JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 7 No. 4 Desember 2025
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v7i4.9988/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

The Power of Screenshot Evidence in Proving Cyber Crimes

Vira Auliya Juliharto
Jurusan Ilmu Hukum, Fakultas Hukum, Universitas Negeri Gorontalo

Article Info
Article history:
Accepted: 13 December 2025
Publish: 27 December 2025

Keywords:
Screenshot;
Electronic Evidence;
Digital Authentication;
Digital Forensics;
Cybercrime.

Abstract
This research analyzes the strength of screenshot evidence in proving cybercrime by combining a normative juridical approach with empirical analysis of investigative practices and court decisions. The findings indicate that screenshots hold significant probative value, although their validity strongly depends on digital authentication, data integrity, and forensic support. Screenshots cannot stand alone and require technical verification through metadata examination, hash value analysis, and digital reconstruction. The study also highlights that Indonesia lacks uniform standards for handling electronic evidence, which affects the quality of proof in court. The analysis demonstrates the urgency of updating national guidelines and improving the technical capacity of law enforcement to ensure the reliability of electronic evidence. Overall, this research emphasizes the importance of proper technical and normative procedures in ensuring the legal strength of screenshot evidence in cybercrime cases.

This is an open access article under the Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional

Corresponding Author:
Vira Auliya Juliharto
Universitas Negeri Gorontalo
Email: vrjuliharto@gmail.com

1. INTRODUCTION

The development of information technology has significantly transformed the social, economic, and legal landscape, particularly in the context of the increasing number of cybercrime cases in Indonesia. Massive digitalization has made people's activities dependent on electronic devices and digital platforms, thus opening up opportunities for computer-based crimes such as online fraud, defamation through social media, hacking, and the unauthorized dissemination of personal data. This situation demands updates to legal instruments, both normative and procedural, particularly regarding the aspect of evidence in the criminal justice system. The Criminal Procedure Code (KUHAP), which was drafted when digital technology was still underdeveloped, now faces new challenges in accommodating electronic evidence. One form of electronic evidence most frequently presented in court is screenshots, as they are considered to be able to quickly and easily record digital interactions. However, their acceptance is challenging, as they must meet the requirements of authenticity, integrity, and reliability to be considered valid evidence.

In Indonesia, the normative recognition of electronic evidence has been strengthened through the Electronic Information and Transactions Law and its amendments. Legally, electronic information and electronic documents, including printouts, have the same legal force as conventional documents. However, judicial practice varies regarding the assessment of screenshot evidence. Some judges accept it as documentary evidence, while others consider it indicative evidence requiring support from other evidence. This diversity of practice stems

from fundamental questions about the authenticity and integrity of screenshots, particularly as technology allows for image manipulation without leaving a visual trace. Without digital forensic support, screenshots are often deemed insufficient to prove the perpetrator's involvement or to prove that the data actually originated from a specific device. This issue is further complicated by the lack of national technical guidelines outlining standard procedures for collecting, storing, and verifying electronic evidence in the form of screenshots (Permana et al., 2021).

Academic studies show that the probative strength of electronic evidence, including screenshots, depends heavily on the investigator's ability to ensure the chain of custody of the evidence in accordance with the chain of custody principle. This chain of custody is crucial for proving that evidence remains unchanged from the time it is first obtained until it is presented in court. Without adequate documentation regarding the device used, the time of capture, or the storage process, judges tend to deem the evidence weak. On the other hand, digital forensic analysis that can examine metadata, hash values, and data sources can increase the credibility of screenshots as evidence. Furthermore, the role of digital forensic experts is crucial in providing technical explanations that investigators or prosecutors cannot explain in court. Thus, the presence of experts is a supporting element that strengthens the probative value of electronic evidence (Hasnawati et al., 2023).

The purpose of this study is to analyze the strength of screenshot evidence in proving cybercrimes by examining normative aspects, investigative practices, and the patterns of judges' considerations in court decisions. This study combines a normative juridical approach and empirical analysis of court decisions that use screenshots as evidence. With this approach, the study is expected to comprehensively explain the position of screenshots in the Indonesian criminal evidence system, the challenges faced by law enforcement officials, and opportunities for strengthening regulations. Furthermore, this study also seeks to address the gap between normative regulations and the reality of practice in the field. Legal reform is needed so that electronic evidence is not only recognized but also can be operationalized appropriately in a justice system that upholds the principle of fair trial.

Technically, the use of screenshots as evidence faces several challenges that cannot be ignored in the process of proving cybercrime. One fundamental issue is the high potential for manipulation of visual content, which can be easily done using various image editing applications, thus raising doubts about the evidence's authenticity. Screenshots essentially only record the visual appearance, not the accompanying raw data, making them vulnerable to alteration without leaving a clear digital footprint. Therefore, the authentication process is crucial to ensure that the submitted evidence accurately reflects the conditions at the time of the incident. This technical challenge is further compounded by the fact that not all digital platforms automatically record or display metadata, making crucial information such as the time, location, and device used often unverifiable. When evidence loses its digital context, the screenshot's probative value is significantly reduced.

Furthermore, evidence collection practices by investigators or reporters often do not follow standard procedures for securing electronic evidence, increasing the risk of damage or doubting the integrity of the data. Many reporters simply take screenshots with personal devices without recording the time, ensuring the system settings are in standard condition, or saving the files on secure storage media. This creates a disconnect between visual evidence and the supporting data that should accompany it. In many cases, submitted screenshots are simply printouts or re-photographs of the device's screen, further diminishing the possibility

of assessing the evidence's authenticity through digital examination. Investigators who lack a thorough understanding of chain of custody procedures also often fail to document the stages of evidence collection, storage, and processing. Yet, even small changes in these processes can affect the judge's assessment of the evidence's integrity. These procedural weaknesses are a major cause of the significant amount of digital evidence not receiving maximum evidentiary weight in court.

Another challenge relates to the limited infrastructure and technical competence of law enforcement agencies in conducting comprehensive digital forensic examinations. Not all police or prosecutorial units have digital forensic laboratories capable of conducting in-depth analysis of metadata, hash values, or digital reconstructions of the devices involved. As a result, the evidentiary process often relies solely on visual assessments, rather than comprehensive technical analysis. In some cases, investigators must send devices or data to a central forensic laboratory, slowing the investigation process and opening up the potential for undetected changes during the transfer of evidence. This uneven forensic capacity creates disparities in the quality of evidence between regions, which can ultimately influence judges' judgments when issuing verdicts. Under these conditions, the technical challenges in using screenshots not only affect the strength of evidence but also have implications for substantive justice in handling cybercrime in Indonesia (Santoso, 2024).

An analysis of several court decisions shows that judges tend to exercise a high degree of caution when assessing the probative value of screenshots as electronic evidence. This caution arises because screenshots are considered the most vulnerable to manipulation, whether through simple editing or more complex digital manipulation. In several cases, judges explicitly rejected the use of screenshots because they lacked digital forensic verification capable of ensuring their integrity and authenticity. When there is no technical explanation that can guarantee the data has not been altered, the evidence is deemed to fail to meet the authentication standards required by procedural law. These findings suggest that without the support of additional evidentiary mechanisms, screenshots are viewed as weak and inadequate evidence to form the basis for a judge's conviction.

However, some decisions indicate that screenshots are admissible and have probative weight as long as they are accompanied by other relevant evidence. Judges in several cases deemed such evidence valid when supported by witness testimony, digital traces of social media accounts, the results of digital forensic expert examinations, or confirmation of access through specific electronic devices. This combination approach aligns with the normative nature of electronic evidence, which does not stand alone but must be tested in conjunction with other supporting evidence. This pattern demonstrates that judges do not reject screenshots outright, but rather position them as supporting data that serves to clarify the sequence of events or corroborate other evidence. In certain cases, the presence of screenshots can provide important chronological context, for example, in cases involving digital communication between the perpetrator and the victim.

In addition to the completeness of the evidence, the context of the case also significantly influences how judges assess the evidentiary strength of screenshots. In cases of defamation, online fraud, or the distribution of illegal content, screenshots often serve as an initial representation of the disputed actions. This evidence can show conversations, commands, or posts that are the subject of the case, thus having strategic value in establishing a logical sequence of events. Nevertheless, the aspect of authentication remains the primary focus in determining whether a screenshot is admissible. Judges will generally evaluate the data source,

the device used, the consistency of the digital footprint, and the possibility of manipulation. Therefore, while screenshots have the potential to assist in the evidentiary process, their strength depends heavily on their technical integrity and the support of other evidence that makes them legally credible (Sanjaya et al., 2022).

A systemic challenge facing law enforcement officials is the lack of national standards regarding procedures for collecting and verifying electronic evidence, particularly screenshots. To date, technical guidelines for managing electronic evidence remain sectoral and not yet fully integrated. National standards are needed to ensure the quality of evidence and avoid differences in local practices. Furthermore, the lack of technical training and supporting facilities within the police force means that the evidentiary process relies on the creativity of investigators or the initiative of the complainant. At the judicial level, judges also need capacity building to better understand the technical aspects of electronic evidence. Without technical competence, there is the potential for misinterpretation that can influence decisions and impact justice for the parties (Marzuki et al., 2025).

This research's contribution lies in its comprehensive normative-empirical analysis of the strength of screenshot evidence. It also identifies an urgent need to update technical guidelines for handling electronic evidence in Indonesia. Furthermore, it provides recommendations that can be used by law enforcement officials, academics, and policymakers to improve the quality of evidence in cybercrime cases. Clear, comprehensive, and standardized guidelines will significantly assist judges in objectively assessing electronic evidence. At the same time, investigators and prosecutors can work more effectively in collecting and presenting evidence that meets formal and material requirements. Thus, screenshots can serve as reliable evidence in the Indonesian criminal justice system.

The overall discussion in this introduction confirms that analyzing the strength of screenshot evidence in proving cybercrimes is a crucial issue that requires further in-depth study. This research stems from the urgent need for an evidentiary system that adapts to technological developments and is capable of addressing the challenges of digital evidence authentication. In a modern society dependent on electronic devices, the existence of digital evidence is unavoidable and will become increasingly dominant in the judicial process. Therefore, this research aims to bridge the practical needs of law enforcement officials with the legal need to establish evidentiary standards that guarantee justice, legal certainty, and the protection of the rights of the parties to a case.

2. RESEARCH METHODS

The research method used in this study is a normative juridical approach combined with limited empirical analysis to understand the strength of screenshot evidence in proving cybercrimes. The normative juridical approach is used to examine relevant laws and regulations, such as the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law and its amendments, and technical regulations regarding electronic evidence. The analysis also focuses on court decisions that consider screenshots as evidence, thus providing an overview of judges' consideration patterns regarding the authenticity, integrity, and probative value of digital evidence. Meanwhile, empirical elements are obtained through tracing investigative practices and procedures for managing electronic evidence, including aspects of the chain of custody, data collection techniques, and the role of digital forensics in supporting the authentication process. The combination of these two approaches allows the study to provide a comprehensive overview of the gap between normative

regulations and field practice, and produces relevant analysis regarding the need to improve evidentiary mechanisms in cybercrimes.

3. RESEARCH RESULTS AND DISCUSSION

3.1.Research result

The research findings indicate that screenshots have significant evidentiary value in cybercrime cases, although their formal strength is highly dependent on digital authentication and integrity. Field findings indicate that law enforcement officials generally accept screenshots as supporting evidence, but have not yet considered them primary evidence due to the perceived high potential for modification. Analysis of several decisions shows that judges place more credence on screenshots when accompanied by metadata, server logs, and testimony from digital forensic experts who can confirm the file's authenticity. Interview data with investigators indicates that procedures for securing electronic evidence do not always meet chain of custody standards, particularly in cases handled at the regional level, thus reducing its evidentiary value. From the victim's perspective, most reporters submit evidence in the form of screenshots without the original file or a complete digital copy, complicating the verification process and hindering the digital evidence collection process.

The study also found that systematic integration of digital forensic procedures can increase the evidentiary weight of screenshots in a case. When screenshots are obtained directly from the device and verified using hashing techniques, network data matching, and temporal examination, they have been shown to strengthen the construction of evidence and help judges more clearly describe the sequence of events. Furthermore, investigators who participated in cyber evidence handling training demonstrated better evidence handling quality than investigators without special training. The analysis also shows that the use of screenshots is becoming increasingly crucial in cases of insults, threats, defamation, and online fraud, as visual evidence facilitates the interpretation of actions. Overall, this study confirms that screenshots have strategic evidentiary power, but their effectiveness is largely determined by consistently applied forensic collection, verification, and analysis procedures.

3.2.Discussion

Normative Validity of Screenshot Evidence

Screenshots are one of the most frequently used forms of electronic data in cybercrimes due to their ease of production, storage, and sharing. However, their normative validity as evidence is often debated, particularly regarding the requirements for authenticity and integrity as stipulated in laws and regulations. In the context of evidence, screenshots are considered valid as long as their connection to the electronic system from which the data originates can be proven. The challenge lies in the potential for visual manipulation through image editing applications, which often results in such evidence being used as preliminary evidence, rather than stand-alone evidence. Therefore, the legal legitimacy of screenshots relies heavily on supporting metadata, system logs, and the presence of forensic tools that ensure even the slightest changes can be detected. This is where the concept of normative validity plays a crucial role as a legal standard for determining the admissibility of screenshots in court (Aisyah et al., 2022).

In judicial practice, screenshots are generally presented as preliminary evidence, providing an initial overview of a digital event before verification through more technical and measurable electronic evidence. Judges do not readily accept screenshots as stand-

alone evidence due to their easily modified nature, often questioning their reliability. Therefore, courts assess the evidentiary strength of screenshots primarily based on the process by which they were obtained—whether the process was legal, procedural, and did not violate privacy or other applicable legal provisions. The assessment also includes whether the chain of custody of the evidence is fully documented, from collection and storage to presentation in court. Documenting this chain of custody is crucial to ensuring that the evidence remains unaltered and that its integrity.

Furthermore, courts give greater evidentiary weight to screenshots when supported by digital forensic expert examination. Forensic experts ensure that the displayed data reflects authentic digital activity without manipulation. The authentication process typically includes hash value analysis to identify whether files have been altered, metadata examination to trace creation and modification times, and file origin tracing through the device used. When these technical aspects are met, screenshots are considered reliable enough to be used as part of a valid evidentiary structure. Conversely, without forensic support, screenshots pose legal risks because they are vulnerable to challenge by opposing parties, especially in cases that require high accuracy.

The urgency of strengthening evidentiary methodologies through electronic evidence is growing as the complexity of cybercrime in Indonesia increases. The increasingly varied modes of crime, ranging from online fraud and digital extortion, conversation manipulation to the distribution of illegal content, require courts to adopt stricter and more systematic standards for evaluating evidence. In this context, screenshots retain strategic value as an initial representation of an incident, but they can only function optimally if tested through an objective and scientifically accountable forensic approach. Therefore, the quality of evidence depends not only on the form of the evidence itself, but also on the accuracy of the technical and legal procedures that accompany its presentation in court (Julian & Sutabri, 2023).

In addition to normative validity, the judge's interpretation also plays a role in assessing the strength of screenshot evidence. Judges often focus their evidentiary analysis on the consistency between the investigator's narrative, witness testimony, and supporting digital evidence. If a screenshot only shows partial information without context, its value is limited. Therefore, investigators must present comprehensive evidence that demonstrates not only the visuals but also the structural relationships between messages, accounts, platforms, and the devices that process them. This aligns to prove evidence in cybercrimes, namely ensuring that electronic evidence is not only legally valid but also provides material certainty regarding the criminal event.

Digital Authentication and Proof of Authenticity

Authentication is a key element in determining whether a screenshot has evidentiary value. The authentication process ensures that the screenshot originates from a legitimate electronic system, without any alterations after it has been acquired. In an investigative context, authentication faces significant challenges because screenshots are merely visual representations without the integral data of the original file, such as complete metadata and a digital footprint. Therefore, forensic examinations must involve direct tracing of the source device or server to match information between the visual and the raw data. Without device authentication, screenshots can potentially be considered mere illustrations without strong probative value (Khairunnisak, 2023).

Authentication issues become even more complex when cases involve instant messaging apps that use end-to-end encryption, such as WhatsApp, Telegram, and Signal. While this encryption technology is designed to protect user privacy, it presents new challenges for law enforcement in ensuring the authenticity of conversations submitted as evidence. Screenshots are often used as initial evidence, but courts cannot accept such evidence without thorough verification. Examiners must ensure that the conversations actually occurred within the account of the person involved, and not the result of fabrication or falsification of the app's interface. This is crucial because the ease of editing visuals in digital conversations allows anyone to create fake dialogue that appears authentic. Therefore, authentication focuses not only on the visual appearance but also requires examining the data source, the device used, and the overall context of the conversation.

One of the most reliable approaches to maintaining data integrity is digital forensic imaging, a process of bit-for-bit duplication of a device suspected of being a source of evidence. This technique forensically copies all the original data on the device without altering its internal structure, allowing experts to conduct in-depth examinations without the risk of evidence contamination. This process allows investigators to explore various elements not visible in screenshots, such as metadata, file systems, digital artifacts, and activity traces stored on the device. This includes login history, application changes, automatic backups, and communication patterns that can confirm whether the conversation depicted in the screenshot actually occurred. Digital forensic imaging provides stronger evidence than relying solely on visuals of conversations because it provides a technical basis that can be tested and justified in court. This method also ensures that the evidence meets the principles of forensic soundness, namely that the evidence remains intact, replicable, and free from interference.

The next, equally important step is checking the hash, timestamp, and activity logs as part of the authentication process. The hash value is used to prove that the data has not been altered since it was first secured, while the timestamp helps verify the exact time of the incident. The activity log provides a comprehensive overview of actions taken on the device, including conversations, deleted messages, network usage, and data synchronization. When all these technical procedures are carried out correctly, screenshots can be substantiated as valid evidence and have sufficient probative value in court. However, judges still view screenshots as complementary evidence that requires support from other digital evidence and expert testimony. In other words, the validity of a screenshot rests not only on its appearance but also on the entire authentication chain, which ensures its integrity, authenticity, and relevance to the criminal event being examined (Yudhana, 2022).

In addition to technical challenges, authentication also faces issues of investigator competence. Many law enforcement officers lack adequate digital forensic skills to professionally assess the authenticity of evidence. As a result, evidentiary procedures often rely on textual interpretation rather than on in-depth technical analysis. This situation demands increased capacity through intensive training in digital forensics and the provision of more advanced analytical tools. Therefore, authentication should not only be a technical process but also part of a law enforcement policy that adapts to developments in digital technology.

The Role of Digital Forensics in Evidence

Digital forensics plays a strategic role in enhancing the evidentiary value of screenshots. When screenshots are submitted as evidence, forensic experts are tasked with ensuring that they originate from legitimate devices, maintain their integrity, and have not been manipulated. Examination typically includes metadata analysis, recovery of original files, and reconstruction of digital activity related to the crime. Techniques such as NIST SP 800-86 are essential standards used in the investigative process to ensure that every step of evidence collection is scientifically and legally justifiable. Through these procedures, the probative value of screenshots is significantly increased (Dasmen et al., 2024).

Furthermore, digital forensics plays a strategic role in providing a comprehensive context to visual evidence presented through screenshots. Generally, visual evidence only shows the surface of a digital interaction without providing in-depth information about how that data is generated, transformed, or transmitted across specific devices and networks. Screenshots do not include information about the communication paths, system settings, or backend processes underlying the digital activity. Therefore, without forensic analysis, visual evidence represents only a small part of the overall sequence of digital events. Digital forensics then functions to uncover hidden layers of data, so that each piece of information displayed in the screenshot can be connected to the actual data structure occurring on the device or application being used.

Through deeper forensic techniques, investigators can examine digital artifacts such as IP addresses, login times, device time zones, data change history, and system activity records that are not visible in screenshots. This information has significant evidentiary value because it helps identify the user accessing the application, the device used, and the exact time of the conversation or activity. Furthermore, communication patterns detected through system logs can indicate the frequency, duration, or sequence of related messages, strengthening the link between the perpetrator and their digital activity. In some cases, analyzing message metadata can even allow investigators to identify indications of manipulation, such as deleting messages, moving files, or altering timestamps. This is crucial because visual evidence can be retrieved after the original data has been tampered with, requiring technical examination to confirm its validity.

Additional data obtained from digital forensics provides a stronger causal link in proving the perpetrator's actions. This information means that screenshots are no longer viewed as stand-alone evidence, but as an integral part of a complementary chain of electronic evidence. With more comprehensive evidence, the court can understand not only what is visible on the screen but also the technical context behind it, indicating how, when, and by whom the digital communication was created or forwarded. The comprehensive presentation of electronic evidence increases the reliability of the evidence, reduces the judge's doubts about potential visual manipulation, and ensures that the law enforcement process adheres to the principles of data authentication and integrity. Thus, digital forensics plays a crucial role in strengthening the validity of screenshot evidence in court, particularly in increasingly complex and dynamic cyber cases (Gemilang, 2024).

Recent developments show that forensic tools like Autopsy, FTK, and Cellebrite are capable of extracting data not visible in screenshots, such as temporary files or deleted messages. This allows for a more detailed reconstruction of events and proves whether a conversation actually occurred or was staged. Thus, digital forensics serves as a key

support for the evidentiary value of screenshots, making them more credible in the eyes of judges. This combination of visual and technical data helps provide a comprehensive picture of the cybercrime being examined and strengthens the judge's confidence in the evidence.

Legal Status of Screenshots

Normatively, electronic evidence, including screenshots, has legal standing in Indonesian criminal procedure law. The Electronic Information and Transactions Law expand the definition of evidence beyond conventional evidence, such as witnesses and letters. However, it should be noted that not all forms of digital evidence have the same degree of validity. Screenshots are often viewed as secondary evidence due to their easily modified nature. Therefore, such evidence must be supported by additional evidence sourced directly from electronic systems to strengthen its relevance and accuracy (Asaad, 2023).

In the modern criminal procedure paradigm, the status of electronic evidence, including screenshots, is regulated within the framework of independent judgment granted to judges. This freedom is not unlimited, but is guided by the principle of freedom and responsibility, a principle that requires judges to link every decision to legal arguments that can be rationally and legally justified. In this context, screenshots as visual evidence is treated as part of electronic evidence that must be tested not only in terms of the substance of the information, but also the process of its formation. Judges cannot accept screenshots solely based on their appearance, as such evidence is highly susceptible to digital manipulation and engineering. The judge's assessment must consider the technical, legal, and procedural aspects surrounding the evidence, so that its validity and integrity can be assessed comprehensively.

A judge's assessment of the evidentiary strength of screenshots depends largely on the extent to which the acquisition process complies with legitimate investigative operational standards. These standards include complete documentation of the time of capture, the device used, who took the screenshot, and how the evidence was secured until it was presented in court. If these steps are carried out correctly, screenshots can gain a stronger standing as evidence, as the judge can assess that the chain of custody of the evidence was properly maintained. Conversely, if there are inconsistencies in security measures, such as the lack of initial recording or the evidence not being forensically tested, the judge is likely to doubt its authenticity. Therefore, the evidence collection process must be carried out by investigators in accordance with legal procedures, so that screenshots are not merely static images, but digital documents protected from potential modification.

This context demonstrates that screenshots are not merely a technical issue, but also concern compliance with investigative administrative procedures and the clarity of the underlying data sources. The integrity of evidence is largely determined by the extent to which investigators apply accountability principles in the process of obtaining digital evidence. The court will ultimately examine whether the evidence directly relates to the case under investigation and whether it demonstrates verifiable relevance and authenticity. If all these requirements are met, screenshots can be positioned as an effective evidentiary tool in criminal cases, particularly in cases involving digital activity as the core of the unlawful act. Therefore, the judge's assessment of screenshot evidence reflects a balance

between technological developments and the fundamental principles of criminal procedural law, which uphold justice, certainty, and expediency. (Putra, 2022).

The legal status of screenshots is also influenced by developments in jurisprudence. Several decisions indicate that courts are beginning to accept screenshots as important evidence, particularly in cases of defamation, online fraud, and threats via social media. This demonstrates the judicial system's adaptation to developments in digital technology. However, strengthening technical regulations regarding evidence authentication is still necessary to avoid legal uncertainty. Drafting more comprehensive electronic evidence guidelines is urgently needed to support the consistency of court decisions.

Standards of Evidence and Prevention of Manipulation

The risk of manipulation is the biggest weakness in using screenshots as evidence. Various image editing applications allow visual changes without leaving visible traces. Therefore, evidentiary standards must strictly regulate how screenshots are obtained, examined, and presented as evidence. Strengthening these standards can be achieved through the implementation of hash values from the seizure stage, recording the chain of custody of evidence, and cross-verification using forensic tools. This aims to ensure that the evidence presented in court is authentic, not fabricated (Anonymous, 2025).

In addition to technical standards governing the digital evidence authentication process, strengthening institutional capacity is a fundamental aspect that cannot be ignored in a modern evidence system. Many cases demonstrate that investigators, especially at the regional level, lack adequate equipment to verify the authenticity of electronic evidence, including screenshots. Limited digital forensic laboratory equipment, such as hash verification software, forensic imaging devices, and electronic evidence management systems, often results in suboptimal digital evidence examination. This situation has direct implications for the quality of evidence, as evidence not examined with standard equipment risks being deemed unauthenticated by judges. Therefore, upgrading equipment and institutional investment in digital forensics is a strategic step that must be undertaken continuously.

In addition to equipment, the presence of competent law enforcement officers plays a crucial role in ensuring that the identification, examination, and storage of digital evidence are carried out according to standards. A sound evidence system cannot simply rely on regulations but must be supported by human resources who understand the dynamics of information technology developments. Many obstacles to evidence arise not because the evidence itself is invalid, but because the method of collection does not follow procedures. For example, screenshots are taken without recording metadata, not using authorized devices, or stored without documenting the chain of custody. If investigators have basic knowledge of digital forensics, these procedural errors can be minimized. This demonstrates that the technical competence of officers is a crucial element in maintaining the integrity of evidence and the credibility of the investigative process.

Therefore, digital forensics training needs to be expanded so that each investigative unit is capable of independently conducting initial examinations of electronic evidence. This training should cover not only technical aspects such as the use of verification tools, metadata analysis, or digital imaging, but also an understanding of administrative obligations, chain of evidence accountability, and the ethics of digital data handling. With strong human resources, the investigation process will no longer be entirely dependent on external experts, allowing for faster, more efficient, and more accurate case handling. This

capacity building will strengthen the legitimacy of evidence presented in court and ensure that law enforcement in the field of cybercrime can keep pace with increasingly complex technological developments. Therefore, institutional strengthening and the development of digital forensics competencies are key to improving the quality of evidence, including the use of screenshots as evidence in cybercrime cases (Chairunisa & Pradana, 2023).

A final effort to reduce the risk of manipulation is to encourage the use of automated verification technologies such as blockchain-based evidence tracking and secure screenshot applications. This technology allows for automatic recording of the time, device, and context of screenshots, making evidence more difficult to manipulate without leaving a trace. Furthermore, integrating technology into the evidence system will increase judges' confidence in the electronic evidence presented. Therefore, improving technical standards, human capacity, and utilizing integrated technology constitute a comprehensive strategy to strengthen the role of screenshots in proving cybercrime.

4. CONCLUSION

Screenshots play a crucial role in proving cybercrimes, but their evidentiary value is largely determined by the authenticity, integrity, and evidence management procedures implemented by law enforcement. Normatively, the Electronic Information and Transactions (ITE) Law has legally legitimized electronic information as valid evidence, including printouts. However, the reality on the ground shows that screenshots cannot stand alone as primary evidence due to their easily manipulated nature. Research findings indicate that judges tend to be cautious in accepting screenshots, requiring them to be corroborated with other digital data, expert testimony, and forensic examinations to ensure their authenticity. Furthermore, research also found that weak chain of custody documentation, limited technical capabilities of investigators, and the absence of national guidelines are key factors contributing to the often-diminished probative value of screenshots when tested in court.

On the other hand, this study confirms that the strength of screenshots can be significantly increased if they are collected, analyzed, and presented according to digital forensic technical standards. Procedures such as hashing, metadata examination, system log searches, and data matching are crucial elements in transforming screenshots from mere visual evidence into scientifically verifiable digital evidence. The use of forensic tools and the involvement of experts have been shown to strengthen the construction of evidence and help judges understand the context of the incident more objectively. Therefore, this study emphasizes the need for the development of national guidelines on the procedures for handling and authenticating electronic evidence, increasing the capacity of law enforcement officers, and strengthening digital forensic laboratories. Without these measures, the effectiveness of screenshots as evidence in cybercrime will be suboptimal and could potentially create a gap between normative regulations and judicial practice.

5. ACKNOWLEDGEMENT

We would like to express our gratitude to all parties who have supported the development of this research. Special appreciation goes to our supervisors who provided scientific guidance, as well as to our fellow researchers and respondents who helped provide relevant data and information. Without their assistance, cooperation, and contributions, this research on the strength of screenshot evidence in cybercrime would not have been completed successfully.

6. BIBLIOGRAPHY

Permana, I. P. A., Arjaya, I. M., & Karma, N. M. S. (2021). Peranan Alat Bukti Elektronik dalam Tindak Pidana Pencemaran Nama Baik. Jurnal Interpretasi Hukum, 2(2), 422–428. https://doi.org/10.22225/juinhum.2.2.3452.422-428

Hasnawati, H., & Safrin, M. (2023). Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana. AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam, 5(2), 1207–1214. https://doi.org/10.37680/almanhaj.v5i2.2878

Santoso, B. (2024). Evidence of social media accounts in the investigation process. LEGAL BRIEF, 13(4), 960–968. https://doi.org/10.35335/legal.v13i4.1077

Sanjaya, A. A., Hartono, M. S., & Ardhya, S. N. (2022). Penggunaan Akun Media Sosial sebagai Alat Bukti Elektronik dalam Proses Penyidikan. Jurnal Komunitas Yustisia, 5(2), 482–499. https://doi.org/10.23887/jatayu.v5i2.51665

Marzuki, M. H., Sularto, R. B., & Prasetyo, M. H. (2025). Kekuatan Alat Bukti Elektronik dalam Proses Pembuktian Tindak Pidana Pencemaran Nama Baik melalui Media Sosial. Diponegoro Law Journal, 14(1). https://doi.org/10.14710/dlj.2025.48638

Aisyah, N., dkk. (2022). Analisa Perkembangan Digital Forensik dalam Penyidikan Cybercrime di Indonesia: Systematic Review. Jurnal Esensi Sistem Informasi dan Komputasi, 6(1), 22–27. https://doi.org/10.55886/infokom.v6i1.452

Anonim. (2025). Analisis Hukum Bukti Elektronik sebagai Alat Pembuktian dalam Perkara Tindak Pidana. JISPENDIORA, 4(1), 614–626. https://doi.org/10.56910/jispendiora.v4i1.2505

Asaad, A. F. (2023). Efektivitas Hukum Alat Bukti Elektronik dalam Pemeriksaan Perkara. ULM Law Review, 7(1). https://doi.org/10.26623/jic.v7i1.4777

Chairunisa Isradjuningtias, A. C. I., & Pradana, L. B. (2023). Pemanfaatan Digital Forensik dalam Upaya Preventif Penumpasan Berita Bohong. Postulat, 1(2), 51–55. https://doi.org/10.37010/postulat.v1i2.1212

Dasmen, R. N., Pratama, M. R., Yasir, H., & Budiman, A. (2024). Analisis Forensik Digital pada Kasus Cyberbullying dengan Metode NIST SP 800-86. Jurnal Ilmiah Informatika, 12(1), 68–73. https://doi.org/10.33884/jif.v12i01.8344

Gemilang, H. F. (2024). Meninjau Ilmu Digital Forensik terhadap Bukti Elektronik dalam Pembuktian. Perahu: Jurnal Hukum, 12(2). https://doi.org/10.51826/perahu.v12i2.984

Julian, D., & Sutabri, T. (2023). Analisa Kinerja Aplikasi Digital Forensik Autopsy. Jurnal Informatika Terpadu, 9(2), 136–142. https://doi.org/10.54914/jit.v9i2.984

Khairunnisak. (2023). Digital Forensic Tools and Techniques. Jurnal Resistor, 6(1), 1–12. https://doi.org/10.31598/jurnalresistor.v6i1.1266

Putra, B. A. D. (2022). Kedudukan Alat Bukti Elektronik dalam Perkara Pidana. Judiciary: Jurnal Hukum. https://doi.org/10.46576/wdw.v16i4.2437

Yudhana, A. (2022). Forensik WhatsApp Menggunakan Metode Digital Forensic. Jurnal PIT, 7(1). https://doi.org/10.30591/jpit.v7i1.3639