure. Video frame analysis using extraction from FFmpeg and difference image analysis and thresholding using Python with the OpenCV and Matplotlib libraries successfully showed the areas of change visually in the copied video frames. The analysis results show that the watermark and subtitle appear as areas of change that are not present in the original video, the results can be seen in Tables 3 and 4. From all the stages of examination and analysis that have been conducted, the examination results show that the digital characteristics of the modified video file have undergone changes. Therefore, it can be concluded that the copied film file is a modified version of the original film file.

5. CONCLUSIONS

This research demonstrated the application of the National Institute of Justice (NIJ) method for investigating a simulated film piracy case involving video modification. The investigation successfully obtained 17 digital artifacts, including the original and copied video files, editing project files, subtitles, and watermark files. Metadata analysis identified differences in codec, processing software, timestamps, and average bitrate, while hash comparison confirmed that the original and copied videos were not identical. Frame extraction and tampering analysis using FFmpeg, OpenCV, and Matplotlib successfully detected and localized added watermarks and hardcoded subtitles in the copied video. These findings indicate that combining file-level, metadata, and frame-based analysis can provide comprehensive evidence of video modification. However, this study is limited to a simulated case and a limited number of modification scenarios. Future research should evaluate the approach using larger and more diverse datasets, various codecs and resolutions, and additional tampering types such as frame insertion, deletion, cropping, and audio manipulation. Automated detection using machine learning can also be explored to improve tampering localization and scalability.

6. REFERENCES

[1] K. Risandi And Tantimin, "Kajian Hukum Pembajakan Film Di Platform Telegram Di Indonesia," *J. Pendidik. Kewarganegaraan Undiksha*, Vol. Vol. 10, 2022, [Online]. Available: Https://Ejournal.Undiksha.Ac.Id/Index.Php/Jjpp/Article/View/45325

[2] G. A. P. K. D. I. W. N. Purwanto, "Pelaksanaan Hukum Terhadap Pelanggaran Hak Cipta Di Bidang Pembajakan Sinematografi (Film/Video)," *Kertha Semaya J. Ilmu Huk.*, No. Vol 5 No 1 (2017), Pp. 1–19, 2017, [Online]. Available: Https://Ojs.Unud.Ac.Id/Index.Php/Kerthasemaya/Article/View/44436/27011

[3] D. Z. Abidin, "Kejahatan Dalam Teknologi Informasi Dan Komunikasi," *J. Process.*, Vol. 10, No. 2, Pp. 509–516, 2015.

[4] S. H. Anak Agung Ngurah Agung Gde Lanang; I Made Dedy Priyanto M.Kn., "Regulasi Penetapan Hukum Mengenai Pembajakan Film Di Media Sosial Dalam Dunia Industri Perfilman Indonesia," *Kertha Negara J. Ilmu Huk.*, No. Vol 11 No 1 (2023), Pp. 63–73, 2023, [Online]. Available: Https://Ojs.Unud.Ac.Id/Index.Php/Kerthanegara/Article/View/91964/50421

[5] G. G. G. Raharja, "Penerapan Hukum Terhadap Pelanggaran Hak Cipta Di Bidang Pembajakan Film," *J. Meta-Yuridis*, Vol. 3, No. 2, Sep. 2020, Doi: 10.26877/M-Y.V3i2.6029.

[6] A. Suran Ningsih And B. Hediyati Maharani, "Penegakan Hukum Hak Cipta Terhadap Pembajakan Film Secara Daring," *J. Meta Yuridis*, Pp. 13–32, Sep. 2019, Doi: 10.26877/M-Y.V2i1.3440.

[7] Diego And S. Barbarosa Ida Ayu, "Peran Kemkominfo Terkait Pembajakan Film Pada Situs Streaming Film Ilegal," *Kertha Desa*, No. Vol 9 No 7 (2021), Pp. 64–76, 2021, [Online]. Available: Https://Ojs.Unud.Ac.Id/Index.Php/Kerthadesa/Article/View/75295/40909

[8] A. Permatasari, "Dalam 10 Bulan, Penonton Streaming Bajakan Menurun 55 Persen," Komdigi.Go.Id. Accessed: May 15, 2025. [Online]. Available: Https://Www.Komdigi.Go.Id/Berita/Sorotan-Media/Detail/Dalam-10-Bulan-Penonton-Streaming-Bajakan-Menurun-55-Persen

[9] M. Nabilah, "Ini Bukti Orang Indonesia Gemar Kunjungi Situs Film Bajakan," Databoks.Katadata.Co.Id.

[10] C. Y. Wowor, "Analisis Hukum Mengenai Pembajakan Film Terhadap Hak Cipta Pada Aplikasi Telegram Di Indonesia," *Lex Crim.*, No. Vol. 12 No. 4 (2024): Lex Crimen, 2024, [Online]. Available: Https://Ejournal.Unsrat.Ac.Id/V3/Index.Php/Lexcrimen/Article/View/58845/47946

[11] Imam Riadi, Abdul Fadlil, And Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute Of Standard And Technology (Nist)," *J. Resti (Rekayasa Sist. Dan Teknol. Informasi)*, Vol. 4, No. 5, Pp. 820–828, Oct. 2020, Doi: 10.29207/Resti.V4i5.2224.

[12] H. Idhofi And G. Zaida Muflih, "Akuisisi Barang Bukti Digital Pada Media Penyimpanan Flashdisk Menggunakan Framework National Institute Of Justice (Nij)," *Jati (Jurnal Mhs. Tek. Inform.*, Vol. 9, No. 3, Pp. 3978–3986, May 2025, Doi: 10.36040/Jati.V9i3.13459.

[13] R. A. Ramadhan And D. Mualfah, "Implementasi Metode National Institute Of Justice (Nij) Pada Fitur Trim Solid State Drive (Ssd) Dengan Objek Eksperimental Sistem Operasi Windows, Linux Dan Macintosh," *It J. Res. Dev.*, Vol. 5, No. 2, Pp. 183–192, Nov. 2020, Doi: 10.25299/Itjrd.2021.Vol5(2).5750.

[14] T. Ruslan, I. Riadi, And S. Sunardi, "Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute Of Justice," *J. Saintekom*, Vol. 12, No. 1, Pp. 69–80, Mar. 2022, Doi: 10.33020/Saintekom.V12i1.210.

[15] A. R. Triyanto And F. Fachri, "Analisis Forensik Bukti Digital Pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute Of Justice," *Jipi (Jurnal Ilm. Penelit. Dan Pembelajaran Inform.*, Vol. 9, No. 2, Pp. 1031–1042, Jun. 2024, Doi: 10.29100/Jipi.V9i2.5558.

[16] M. A. Kustian, "Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video , Metadata Image Dan Magic," Vol. 2, No. 2, 2023, Doi: 10.20885/Snati.V2i2.21.

[17] E. I. Alwi And S. Anraeni, "Analisis Rekaman Video Cctv Dengan Teknik Enhancement Menggunakan Metode National Institute Of Justice (Nij)," Vol. 17, No. 1, Pp. 88–95, 2024.

[18] I. Riadi, R. Umar, And I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

[19] Maria Oktaviani Kartika Tua, Aksi Sinurat, and Adrianus Djara Dima, "Perlindungan Hukum terhadap Pencipta Karya Sinematografi dalam Pembajakan Film pada Situs Streaming Ilegal," *Jemb. Huk. Kaji. ilmu Hukum, Sos. dan Adm. Negara*, vol. 1, no. 4, pp. 39–48, Nov. 2024, doi: 10.62383/jembatan.v1i4.922.

[20] S. Battiato, O. Giudice, and A. Paratore, "Multimedia Forensics : discovering the history of multimedia contents," no. June, pp. 23–24, 2016, doi: https://doi.org/10.1145/2983468.2983470.

[21] I. Riadi, A. Fadlil, and M. I. Aulia, "Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 3, pp. 107–118, 2019.

[22] I. Riadi and E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," vol. 10, no. 1, pp. 18–22, 2018.

[23] Marc Buccat, "How FTK Became the Gold Standard of Digital Forensics," mcafeeinstitute.com. Accessed: Jun. 18, 2026. [Online]. Available: https://www.mcafeeinstitute.com/blog/ftk-computer-forensics-complete-guide

[24] I. Riadi, A. Yudhana, R. Verry, and A. Saputra, "Forensik Video Pada CCTV Menggunakan Framework Generic Computer Forensics Investigation Model (GCFIM)," vol. 10, no. 2, pp. 540–547, 2023, doi: 10.30865/jurikom.v10i2.5888.

[25] P. Harvey, "ExifTool by Phil Harvey," exiftool.org. Accessed: Jun. 18, 2026. [Online]. Available: https://exiftool.org/

[26] Nir Sofer, "HashMyFiles v2.50 - Calculate Md5/Sha1/Crc32/Sha-256/Sha-512/Sha-384 hashes of your files Copyright (c) 2007 - 2024 Nir Sofer," nirsoft.net. Accessed: Jun. 18, 2026. [Online]. Available: https://www.nirsoft.net/utils/hash_my_files.html

[27] Fabrice Bellard, "About FFmpeg," ffmpeg.org. [Online]. Available: https://ffmpeg.org/about.html

[28] Dicoding, "Python: Pengertian, Contoh Penggunaan, dan Manfaat Mempelajarinya," dicoding.com. Accessed: Jun. 18, 2026. [Online]. Available: https://www.dicoding.com/blog/python-pengertian-contoh-penggunaan-dan-manfaat-mempelajarinya/

[29] Kamal DS, "The difference in Reading an image using OpenCV and Matplotlib," medium.com. Accessed: Jun. 18, 2026. [Online]. Available: https://korlakuntasaikamal10.medium.com/the-difference-in-reading-an-image-using-opencv-and-matplotlib-5529415704e5

[30] Revoupedia, "Mengenal Matplotlib dalam Python untuk Visualisasi Data," revou.co. Accessed: Jun. 18, 2026. [Online]. Available: https://www.revou.co/panduan-teknis/matplotlib-python