Digital Forensic Analysis of YouTube Live Streaming Services using National Institute of Standards and Technology Method

Ahmad Raihan Faaza Wildan
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Technological advancements have made it easier for users to interact directly through various features, one of which is live streaming. On the other hand, this feature has the potential to be misused as a promotional medium for online gambling sites. This study aims to obtain digital evidence that can serve as artifacts and prove the existence of online gambling site promotion activities on YouTube using a digital forensic approach. The research was conducted through a simulated case scenario in which the perpetrator promoted an online gambling site via the donation feature during a live stream. The investigation process utilized the National Institute of Standards and Technology (NIST) methodology, which includes the stages of Collection, Examination, Analysis, and Reporting. The tools used included OBS Studio to capture live stream recordings as digital evidence, ExifTool to extract video file metadata. The metadata examination successfully identified characteristics of the video file. Results of this study yielded a live streaming recording file as digital evidence an examination of the frames revealed 2 key timestamps and 3 key frames at 00:12:37, when the donation message appeared on the screen, and at 00:12:49, when the live streaming read the message aloud. Based on these results, it can be concluded that the NIST method is capable of supporting the digital forensic investigation process in acquiring, examining, and analyzing digital evidence, thereby enabling the systematic verification of promotional activities for online gambling sites on YouTube's live streaming service.

Keywords
Online Gambling; Digital Forensics; NIST; Live Streaming.

1. INTRODUCTION
The Internet has become an essential part of the digital age. The Fourth Industrial Revolution posits that every member of society will always be connected to the Internet for communication[1]. Anyone can access the Internet anytime, anywhere[2]. This change has brought about significant shifts in society, one of which is the way people access entertainment and information however, the ease of accessing the internet has also led many to abuse this convenience for personal gain and to the detriment of others[3][4].

One of the most widely used platforms today is YouTube, which is easily accessible. YouTube is a social media service that allows users to upload, watch, and share videos, as well as conduct live streams, all of which are accessible to anyone[5].

This ease of use creates opportunities for abuse, particularly through the donation feature on live streams. Donations intended to promote online gambling sites are one of the most common forms of illegal activity on YouTube's live streaming platform[6]. This situation presents a unique challenge for law enforcement in the digital realm, as the promotion of online gambling sites through the donation feature is often disguised with more subtle narratives, making it difficult for both streamers and viewers to recognize immediately and creating a new loophole for unscrupulous individuals to insert promotions for online gambling sites[7].

This reinforces the urgency of research into the process of identifying and extracting digital evidence on YouTube's live-streaming service, with the aim of clarifying the role of digital forensics in handling cases involving the promotion of online gambling sites while also deepening understanding of the potential misuse of live-streaming features as a medium for illegal promotion[8].

Various previous studies have applied a digital forensic approach to the investigation of digital evidence. A study by Azhiman et al. used ExifTool to verify the authenticity of YouTube videos in order to counter misinformation and found no anomalies in the metadata, such as file modifications[9]. Researchers Muharam et al. conducted a study on the use of influencers in promoting online gambling sites using sentiment analysis and found a public opinion trend of sharp criticism regarding influencer involvement[10].

Although previous studies have addressed the acquisition of digital evidence and the analysis of metadata, this study focuses on YouTube's live-streaming service by examining whether the promotion of online gambling sites through the donation feature during live streams is indeed occurring, using the National Institute of Standards and Technology (NIST) methodology which is widely adopted by forensic experts as a framework for the structured search for digital evidence[11], which consists of four main stages: Collection, Examination, Analysis, and Reporting[12].

The study was conducted using a simulated live-streaming scenario with OBS Studio, ExifTool, and various frames obtained from the recording to obtain digital evidence. Based on this description, this study aims to obtain digital evidence that can be used as artifacts and to analyze the promotion of online gambling sites on YouTube's live-streaming service using a digital forensic approach based on the NIST methodology.

2. LITERATUR STUDY
2.1 Live Streaming YouTube
YouTube is one of the digital platforms that offers a live

streaming feature[13]. The live streaming service allows users to watch an event in real time. YouTube, which allows users to access the platform from various devices such as laptops and smartphones, offers a donation feature to convey information or provide direct support to streamers during live streams. This feature has been exploited to disseminate content containing promotional messages for online gambling sites through the live streaming service[14].

2.2 Forensik Digital

Digital forensics is a branch of forensic science used to collect, analyze, and present valid evidence[15]. Digital forensics is a technique applied to obtain electronic or digital evidence, with the aim of reconstructing cybercrimes and supporting the analysis process in technology-based criminal cases[16][17]. It also involves obtaining admissible digital evidence or evidence related to actions involving digital devices or media, including the identification, collection, examination, and preservation of digital evidence related to legal violations[18].

2.3 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) provides a digital forensics framework used for structured investigations[19]. It consists of four stages: collection, which is the identification stage that maintains data integrity[20]; examination, which processes the collected data using standardized forensic techniques and tools; analysis, which evaluates the data obtained from the previous stage; and reporting, which involves compiling a final report covering all the information and data obtained[12].

2.4 ExifTool

ExifTool is forensic software that includes a command-line application for reading, writing, and identifying hidden information in a file, as well as manipulating metadata[21]. Metadata provides details about a file's information, making it possible to determine whether a file is authentic or has been tampered with[9][22]. Metadata can be used to verify the validity of the analyzed video and prevent manipulated content from being used as evidence.

2.5 OBS Studio

OBS Studio is screen recording software capable of recording video and audio in real time without downloading content from the platform, so the resulting data accurately reflects the original display without any changes[25].

3. RESEARCH METHOD

This research employs a framework from the National Institute of Standards and Technology (NIST), which consists of four research stages. In the Collection stage, live broadcast activities are recorded using OBS Studio, accompanied by the documentation of URLs, channel names, access times, and live chat content.

The Examination stage involves verifying the authenticity of the videos using ExifTool, as well as analyzing video frames and timestamps to prepare digital evidence for file structure inspection. The Analysis stage is conducted to understand how the promotion of online gambling sites occurs on YouTube's live streaming service, focusing on three aspects.

First, data analysis is performed by evaluating the visual content of the video recordings to identify donation messages containing the names of online gambling sites, while also analyzing metadata and text artifacts to validate the authenticity of the videos.

Second, contextual and activity analysis focuses on understanding the behavior of streamers specifically how they receive and read out donation messages to determine their intent.

Third, the entire analysis process adheres to the stages outlined in the NIST methodology.

Finally, the Reporting stage compiles all investigative findings into a forensic report. These stages are illustrated in Figure 1.



Figure 1 : Stages of the NIST Method

4. RESULT AND DISCUSSION

This study was conducted to analyze promotional activities for online gambling sites occurring on YouTube's live streaming service. The analysis aims to understand how these promotional activities take place on YouTube's live streaming service by focusing on three aspects.

First, data analysis was conducted by evaluating the visual content of video recordings to identify donation messages containing the names of online gambling sites, as well as by analyzing metadata and textual artifacts to validate the authenticity of the videos. Second, contextual and activity analysis focused on the behavior of streamers when receiving and reading donation messages. Third, the entire analysis process followed the NIST methodological framework to ensure the investigation was conducted systematically and the results could be compiled into a structured digital forensic report.

The research subjects consist of YouTube live stream video recordings obtained through simulation, including URLs, access times, donation activity, and channel names to protect the identity of the data sources.

A visual simulation was conducted to illustrate a case of online gambling site promotion. This simulation is used to provide an overview of the sequence of events in the promotion of an online gambling site, as well as the relationships between the various stages of the method, thereby facilitating a structured understanding.

The simulation also presents a representation of the situation when investigators received a report regarding a live stream promoting an online gambling site, before, during, and after the promotional activities took place. This allows the digital evidence obtained from the recordings to be analyzed based on the chronological sequence of events. The first stage is the pre-incident phase, as shown in Figure 2.

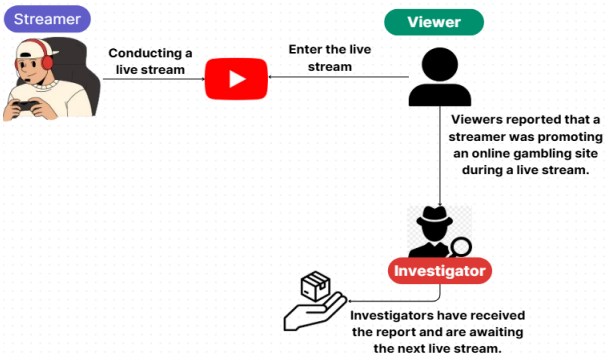

Figure 2 : Pre Incident phase

Figure 2 shows the initial situation: the streamer is live-streaming as usual, and viewers are joining. The viewer repor to investigator that te live stream appeared to promot an online gambling site. Investigator receiving the report and waiting for the next live stream to gather digital evidence.

Next is the incident phase, shown in Figure 3.

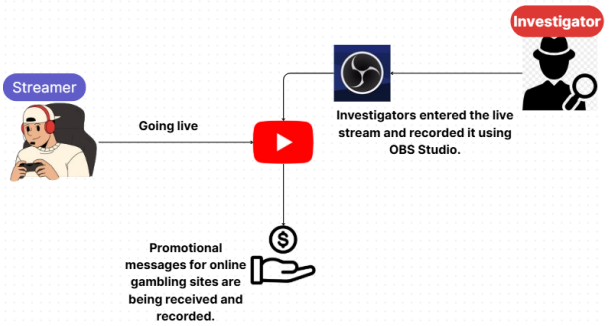

Figure 3 : Incident phase

Figure 3 shows an example of an online gambling site being promoted during a live broadcast on YouTube. Investigators accessed the live broadcast and used OBS Studio to record the stream. The recording captured donation messages that included the name of an online gambling site, an invitation to play, and promises of winnings on that site. Whenever such a message appeared during the live broadcast, the streamer would read it aloud immediately after receiving it.

The next stage is the final stage the post-incident phase as shown in Figure 4.

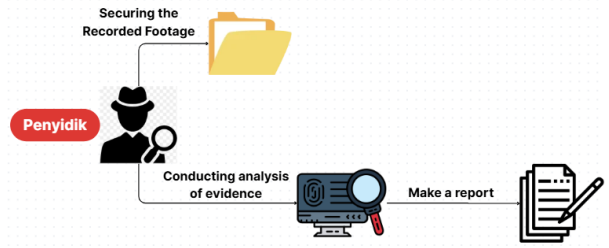

Figure 4 : Post Incident Phase

In the post incident phase, as shows in Figure 4, the live-streaming recordings obtained through the simulation process are secured as digital evidence for digital forensic investigation. The evidence, in the form of screen-recording video files, is then examined using the National Institute of Standards and Technology (NIST) methodology through the stages of Collection, Examination, Analysis, and Reporting to obtain and analyze digital artifacts related to the promotional activities of online gambling sites.

4.1 Collection

The Collection phase is the initial stage in the digital forensics process, aimed at collecting and securing digital evidence relevant to the research. In this study, the data collection effort focused on live-streaming activity recordings on the YouTube platform that contained promotional elements for a specific website via the donation feature.

The evidence collection process was conducted in accordance with digital forensic principles, particularly regarding the preservation of data authenticity and integrity from the very beginning of the acquisition process. The acquired data was then stored in a dedicated directory separate from other data to prevent accidental changes or manipulation of the files. In addition to video recording, documentation of the live streaming activity was also performed by capturing frames from specific sections containing promotional elements for a particular website.

Digital evidence in the form of screen-recorded video files was obtained through a live-streaming simulation using OBS Studio as a real-time capture tool. During the recording process, the original YouTube platform interface including the URL, channel name, live chat, and access time was preserved to ensure the data source's identity remained intact time of acquisition, as shows in Figure 5.

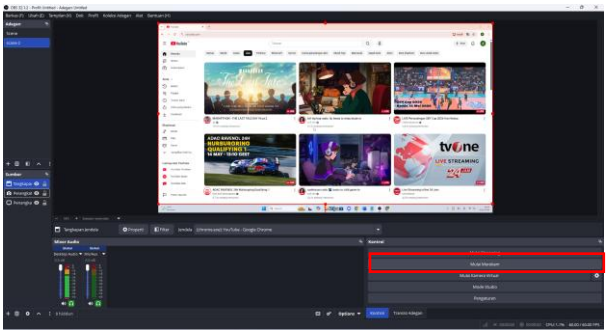

Figure 5 : Recording Process with OBS Studio

Figure 6 shows the initial conditions when recording a live stream with the channel account name tyyy.

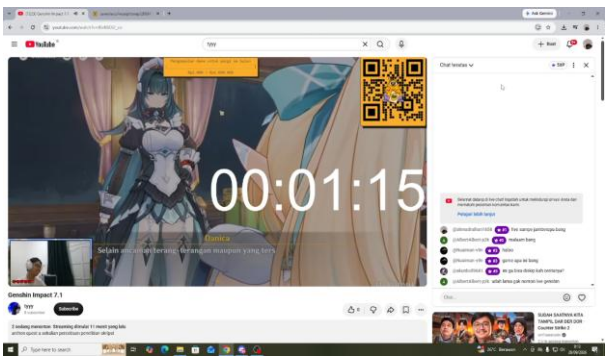

Figure 6 : recording from a live streaming

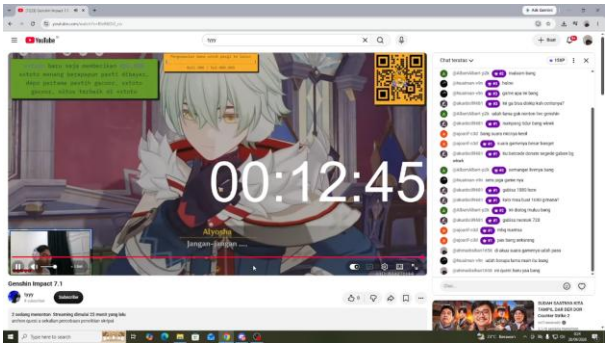

Figure 7 : Donation message that appears

Based on Figure 7, the donation message includes the name of an online gambling site, "xxtoto", while Figure 8 display imagery associated with that site.

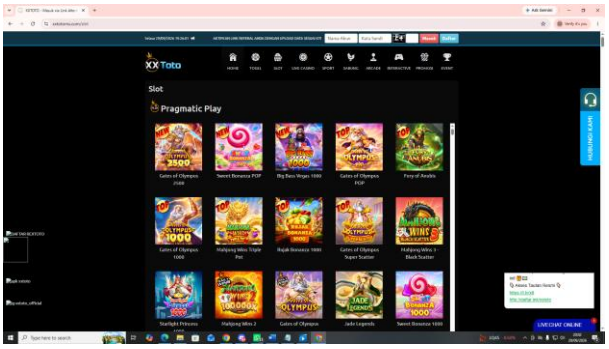

Figure 8 : Online gambling site xxtoto

Prior to further investigation, the donation link provided during the live stream was examined; this link leads to a donation platform, as illustrated in Figure 9.



Figure 9 : Donation platfrom

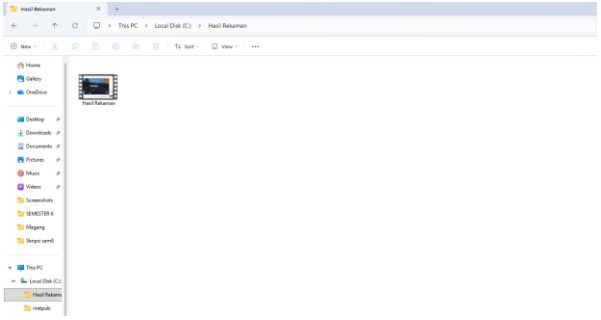

Figure 10 : Folder for storing recording files

After receiving donation messages that appeared during a live stream and verifying both the donation platform and the name of the online gambling site the next step is to save the recording into a folder, as shown in the image 10.

4.2 Examination

An examination of the digital evidence was conducted to obtain information that could support further analysis. At this stage, an initial examination was performed on the live-streaming video files to obtain technical information that could be used to support the investigation.

The metadata examination was conducted via Command Prompt, followed by an analysis of the live streaming video files during the Examination phase using ExifTool, which successfully yielded information such as the format, encoder, and recording time. This information was used to examine the file characteristics and verify them against the acquisition process that had been carried out.

The metadata obtained from this examination also provides supporting information regarding the characteristics of the video file used as digital evidence. The results of this examination are then used as the basis for subsequent analysis stages, particularly in ensuring that the video file is consistent with the acquisition process, As shows in Figure 11.

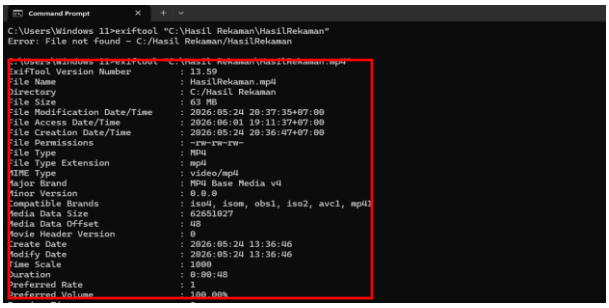

Figure 11 : Exiftool Results

Figure 12 also shows the encoder used, indicating that the video file used as evidence was recorded during the Collection phase. This information is used to ensure that the recorded video file is valid and consistent with the acquisition process carried out during the Collection phase.

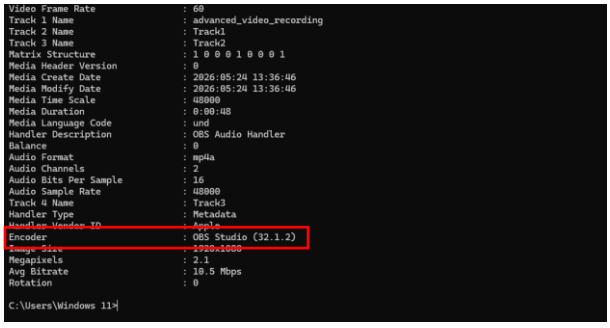

Figure 12 : Information on the Encoder Used

In addition to metadata examination is also performed. The results from this stage serve as the basis for proceeding to the next stage. The metadata examination provides information about the file's characteristics, allowing the video file to be used to identify the activities occurring in the live stream recording.

4.3 Analysis

The Analysis phase is the core phase of this study, focusing on identifying digital evidence obtained from video recordings related to the promotion of online gambling sites.

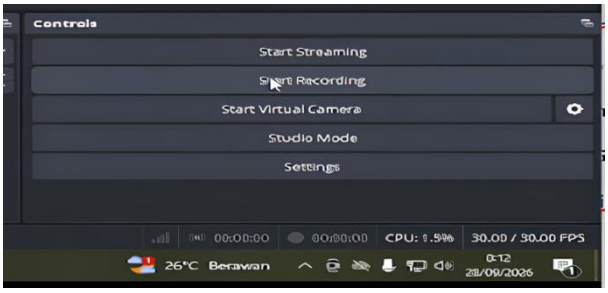

Figure 13 : Observation result

Based on the examination results using ExifTool, several pieces of information were found, such as the file modification date/time on 28/09/2026 at 00:26:00, whereas the observation of the recording process began on 28/09/2026 at 00:12. The recording file has a duration of 13 minutes and 44 seconds; thus, if the start time is used as a reference, this value matches the file modification date/time in the metadata results. Consequently, the timestamp shows consistency between the metadata and the end time of the recording. Figure 13 shows the observation time of the recording file.

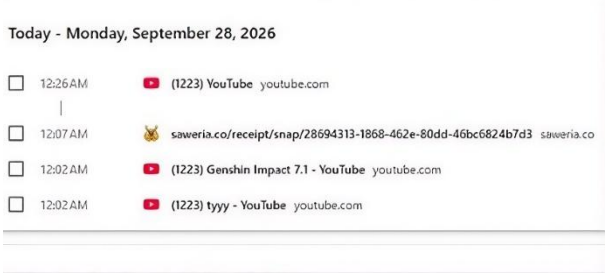

Figure 14 : History chrome

Next, matching was performed with Google Chrome digital artifacts in the form of Chrome history, with a time range of approximately 00:02 for accessing the live streaming account "tyyy" and ending at 00:26 on 28/09/2026, as shown in Figure 14.

An analysis of several video frames revealed the initial appearance of a donation message, as shown in Figure 15.

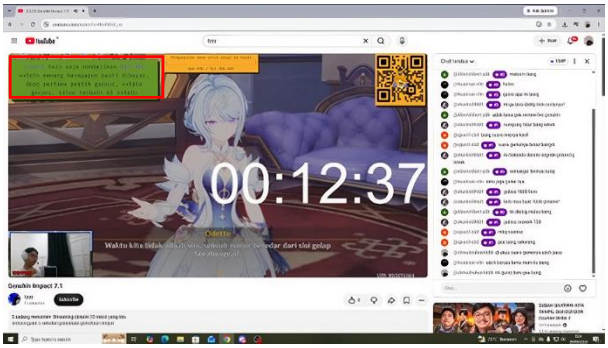

Figure 15 : Initial Appearance Of The Donation Message

Based on the screenshot, the donation message appears in the live stream and can be seen by both the streamer and viewers watching the live stream. The donation message contained information in the form of the name of an online gambling site and a sentence encouraging viewers to access the site, as shown in Figure 16.

Thus, the donation message that appeared can be categorized as an artifact related to promotional activities. This finding indicates that the donation feature can be utilized as a promotional medium for both streamers and viewers following the live stream.

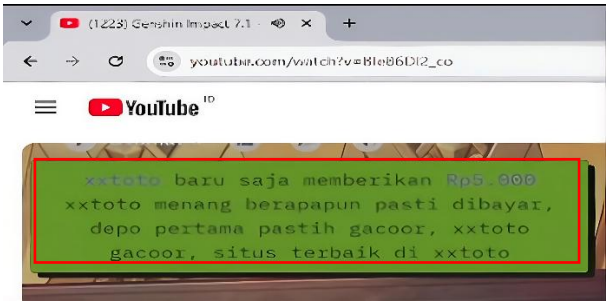

Figure 16 : Donation Online Gambling Site Promotion

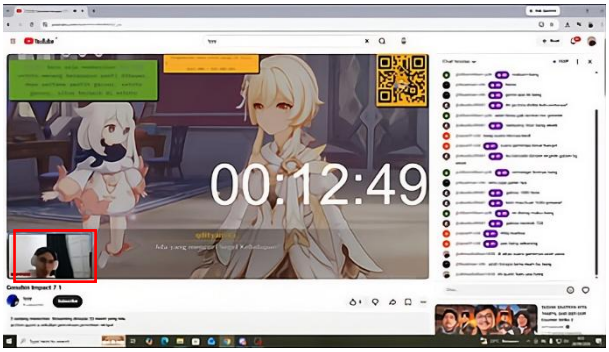

Figure 17 : The Streamer Reads Out Donation Messages

The analysis also showed that the streamer read aloud the donation message as it appeared on the live-streaming screen, based on a frame by frame review. Thus, information containing promotional elements was not only disseminated through visual media but was also reinforced through verbal delivery during the live stream, as shown in Figure 17.

The findings indicate that promotional activities can be observed not only through the presence of donation messages but also through the context in which these messages appear during live streams. The appearance of messages, their content, and the streamer's reading of them are interrelated findings in the analysis process. Each finding provides additional information that can be used to understand the chronology of activities occurring during live streams.

The results of the analysis show that promotional information is not only displayed visually through donation messages that appear on the live streaming screen, but is also verbally relayed by the simulation participants to the audience watching the broadcast. These findings indicate a correlation between the donation messages received and the activity of reading those messages.

In addition, the digital artifacts obtained from the frame

extraction successfully revealed the chronology of promotional activities that took place during the broadcast. Each analyzed frame provided complementary information, ranging from the appearance of donation messages to the process of conveying information to viewers. Thus, the Analysis phase successfully identified promotional activities for online gambling sites on YouTube's live streaming service and reinforced the findings obtained from the digital evidence analyzed using the National Institute of Standards and Technology (NIST).

Based on the overall results of the analysis, promotional activities for online gambling sites during live streams can be identified through the donation feature. Evidence of the appearance of donation messages, message content containing promotional information, and streamers' responses to these messages are findings that support one another. These results were then used as the basis for compiling the investigative findings during the reporting phase.

4.4 Reporting

The Reporting phase is the final stage in the digital forensic investigation, which serves to document and present all research results and analyses conducted in the previous stages. In this phase, all forensic findings are systematically compiled to ensure they are clearly understood and scientifically accountable.

The Reporting phase also presents a summary of the digital forensic findings obtained throughout the investigation process. This summary aims to display the results acquired at each investigative stage of the study and to prove the existence of promotional activities for online gambling sites via the donation feature on YouTube's live-streaming service, as shows in Table 1.

Table 1 : Research Findings

Stage	Findings
Collection	• live broadcast recording file was successfully obtained as digital evidence. • Donation barcode successfully accessed • The site name has been successfully verified as an online gambling site.
Examination	• Video file metadata was successfully retrieved using ExifTool
Analysis	• The frame containing a donation message was successfully identified. • Donation message promoting an online gambling site was discovered. • The streamer was observed reading out donation messages during a live stream. • Analysis of the frame was successfully conducted. • Analysis of the timestamp was successfully conducted.

Furthermore, based on the examination of the recording file using ExifTool, several pieces of metadata related to the characteristics of the video file were obtained. This information includes the file name, file type, recording duration, file modification time, and the software used to perform the recording. The results of this metadata examination are shown in Table 2.

Table 2 : Exiftool results

Parameter	Results
File Name	HasilRekaman.mp4
File Type	MP4
Duration	13.44
File Modification date/Time	28-0902026 00.26:00
Encoder	OBS Studio (32.2.2)

Next timestamp correlation was performed to identify the timing of activities related to the research object in order to ensure the authenticity of the digital evidence used, as shown in Table 3.

Table 3 : TimeStamp Analysis

Source evidence	Time	Interpretation
Observation recordings	28/09/2026 00:12	At the beginning of the recording, based on the recorded material
File Modification Date/Time	28/09/2026 00:26	Metadata
Recording duration	13 minutes 44 seconds	Metadata
Chrome History	00:02 – 00:26	Chrome History

Table 4 : Frame Analysis

TimeStamp	appearance	Analisis
00:12:37	The initial appearance of a donation message	Donations are used as a medium to convey messages; these donations contain information promoting online gambling sites
00:12:49	Reading of donation messages by the streamer	Promotional information is conveyed to the audience through the live reading of messages

Table 4 shows the results of the frame analysis on the recording file. Based on all findings ranging from the collection of digital evidence, examination, and analysis, to the preparation of the investigation report, the results show that the recording during the live streaming process can be used as a source of digital evidence to identify the sequence of activities related to the delivery of online gambling site promotional information through the donation feature on YouTube's live streaming service.

All analysis results are then documented in the form of tables, metadata information, timestamps, and frames showing relevant parts of the recording, and the donation barcode as well as the name of the online gambling site were also successfully examined. Thus, the application of the NIST methodology through the Collection, Examination, Analysis, and Reporting stages can help the digital forensic investigation process be conducted in a structured manner, starting from viewer reports, acquiring digital evidence, to documenting the findings. The use of OBS Studio in the recording process and ExifTool in metadata examination also supported the process by generating recordings and technical information that can be used as material for examination and analysis in the research. Consequently, this study demonstrates that the NIST methodology was successfully applied and produced a reliable report.

5. CONCLUSION

The research results show that digital evidence in the form of live-streaming recording files from the simulation was successfully obtained, examined using ExifTool to extract metadata. Analysis of the video frames successfully identified 2 key timestamps and 3 key frames at 00:12:37, when the donation message appeared on the screen, and at 00:12:49, when the live broadcast read the message aloud, as well as the activities of the simulation participants who read the contents of the donation messages during the live stream; thus, the live stream recording can be used as a digital artifact to prove the existence of promotional activities for online gambling sites.

The National Institute of Standards and Technology (NIST) methodology which includes the Collection, Examination, Analysis, and Reporting phases was successfully and systematically applied in the digital forensic investigation process for this study. The Collection stage successfully obtained digital evidence in the form of live-streaming recording files the Examination stage successfully identified metadata and verified the integrity of the evidence the Analysis stage successfully identified promotional activities for online gambling sites through the donation feature based on the results of video frame analysis and the Reporting stage successfully documented all investigation results systematically. Thus, the NIST method has proven capable of supporting the legal and accountable substantiation of online gambling site promotional activities on the YouTube live streaming platform.

6. REFERENCES

[1] A. Khaliq and S. Novida Sari, “Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (Ids),” *J. Nas. Teknol. Komput.*, vol. 2, no. 3, pp. 150–158, 2022, doi: 10.61306/jnastek.v2i3.52.

[2] I. Riadi, Y. Safitri, and U. Ahmad Dahlan, “Hal. 1∼8 Menggunakan Metode Association of Chief Police Officers,” *J. Bumigora Inf. Technol.*, vol. 5, no. 1, pp. 1–8, 2023, doi: 10.30812/bite/v5i1.2977.

[3] M. Febrian As Shidiq, D. Alita, and L. Ratu Kec Kedaton Kota Bandar Lampung, “analisis sentimen masyarakat terhadap kasus judi online menggunakan data dari media sosial x pendekatan naive bayes dan svm,” *J. Sist. Inf. dan Inform.*, vol. 8, no. 1, 2025.

[4] I. Riadi *et al.*, “Investigasi Forensik Digital Kasus Pelecehan Seksual,” vol. 10, no. 2, pp. 2220–2228, 2026.

[5] V. Bee, M. A. Rizi, N. Rachmat, U. Multi, D. Palembang, and M. Sosial, “Klasifikasi komentar terhadap kriminal saat malam hari pada media sosial youtube menggunakan naïve bayes,” vol. 3, no. 2, pp. 101–105, 2024.

[6] U. Kristiana, A. R. Lahitani, C. B. Setiawan, and N. A. Sa’diya, “Analisis Forensik Digital Pada Komentar Youtube Live Menggunakan Sentiment Analysis.” [Online]. Available: http://ejournal.unjaya.ac.id/index.php/Teknomatika/

[7] D. Kharismanto, R. R. Phahlevy, and L. S. Program, “Volume 1 Number 10 Oktober 2024,” vol. 1, no. 10, pp. 49–65, 2024.

[8] R. N. Dasmen, M. Fikri, and H. E. Tritama, “Analisis Barang Bukti Pada Aplikasi Whatsapp Menggunakan FTK Imager di Kelas Teknik Komputer Universitas Bina Darma,” vol. 13, no. 2, pp. 321–326, 2024.

[9] F. Azhiman, R. N. Dasmen, and A. Apriyanto, “Implementasi Exiftool pada Forensik Metadata Video untuk Antisipasi Berita Hoax,” *J. Bina Komput.*, vol. 5, no. 1, pp. 23–28, 2023, doi: 10.33557/jbkom.v5i1.2422.

[10] Z. K. Muharam, W. Astuti, R. Prasida, and D. Syahputra, “penggunaan influencer dalam promosi judi online dan sentimen publik the use of influencers in promotion online gambling and public sentiment,” 2024. [Online]. Available: https://journals.telkomuniversity.ac.id/IJDPR

[11] I. Fawzan, “Identifikasi Jenis File pada Artefak Digital Menggunakan Algoritma Machine Learning,” 2024.

[12] M. Ali Diko Putra, A. Wirawan Muhammad, B. Parga Zen, R. Yunita Kisworini, and T. Rohayati, “Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86,” *J. Sist. Inf. Galuh*, vol. 2, no. 1, pp. 44–54, 2024, doi: 10.25157/jsig.v2i1.3695.

[13] D. Jalali Wal Ikram and S. Fachri Pane, “Deteksi Spam Bot Pada Komentar Youtube: Tinjauan Literatur Sistematis Bot Spam Detection on Youtube Comments: A Systematic Literature Review,” vol. 15, no. 2, pp. 103–123, 2023, doi: 10.22303/csrid.15.2.2022.103-123.

[14] P. Ramadaniar *et al.*, “Mobile Legend Bang Bang (MLBB) Youtube Video Streaming Sebagai Media Periklanan Dalam Judi Online English Title: Mobile Legend Bang Bang Youtube Video Streaming as Advertising Medium for Online Gambling”, [Online]. Available: http://ejournal.unitomo.ac.id/index.php/jkp

[15] M. Fransiskus and N. P, “Analisis Digital Forensik Metadata pada Rekayasa Digital Image sebagai barang bukti Digital,” *J. SAINS DAN Komput.*, vol. 8, no. 01, pp. 1–5, Jan. 2024, doi: 10.61179/jurnalinfact.v8i01.439.

[16] T. Rochmadi, A. Fadlil, I. Riadi, K. Nisa Panilestari, and Y. Wicaksono, “Analisis Teknologi Dan Prosedural Dalam Penanganan Insiden Untuk Mendukung Forensik Digital,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 10, no. 2, pp. 3285–3293, 2026, doi: 10.36040/jati.v10i2.17792.

[17] I. Hotul Hamdalah and F. Fachri, “Analisis Forensix Bukti Digital Penipuan Online pada Facebook Menggunakan Metode NIST (National Institute of Standards Technology),” *Remik*, vol. 9, no. 3, pp. 1072–1080, 2025, doi: 10.33395/remik.v9i3.15105.

[18] A. Fahrudin and G. Zaida Muflih, “Analisis Forensik Digital Pada Pesan Whatsapp Yang Terenkripsi Dengan Pretty Good Privacy (Pgp) Menggunakan Framework

Dfrws," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 780–787, 2024, doi: 10.36040/jati.v9i1.12506.

[19] M. Syukri, Imam Riadi, and Tole Sutikno, "Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. Process.*, vol. 20, no. 1, pp. 58–67, 2025, doi: 10.33998/processor.2025.20.1.2012.

[20] D. Royadi, M. Asfi, and A. Sevtiana, "Implementasi Metode Standar NIST Dalam Analisis Data Forensik Studi Kasus Penipuan Salah Transfer Mencatut Nama Wabup Pada SMP Ar-rohman Krangkeng," *LOFIAN J. Teknol. Inf. dan Komun.*, vol. 3, no. 1, pp. 12–19, 2023, doi: 10.58918/lofian.v3i1.216.

[21] N. C. P. Trisuwita and R. P. Kristianto, "Analisis Metadata EXIFtool dan Framework NIST Untuk Deteksi Manipulasi Citra," *JUPITER J. Comput. Inf. Technol.*, vol. 6, no. 2, pp. 165–174, 2025, doi: 10.53990/jupiter.v6i2.462.

[22] M. A. Kustian, "Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video, Metadata Image Dan Magic Number File," *J. Sains, Nalar, dan Apl. Teknol. Inf.*, vol. 2, no. 2, pp. 10–16, 2023, doi: 10.20885/snati.v2i2.21.

[23] N. Halimah and F. Ami, "Analisis Bukti Digital Twitter Web Menggunakan Live Forensic Pada Kasus Cyberbullying," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1005–1010, 2024, doi: 10.36040/jati.v9i1.12554.

[24] F. Isnaeni *et al.*, "ANALISIS FORENSIK SMARPHONE ANDROID," vol. 9, no. 1, pp. 1404–1410, 2025.

[25] V. G. Calabr, "Web Forensics - Acquisizione delle fonti di prova online," pp. 1–57.