Digital Forensic Analysis of Pirated Mobile Game Distribution on Telegram Platform using National Institute of Standards and Technology Method

Ghifari Tristan Fadli
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The distribution of illegal digital content, such as pirated mobile games, through instant messaging applications has become a serious threat to digital security and copyright protection. Telegram, as one of the most widely used messaging platforms, is frequently exploited by perpetrators to distribute APK files on a massive scale through public channels due to inadequate moderation mechanisms. This study aims to analyze the distribution of pirated mobile games on the Telegram platform using a digital forensic approach based on the National Institute of Standards and Technology (NIST) framework. Data were collected through a simulated distribution of pirated APK files on a rooted Android device. The extraction and analysis processes were conducted using MOBILedit Forensic Express and Magnet AXIOM forensic software. The forensic investigation successfully identified and extracted significant artifacts, including the pirated APK file (minecraft-1-21-130 (1).apk), public channel URL access history, Telegram user identity metadata, and application execution traces on the device. Cross-verification results from both forensic tools demonstrated that the NIST framework is effective in reconstructing the incident chronology and presenting valid, objective, and accountable digital evidence.

Keywords
Digital forensics, pirated mobile games, Magnet AXIOM, NIST, Telegram.

1. INTRODUCTION
The use of Information and Communication Technology (ICT) has significantly transformed nearly every aspect of human life, including the way people communicate and interact [1]. One tangible manifestation of this transformation is the rapid development of instant messaging services such as Telegram, which provides text, voice, image, and large file-sharing features with a high level of security through end-to-end encryption. Telegram allows users to create groups with up to 200,000 members as well as unlimited public channels. Unfortunately, these advanced features are highly susceptible to misuse for the illegal distribution of copyrighted content [2]. Telegram has become a major platform for the distribution of illegal applications, with 339 channels reportedly dedicated to cybercriminal activities, including the dissemination of pirated software, pirated media, and illegal mobile applications [3]. In Indonesia, the platform is also frequently used to distribute illegal content due to the lack of strict moderation controls [4]. The risks associated with such digital crimes have become increasingly concerning, particularly following reports indicating a rise in Telegram users from 60.2% in 2023 to 61.3% in 2024 [5].

Digital forensics is a systematic process of collecting, analyzing, and reporting digital data [6]. To support this process, several investigative frameworks have been developed, including the National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), Digital Forensic Research Workshop (DFRWS), and Integrated Digital Forensics Investigation Framework (IDFIF) methods [7]. The NIST framework was adopted in this study because it systematically outlines each stage of the investigation process, making it an effective guideline for resolving investigative problems [8]. The implementation of the NIST method has also proven effective in optimally identifying digital evidence from Telegram services [9].

Several previous studies have validated the reliability of the NIST method in investigations involving instant messaging applications. Earlier research successfully revealed the use of Telegram as a communication medium in online prostitution practices [10]. Another study identified the distribution of illegal content through the re-uploading of movies via public Telegram channels [11]. Mobile forensic implementations have also been successfully conducted to analyze the misuse of MiChat and Telegram applications [12]. The flexibility of the NIST framework has further been demonstrated through its application in investigating cyber fraud cases on Signal Messenger [13]. Moreover, the framework has been utilized in investigations of hoax dissemination on Facebook and Instagram [14], as well as in the analysis of negative content in WhatsApp group conversations using the Support Vector Machine algorithm [15]. Although numerous forensic studies have examined Telegram, research specifically focusing on the distribution of pirated mobile games remains very limited.

Based on this research gap, this study aims to analyze the distribution of pirated mobile games through the Telegram platform using a NIST-based digital forensic approach. The primary focus of this research is to identify relevant digital artifacts and evaluate the effectiveness of the NIST framework in uncovering digital evidence related to illegal content distribution cases. The findings of this study are expected to contribute academically and serve as a reference for law enforcement agencies in addressing digital crimes in Indonesia.

2. LITERATURE STUDY
2.1 Telegram
Telegram is a cloud-based instant messaging application developed by Pavel Durov [16]. The platform offers various advanced features, including the transmission of text messages, images, videos, documents, and the creation of groups and public channels with exceptionally large member capacities.

Telegram implements end-to-end encryption for secret chats and allows messages to be deleted without leaving traces for either party [17]. This flexibility and large-scale capacity have contributed to its popularity; however, due to the lack of strict moderation mechanisms, Telegram is frequently exploited as a primary channel for distributing illegal content, such as pirated movies obtained from streaming services [18], music, and pirated mobile applications.

2.2 Pirated Mobile Games

Pirated mobile games are unauthorized versions of game applications that have been modified or distributed without permission from the copyright holders. The distribution of such pirated applications not only causes economic losses to developers but also poses significant risks to users, as these applications may contain malware such as spyware, ransomware, or backdoors that threaten data privacy and security [19]. Numerous cases have demonstrated that cloned or repackaged versions of popular games often carry malicious payloads intended for illegal distribution through application marketplaces such as the Google Play Store [20].

2.3 APK File (Android Package Kit)

An APK file (Android Package Kit) is a file format with the .apk extension used by the Android operating system to distribute and install applications.

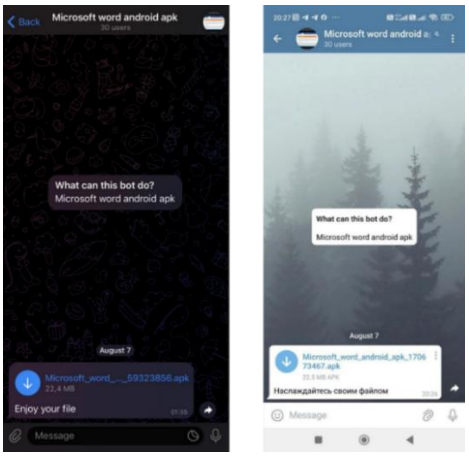

Figure 1 : Example of APK File Distribution

As shown in Figure 1, an illegal distribution practices, APK files are often modified (modded) to remove license protection mechanisms, insert additional advertisements, or even embed malware before being redistributed through platforms such as Telegram [21]. In forensic investigations, APK file analysis can be conducted using hybrid analysis, which combines static and dynamic approaches to comprehensively identify malicious components and examine the file structure [22].

2.4 Digital Forensic

Digital forensics is an activity related to the processes of preserving, identifying, filtering, and documenting digital evidence in computer-related crimes [23]. As a branch of forensic science, this field is specifically intended to investigate cybercrime evidence originating from digital devices or media [24]. The primary stages of digital forensics generally include identification, preservation, analysis, documentation, and presentation processes [25].

2.5 Mobile Forensics

Mobile forensics is a branch of digital forensics that focuses on the acquisition, analysis, and reporting of digital evidence from mobile devices such as smartphones and tablets [26]. Extraction techniques commonly applied in mobile forensics include logical acquisition, physical acquisition, and advanced extraction through rooting to obtain digital artifacts more comprehensively [27][28].

2.6 Digital evidence

Digital evidence refers to any information in the form of electronic data—such as data stored on computers, servers, cloud services, network logs, and metadata—that can be utilized in investigative and law enforcement processes [29]. In the context of digital forensics, digital evidence is not limited to message content or files, but also includes metadata, system logs, activity traces, and hidden artifacts that record user interactions with systems or applications [30].

2.7 National Institute of Standards and Technology (NIST)

The NIST method is a forensic framework that provides systematic, internationally standardized, and flexible guidelines for digital investigations, as illustrated in Figure 2.

Figure 2 : Stages of the NIST Method

This framework consists of four primary stages: Collection, which involves gathering evidence without altering the authenticity of the data [31]; Examination, which focuses on inspecting and filtering information [32]; Analysis, which involves evaluating data and reconstructing criminal events [33]; and Reporting, which is aimed at compiling the findings into a valid and objective report [34].

2.8 Digital Forensics Tools

The use of appropriate forensic software is crucial for extracting data from closed operating systems or encrypted applications. In Android device investigations, tools such as MOBILedit Forensic Express and Magnet AXIOM are frequently utilized, alongside other popular forensic tools such as Oxygen Forensic Detective and Cellebrite UFED [35].

2.9 MOBILedit Forensic Express

MOBILedit Forensic is a commercial software application designed to acquire, analyze, and generate data from mobile devices such as smartphones [36][37]. This software is highly reliable in accessing internal file system structures, mapping activity logs, extracting multimedia artifacts, and generating reports from deleted data.

2.10 Magnet AXIOM

Magnet AXIOM is a forensic tool developed by Magnet Forensics that is capable of extracting and organizing data from smartphones, computers, and social media platforms. The primary advantage of this tool lies in its timeline visualization feature, which enables investigators to more easily understand communication flows chronologically and recover deleted files with a high level of accuracy [38].

3. RESEARCH METHOD

This study was conducted through a simulation of pirated mobile game distribution via the Telegram platform within a controlled testing environment. The overall research design followed a systematic flow: Literature Study, Case Scenario Creation, Hardware and Software Setup, Scenario Simulation,

and the application of the National Institute of Standards and Technology (NIST) framework for forensic analysis.

3.1 Hardware and Software Specifications

To ensure optimal acquisition and analysis, specific hardware and software were utilized. The forensic workstation used was an HP Victus 16 laptop equipped with an AMD Ryzen 7 5600H processor, 16 GB RAM, 512 GB SSD + 1 TB storage, and an Nvidia Geforce RTX 3060 6 GB GPU. The primary object of this research was a rooted Android smartphone, specifically a Samsung Galaxy A04e with 3 GB RAM and 64 GB internal memory, running on Android 14 (One UI 6.1). The software versions strictly employed during the investigation were Telegram version 12.6.4, MOBILedit Forensic Express version 4.1.0.9887, and Magnet AXIOM version 5.4.0.26185.

Figure 3 : Smartphone Digital Evidence

3.2 Research Scenario

The research scenario was designed to represent a real-world illegal content distribution incident and was divided into three primary phases:

1. Pre-Incident

Figure 4 : Pre-Incident Simulation

As shown in Figure 3, he research infrastructure was prepared using the rooted Samsung Galaxy A04e. Crucially, the device was prepared by enabling Developer Mode and USB Debugging to allow forensic tools to communicate with the system securely. The Telegram application was downloaded, installed, and subsequently used to access public channels known for distributing modified application files (APKs).

2. Incident

Figure 5 : Incident Simulation

As shown in Figure 4, This stage involved the simulation of content distribution. The perpetrator (channel administrator) uploaded a pirated mobile game APK file (e.g., minecraft-1-21-130 (1).apk) to a public channel. The research device then functioned as a user who downloaded the link and executed the APK file. This process was intentionally performed to naturally generate digital traces within the system, such as browser history, installation logs, and cache files.

3. Post-Incident

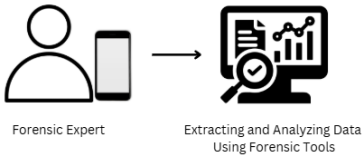

Figure 6 : Post-Incident Simulation

As shown in Figure 5, this phase focused on evidence handling. The device was immediately secured and isolated. The collected data were subsequently acquired and analyzed using the designated forensic software tools to identify the presence of the APK file, user metadata, and distribution flow patterns.

3.3 National Institute of Standards and Technology Framework

The digital investigation was specifically conducted through the four stages of the NIST method, as depicted in Figure 6.

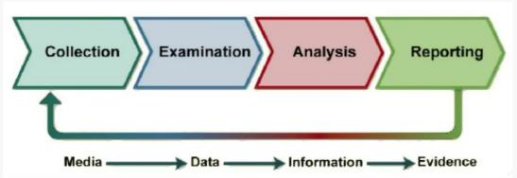

Figure 7 : Stages of the NIST

1. Collection

Digital evidence was acquired and secured from the target device without altering the authenticity of the data. During this stage, the previously enabled USB Debugging proved essential. Magnet AXIOM was utilized for logical acquisition through an Android Debug Bridge (ADB) connection to extract user-level data, including application files and media. In contrast, MOBILedit Forensic Express was employed for full content extraction by directly leveraging the device's root access. This root-level access allowed the tool to bypass standard Android restrictions and acquire comprehensive data from deeper memory partitions and locked system directories.

2. Examination

The raw data obtained from the acquisition process were examined and filtered. The examination focused on the internal Telegram application directory (org.telegram.messenger) to identify installation files with the .apk extension, conversation database records (SQLite), as well as cache files and web links.

3. Analysis

The relationships among the discovered digital artifacts were analyzed. Magnet AXIOM was intensively used to reconstruct the event chronology through timeline analysis, enabling investigators to observe the sequence of activities, including link access, APK downloading, and application execution within the Android system. Cross-validation was performed using MOBILedit to ensure that the application file was recorded as a sideloaded application (an application installed from an unofficial source).

4. Reporting

The final stage involved compiling the forensic findings into a systematic and objective report. This report summarized all relevant digital evidence, including Chat IDs, URL links, channel names, and APK file sizes, as valid references for cybercrime investigation reporting.

4. RESULTS AND DISCUSSION

This section presents the results of the digital forensic investigation conducted on the simulation of pirated mobile game distribution through the Telegram platform. The processes of extraction, analysis, and disclosure of digital evidence from the acquired evidence were systematically performed based on the four stages of the NIST framework, namely Collection, Examination, Analysis, and Reporting.

4.1 Collection

Collection is the initial stage aimed at securing and acquiring digital evidence without altering the authenticity of the data. The primary evidence secured in this study consisted of an Android smartphone device (Samsung Galaxy A04e) that had undergone a rooting process. The rooted condition of the device was crucial, as it enabled forensic investigators to obtain full access to the file system and database directories of the Telegram application.

Figure 8 : Distribution of APK Files Through Telegram Channels

As shown in Figure 7, the device was used to access a public Telegram channel named 'chiyo's sweet land', which was strongly suspected of distributing pirated application files. Preliminary examination of the evidence confirmed the presence of activities involving the distribution of files with the .apk extension, one of which was a file named minecraft-1-21-130 (1).apk. The file was shared through uploads within the channel, allowing it to be directly downloaded by other users. After the identification and initial evidence collection stages were completed, the device was immediately prepared by enabling USB Debugging mode for the data acquisition process using forensic tools.

4.2 Examination

The examination stage aims to systematically acquire and filter data from digital evidence while maintaining the integrity of the original data. In this study, the data extraction process was conducted simultaneously using two forensic software tools, namely Magnet AXIOM and MOBILedit Forensic Express. The use of these two instruments was intended to maximize the acquisition of digital artifacts while also enabling cross-validation of the findings obtained.

The initial acquisition process was performed using Magnet AXIOM through the logical acquisition method via an Android Debug Bridge (ADB) connection. This method extracted logical user data, including application configuration files, media files, and storage archives, which subsequently compiled into a unified raw image file, as illustrated in Figure 8.

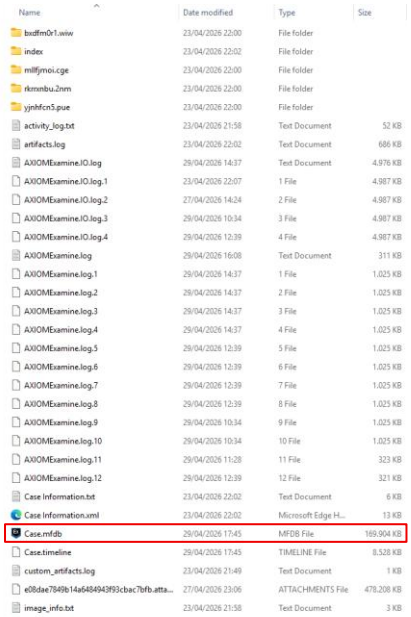

Figure 9 : Magnet AXIOM Acquisition Output in the Storage Directory

The second acquisition process was carried out using MOBILedit Forensic Express through the full content extraction method, which leveraged root access on the target device. Root access was essential because it enabled the forensic software to access the deepest data partitions within Android directories that are locked by default. The extraction results generated by MOBILedit automatically organized the data into structured folders based on categories such as applications, media, and system logs, while also producing report documents in PDF and spreadsheet formats.

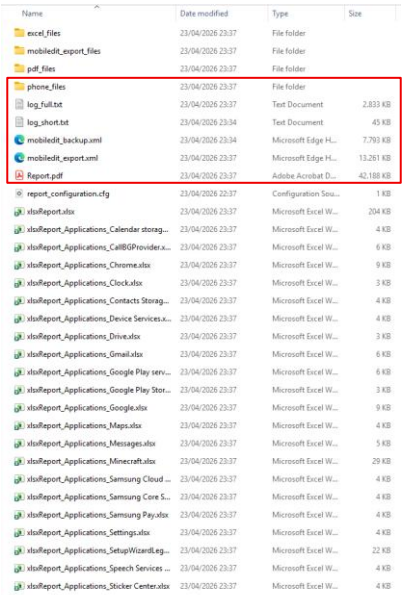

Figure 10 : MOBILedit Acquisition Output in the Storage Directory

As shown in Figure 9, the successful full extraction using both forensic software tools ensured that all raw data were ready to be filtered and evaluated during the analysis stage.

4.3 Analysis

The analysis stage involved the process of identifying and interpreting digital artifacts obtained from the extraction results to reconstruct the traces of pirated mobile game distribution chronologically, based on the cross-validation between Magnet AXIOM and MOBILedit Forensic Express. The initial investigation detected a search for the keyword "Telegram" on the Google Play Store, followed by the installation of the application, which then left browsing history traces directing to a public Telegram channel link: https://t.me/sweetiyland. Analysis of Telegram internal directory structure and database (cache4.db) successfully identified crucial metadata, including communication records associated with Chat ID (-1765428770) for the channel "chiyo's sweet land", as well as the User ID (1403841167). As the culmination of forensic investigation, a 414.9 MB application file named minecraft-1-21-130 (1).apk was discovered stored locally within system path(/storage/emulated/0/Android/data/org.telegram.messenger/files/Telegram/Telegram Files/). The presence of the file within this directory definitively proves that the pirated APK file was obtained directly through download from Telegram application rather than from other source, as seen in Figure 10.

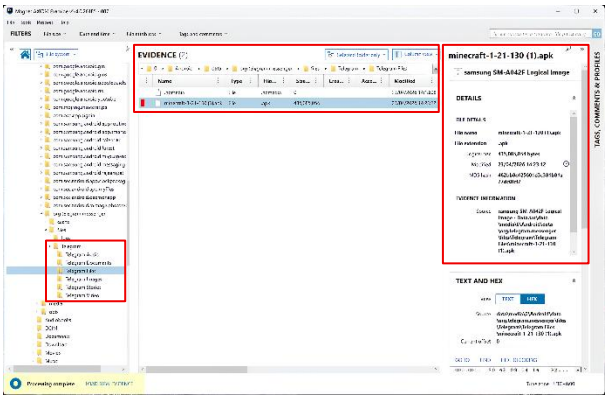

Figure 11 : Discovery of the APK File in the Telegram Files Directory

Evidence of system program execution logs was discovered for the package name com.mojang.minecraftpe. Validation results using MOBILedit confirmed that the application had been installed and recorded as a sideloaded application (an application installed from an unofficial source) through the Package Installer.

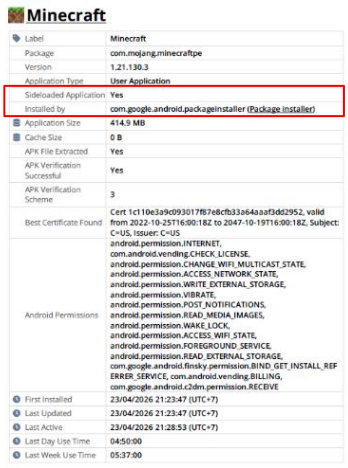

Figure 12 : Minecraft Application Information Based on MOBILedit Analysis Results

As shown in Figure 11, this finding serves as strong evidence that the pirated APK file downloaded from Telegram was not merely stored on the device, but had also been actively executed and run on the target device.

4.4 Report

The reporting stage represents the final process of compiling all digital forensic analysis results into systematic and comprehensive documentation. In this study, the reporting process focused on comparing the extraction results obtained from Magnet AXIOM and MOBILedit Forensic Express, as well as reconstructing the chronology of the pirated mobile game distribution incident on Telegram. The reporting process was conducted objectively to ensure that all identified evidence could be properly documented, validated, and presented as accountable digital forensic findings.

Based on the investigation results, both forensic software tools demonstrated effective cross-validation capabilities by consistently identifying browser access history to the public Telegram channel, extracting user identity metadata, and recovering the primary file minecraft-1-21-130 (1).apk along with its execution logs. The findings also confirmed communication traces, application installation activities, and evidence of APK execution within the Android system, strengthening the reconstruction of the incident chronology. Magnet AXIOM proved effective in organizing communication artifacts and reconstructing digital timelines, while MOBILedit Forensic Express demonstrated strong capabilities in identifying sideloaded applications and performing in-depth extraction through root access. The combined use of both forensic tools provided comprehensive and reliable investigation results. Detailed comparisons of the identified digital evidence are presented in Table 1.

Table 1. Details of Digital Evidence Obtained from the Smartphone Evidence Device

Types of Digital Evidence	Magnet AXIOM	MOBILedit Forensic Express
Link / URL Access	https://t.me/sweetiyland(Found in Chrome Top Sites)	https://t.me/sweetiyland (Found in Web Browsing History)
Initial Search Activity	Search for the keyword "telegram" (Google Play Searches)	Search for the keyword "telegram" (Google Play Store)
Identity & Metadata	User ID: 1403841167 (Ghifari Tristan) Chat ID: -1765428770 (chiyo's sweet land)	Package Name: org.telegram.messenger Version: 12.6.4
Primary File Evidence (APK)	minecraft-1-21-130 (1).apk identified (Logical size: 435,085,054 bytes)	Application com.mojang.minecraftpe identified (Application Size: 414.9 MB)
Execution Evidence (Usage)	Recorded as program execution in system logs	Identified as a sideloaded application via Package Installer
File Size	7.01 GB	9.48 GB
Extraction Duration	03 Minutes 45 Seconds	56 Minutes 40 Seconds

To provide a comprehensive overview of the incident flow, all identified artifacts were reconstructed into a digital activity timeline (chronology). This chronology summarizes the sequence of events, beginning with the search and installation of the Telegram application from the Google Play Store, followed by access to the public channel link, the APK file download process, and finally the execution of the file within the Android system. The detailed chronology of these digital activities is presented in Table 2.

Table 2. Digital Activity Timeline

Time	Application	Activity	Details
23/04/2026 21:17:15	Google Play Store	Search Activity	Search for the keyword "Telegram" on the Google Play Store
23/04/2026 21:17:50	Google Play Store	Installation	Installation of org.telegram .messenger
23/04/2026 21:20:58	Chrome	URL Access	Access to https://t.me/ sweetiyland
23/04/2026 21:23:00	Telegram	File Storage	minecraft-1-21-130 (1).apk
23/04/2026 21:28:53	System	Application Execution	com.mojang .minecraftpe

The reconstructed timeline demonstrates a clear sequence of digital activities, beginning with the installation of Telegram, followed by access to the public channel, the download of the pirated APK file, and ultimately the execution of the application on the Android system. These findings strengthen the validity of the forensic investigation by confirming the complete flow of pirated mobile game distribution activities on the target device.

4.5 Comprehensive Evaluation of Forensic Tools

A comprehensive evaluation of the forensic extraction processes reveals significant operational differences between the utilized tools, which directly impacted the investigation results. As presented in Table 1, Magnet AXIOM completed the extraction significantly faster (3 minutes 45 seconds), yielding 7.01 GB of data. This efficiency is attributed to its logical acquisition approach via an ADB connection, which rapidly extracts user-level data without altering the system structure. In contrast, MOBILedit Forensic Express required a substantially longer duration of 56 minutes and 40 seconds, producing a larger data size of 9.48 GB. This significant discrepancy occurs because MOBILedit performed a full content extraction by leveraging the device's root access, allowing it to bypass default Android restrictions and thoroughly scan deeper, hidden system partitions that are otherwise inaccessible.

Evaluation of their analytical capabilities shows that each tool possesses specific strengths. Magnet AXIOM demonstrated superiority in systematically reconstructing the chronological timeline of digital activities, effectively linking the web browsing history to the Telegram installation and execution logs. Conversely, MOBILedit excelled in identifying the specific system-level status of the extracted APK, successfully tagging it as a 'sideloaded application' installed via the Package Installer. This evaluation strongly indicates that relying on a single forensic tool may leave investigative gaps, particularly in complex instant messaging cases. Therefore, the cross-validation approach employed in this study successfully maximizes evidence recovery and ensures the absolute integrity of the forensic findings.

4.6 Evaluation of Alternative Scenarios

1. Non-Rooted Device Scenario

In the primary dataset, a rooted Samsung Galaxy A04e was utilized, allowing MOBILedit Forensic Express to perform a full content extraction and identify the APK as a 'sideloaded application' from deep system logs. In a non-rooted scenario, forensic tools are restricted to logical acquisition (e.g., via an ADB connection). While Magnet AXIOM can still successfully extract user-level data—such as the cache4.db database and downloaded APK files within the accessible /Telegram Files/ directory—deeper execution logs from the Android Package Installer remain restricted. This indicates that while distribution traces can be found without root access, proving the actual execution of the pirated game becomes significantly more challenging.

2. Secret Chat Distribution Scenario

The primary investigation focused on a Public Channel. If the pirated application dataset were distributed via Telegram's 'Secret Chat' feature, the forensic acquisition would face different obstacles. Telegram implements end-to-end encryption for secret chats and allows messages to be deleted automatically using self-destruct timers. Consequently, the SQLite databases would not permanently retain the chat metadata or file transfer logs, requiring investigators to perform live forensics or acquire the device immediately before the artifacts are wiped by the system.

3. Alternative APK Datasets

The primary dataset analyzed a large modified game file (minecraft-1-21-130 (1).apk, 414.9 MB). However, evaluating the framework against different datasets such as smaller modded utility applications or different game genres demonstrates that the framework's effectiveness remains consistent. Regardless of the APK size or type, Telegram's system architecture will consistently store the downloaded payload in the org.telegram.messenger directory. This proves that the applied NIST framework is adaptable and reliable for various forms of pirated application distributions, not just specific game titles.

5. CONCLUSION

Based on the research results and digital forensic analysis, the investigation into the distribution of pirated mobile games through the Telegram platform was successfully uncovered in a structured manner using the National Institute of Standards and Technology (NIST) framework. The use of Magnet AXIOM and MOBILedit Forensic Express proved effective in providing comprehensive forensic results through a cross-validation approach. The investigation successfully identified and extracted the primary evidence in the form of a pirated APK file (minecraft-1-21-130 (1).apk) stored within Telegram's local storage directory, along with supporting artifacts including URL access history to the public channel (https://t.me/sweetiyland), user identity metadata, and Application Usage system logs. These findings confirmed that the illegal application downloaded from Telegram had not only been stored on the device but had also been executed and

installed as a sideloaded application on the target smartphone. In addition, the reconstruction of digital artifacts successfully demonstrated the complete chronology of activities, beginning from Telegram installation to the execution of the pirated application on the Android system. Despite the successful investigation, this study has several limitations that may be addressed in future research, including the need for forensic investigations on iOS-based devices, comparative evaluations using other industry-standard forensic tools such as Autopsy, Cellebrite UFED, and Oxygen Forensic Detective, as well as the implementation of Malware Analysis to detect potentially embedded malicious code such as spyware or backdoors within pirated APK files.

6. REFERENCES

[1] Rizky Febriansyah, "Dampak Kemajuan Teknologi Informasi dan Komunikasi terhadap Nilai-Nilai Budaya," Venus: Jurnal Publikasi Rumpun Ilmu Teknik , vol. 3, no. 1, pp. 01–10, Jan. 2025, doi: 10.61132/venus.v3i1.687.

[2] H. T. W. Visa and M. T. Multazam, "Legal Obligations of Telegram Users Regarding Copyrighted Content Distribution in Public Groups," Indonesian Journal of Law and Economics Review, vol. 19, no. 2, May 2024, doi: 10.21070/ijler.v19i2.1011.

[3] S. S. Roy, E. P. Vafa, K. Khanmohammadi, and S. Nilizadeh, "DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram," arXiv preprint, Sep. 2024.

[4] M. Elizabeth Sutrahitu, S. Selfina Kuahaty, and A. Balik, "Perlindungan Hukum Pemegang Hak Cipta terhadap Pelanggaran Melalui Aplikasi Telegram," TATOHI: Jurnal Ilmu Hukum, vol. 10, no. 5, pp. 346–355, 2021, doi: 10.47268/tatohi.v1i4.611.

[5] D. Mutiara Syafitri and F. Fachri, "Analisis Forensik Digital Telegram Pada Android Untuk Cybercrime Dengan Kerangka Nasional Institute Of Standard Technology (NIST)," Rabit : Jurnal Teknologi dan Sistem Informasi Univrab, vol. 10, no. 1, pp. 41–50, Jan. 2025, doi: 10.36341/rabit.v10i1.5402.

[6] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," Jurnal Telekomunikasi dan Komputer, vol. 9, no. 3, p. 186, Jan. 2020, doi: 10.22441/incomtech.v9i3.7210.

[7] T. Ruslan, I. Riadi, and S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," JURNAL FASILKOM, vol. 13, no. 02, pp. 286–292, Aug. 2023, doi: 10.37859/jf.v13i02.5540.

[8] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 4, no. 5, pp. 820–828, Oct. 2020, doi: 10.29207/resti.v4i5.2224.

[9] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," REPOSITOR, vol. 2, no. 10, pp. 1400–1405, 2020.

[10] M. Prasetio, U. A. Dahlan, and I. Riadi, "Investigation Telegram based-on Web using National Institute of Standards and Technology Method," 2022.

[11] W. O. Rini, T. D. Hariyana, and I. Makhali, "Pengunggahan Ulang Video Perfilman Indonesia Secara Ilegal Melalui Public Channel Telegram," Yustitiabelen, vol. 8, no. 2, pp. 118–142, Aug. 2022, doi: 10.36563/yustitiabelen.v8i2.495.

[12] N. A. I. Maniar and T. Yuniati, "Implementasi Mobile Forensic Pada Aplikasi MiChat Dan Telegram Dengam Framework NIST 800-101," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 60–65, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3764.

[13] I. Riadi, H. Herman, and N. H. Siregar, "Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode NIST," JOINTECS (Journal of Information Technology and Computer Science), vol. 6, no. 3, p. 137, Sep. 2021, doi: 10.31328/jointecs.v6i3.2591.

[14] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode NIST," Cyber Security dan Forensik Digital, vol. 4, no. 1, pp. 49–57, Jun. 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[15] D. Hariyadi, M. W. Indriyanto, and M. Habibi, "Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine," Cyber Security dan Forensik Digital, vol. 3, no. 2, pp. 34–38, Dec. 2020, doi: 10.14421/csecurity.2020.3.2.2193.

[16] N. Citra Dewi, T. Sutabri, and F. Putrawansyah, "ANALISIS PENYADAPAN PADA TELEGRAM DENGAN NETWORK FORENSIC," JIKO (Jurnal Informatika dan Komputer), vol. 7, no. 2, p. 183, Sep. 2023, doi: 10.26798/jiko.v7i2.789.

[17] Y. Sri Maharani, S. Trisdiatin, M. Rafli Ihsanuddin, and F. Rahma, "Kekuatan Enkripsi End-to-End: Kajian Literatur Mengenai Kerahasiaan Komunikasi Digital dalam Aplikasi Pesan Instan," SEMIOTIKA: Seminar Nasional Teknologi Informasi dan Matematika, vol. 2, pp. 1–7, 2023.

[18] I. Safira, E. Lubis, and F. Fauziah, "Copy Right Protection For Netflix Streaming Video Circulated In Telegram," Jurnal Hukum Jurisdictie, vol. 4, no. 1, pp. 80–88, Aug. 2022, doi: 10.34005/jhj.v4i1.84.

[19] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review," Jun. 01, 2024, Elsevier B.V. doi: 10.1016/j.teler.2024.100130.

[20] Md Fahim Ahammed, "Clone detection to prevent software piracy in android play store," GSC Advanced Research and Reviews, vol. 21, no. 3, pp. 108–131, Dec. 2024, doi: 10.30574/gscarr.2024.21.3.0487.

[21] M. I. Zulfa, S. Tena, and S. D. Rizkiono, "Aktivitas Sniffing pada Malware Pencuri Uang di Smartphone Android," RENATA: Jurnal Pengabdian Masyarakat Kita Semua, vol. 1, no. 1, pp. 7–10, Apr. 2023, doi: 10.61124/1.renata.4.

[22] G. Setya Agung and T. Yuniati, "Analisis Malware Trojan Dalam File Undangan Pernikahan.Apk Pada Smartphone Android Dengan Metode Hybrid Analysis," eProceedings of Engineering, vol. 12, no. 2, p. 3312, 2025.

[23] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," Jurnal Pengabdian Masyarakat dan Penerapan Ilmu Pengetahuan, vol. 3, no. 2, pp. 1–6, Nov. 2022, doi: 10.25299/jpmpip.2022.11003.

[24] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media SosialDigital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," Techno.Com, vol. 20, no. 4, pp. 527–539, Nov. 2021, doi: 10.33633/tc.v20i4.5170.

[25] Program Studi Informatika, "Tahapan Digital Forensik secara umum," Universitas Ahmad Dahlan. Accessed: Jun. 30, 2025. [Online]. Available: https://tif.uad.ac.id/tahapan-digital-forensik-secara-umum/

[26] A. I. Yuladi and R. Indrayani, "Analisis dan Perbandingan Tools Forensik menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber," Jurnal Teknologi Terpadu, vol. 9, no. 2, pp. 95–100, Dec. 2023, doi: 10.54914/jtt.v9i2.636.

[27] R. P. Prambudi, Imam Riadi, and Murinto, "Analisis Forensik Mobile pada Aplikasi E-Commerce Menggunakan Metode Association of Chief Police Officers," Cyber Security dan Forensik Digital, vol. 8, no. 1, pp. 44–52, Jun. 2025, doi: 10.14421/csecurity.2025.8.1.5234.

[28] I. W. Putra, A. Suharso, and C. Rozikin, "Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA," Jurnal Sains Komputer & Informatika (J-SAKTI), vol. 5, pp. 712–726, 2021, Accessed: Jun. 29, 2025. [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/370

[29] C. Mustafa, "Integritas Chain Of Custody Pada Pemeriksaan Bukti Digital," Judex Laguens, vol. 2, no. 1, pp. 75–96, Mar. 2024, doi: 10.25216/ikahi.2.1.4.2024.75-96.

[30] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)," Cyber Security dan Forensik Digital, vol. 7, no. 1, pp. 18–24, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[31] 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," Jurnal Sistem Informasi Galuh, vol. 2, no. 1, pp. 44–54, Jan. 2024, doi: 10.25157/jsig.v2i1.3695.

[32] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," IT Journal Research and Development, vol. 5, no. 2, pp. 171–182, Nov. 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[33] H. Supardin, R. Satra, Muh. A. Asis, and M. F. Teng, "Comparison Analysis of Digital Forensic Tools on Instagram Messenger using The National Institute of Standards and Technology (NIST) Method," Bulletin of Social Informatics Theory and Application, vol. 6, no. 1, pp. 65–75, Mar. 2022, doi: 10.31763/businta.v6i1.534.

[34] K. Khairunnisak, H. Ashari, and A. P. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST," Jurnal RESISTOR (Rekayasa Sistem Komputer), vol. 3, no. 2, pp. 72–81, Nov. 2020, doi: 10.31598/jurnalresistor.v3i2.634.

[35] Elsya indah Fitria, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video," Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI), vol. 2, no. 2, pp. 390–399, Sep. 2023, doi: 10.62712/juktisi.v2i2.108.

[36] N. Hamid, J. Kuswanto, D. Nurani, A. Dwi Putra, F. Mahananing Puri, and S. Tri Atmaja Ramadhani, "Forensic Recovery Techniques on Android Devices with the National Institute of Standards and Technology (NIST) Approach," JTECS : Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem dan Komputer, vol. 4, no. 1, p. 53, Jan. 2024, doi: 10.32503/jtecs.v4i1.4676.

[37] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 21, no. 3, pp. 489–502, Jul. 2022, doi: 10.30812/matrik.v21i3.1620.

[38] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," Jurnal Edukasi dan Penelitian Informatika (JEPIN), vol. 7, no. 3, p. 322, Dec. 2021, doi: 10.26418/jp.v7i3.48805.