

Digital Evidence in the International Criminal Court

Abdelbasset Mehda*

Laboratory of International

Legal Transformation and Its Impact on Algerian Legislation

University of El Oued-Algeria-

mehda-abdelbasset@univ-eloued.dz

Submission date: 11/06/2026

Acceptance date: 19/09/2026

Publication date: 01/10/2026

Abstract:

This study aims to highlight the importance of digital evidence in international criminal proceedings before the International Criminal Court. It examines the concept of digital evidence and the mechanisms for its collection within the International Criminal Court. The study further assesses the reliability of digital evidence based on the criteria of relevance and probative value. In addition, it addresses the main challenges associated with the use of digital evidence, including issues of authenticity and chain of custody, algorithmic bias, deepfakes, and privacy concerns. The study concludes that digital evidence has become a fundamental component of the international criminal justice system; however, its effectiveness remains dependent on the development and proper implementation of robust legal and technical frameworks.

key words: *Digital evidence; International Criminal Court; Reliability; Authenticity; Probative Value.*

Introduction:

Technology has an integral part of international criminal investigations, as it is no longer possible to rely solely on traditional methods in the face of rapid digital development. The International Criminal Court has kept pace with this shift by utilizing technological tools in the collection and management of evidence, particularly given the increasing volume of digital evidence documenting serious human rights violations.

The procedures of the International Criminal Court have undergone a clear evolution because of this digital transformation, with digital evidence no longer merely serving as an aid but becoming a key element in forming the judges' convictions and proving serious crimes. This development reflects a significant shift in the conduct of international judicial proceedings, alongside the diversification of sources of digital evidence.

However, legal and procedural difficulties remain regarding how the Court handles digital evidence, particularly concerning its authenticity and

** Corresponding Author*

reliability. This may affect the assessment of evidence in proceedings before the Court.

Considering the above, the central question of this study is as follows: To what extent has digital evidence contributed to the development of the work of the International Criminal Court, and what are the challenges facing their adoption?

Based on the central question of the study, the research hypothesis can be formulated as follows: Digital evidence has significantly contributed to the development of the work of the International Criminal Court. However, legal practices are likely to face technical and ethical challenges, particularly regarding issues of authenticity, reliability, and evidentiary assessment, which calls for the development of effective strategies for their management.

To answer this research question, the study primarily relied on the descriptive method by presenting the concept of digital evidence, its types, and the mechanisms of its use before the International Criminal Court, as well as describing the legal and procedural framework governing it within the Court's Statute and international judicial practice. The analytical method was also employed to analyze the relevant legal texts, examine international case law, and assess the standards applied to the admissibility of digital evidence and the evaluation of its probative value, while highlighting the associated challenges.

The study aims to clarify the concept, characteristics, and types of digital evidence within the framework of the International Criminal Court, and to analyze its role in enhancing the Court's work and strengthening its ability to prosecute and prove international crimes. It also seeks to examine the mechanisms for the collection, management, and use of digital evidence in judicial proceedings, as well as to review the legal and technical standards applied in assessing its probative value and verifying its authenticity and reliability in accordance with the Rome Statute and international judicial practice. Furthermore, the study aims to highlight the impact of digital transformation and modern technologies on the development of evidence management before the Court, while shedding light on the main legal, technical, and ethical challenges associated with the use of digital evidence in international criminal justice.

To achieve the intended objectives, this study was divided into two chapters: the first chapter addresses the role of digital evidence in the work of the International Criminal Court, while the second chapter focuses on the assessment of digital evidence before the International Criminal Court and the challenges associated with it.

1- Digital Evidence in the Practices of the International Criminal Court

Digital evidence represents one of the most significant developments in the work of the International Criminal Court in recent years; its role is no longer limited to serving as means of evidence but has become a central element in forming judicial findings. This chapter aims to examine the conceptual framework of digital evidence in the practice of the International Criminal Court, and then to analyze the evolution of its use.

1-1-Conceptual Framework of Digital Evidence in the Practice of the International Criminal Court

The concept of digital evidence has evolved within the framework of the International Criminal Court; we shall therefore attempt to present a conceptual framework that clarifies what digital evidence is and its key characteristics, whilst outlining its main classifications in the Court's judicial practice, thereby aiding an understanding of the nature of this type of evidence and its role in supporting international criminal justice.

1-1-1-Definition of Digital Evidence

Digital evidence is defined as:" Information of probative value that is stored or transmitted in binary form and may be relied upon in court."¹

Digital evidence is also defined as "any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi"².

The term digital evidence refers to"Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination."³

In general, these definitions seem to summaries that digital evidence is data or information collected, stored, or analyzed through electronic media and devices in accordance with specific legal and technical procedures, for the purpose of using it in investigations and judicial proceedings to prove or disprove the commission of a crime.

This evidence plays a pivotal role in International Criminal Court trials, driven by the increasing use of digital technologies in armed conflicts by both civilians and combatants⁴. This generates vast amounts of data that can be used as evidence in legal proceedings.

The court is entitled to admit any evidence that helps it meet its aim of discovering the truth⁵. In this context, aerial photographs, satellite images, and videos are essential for proving that crimes have been committed.

For example, in the Tolimir case, the International Criminal Tribunal for the Former Yugoslavia used satellite imagery provided by the U.S. military to prove the existence of mass graves, as well as large concentrations of prisoners and bodies at specific locations. Aerial

photographs were also used in the Krstić case to prove the mass killings committed in Srebrenica⁶.

Moreover, artificial intelligence can play a crucial role in translation, summarization, and cross checking testimonies, facilitating more efficient case preparation, judicial deliberations, and the drafting of judgments.⁷ In this context, digital evidence plays a key role in strengthening the capacity of the international criminal justice system to uncover international crimes by providing accurate and reliable data that helps to document serious violations, particularly when it is difficult to rely on traditional evidence.

1-1-2- Classification of Digital Evidence

Digital evidence comes in many different forms and continues to evolve alongside technological advancements. As international criminal justice remains a relatively new field of law, most cases deal with unprecedented sets of facts and legal issues. We shall attempt to outline the most common types of digital evidence that have already been used before international criminal courts⁸, as follows:

A. Communication evidence

It is used to identify suspects and track their movements by analyzing call records and location data held by telecommunications service providers. Its importance was highlighted in the case of Ayash and others before the Special Tribunal for Lebanon, where telecommunications records and mobile phone tower data helped track the movements of the accused and link them to the events under investigation⁹.

B. Open-source Evidence

This refers to digital or electronic information available to the public online, which is collected, analyzed and used in the context of criminal investigations to establish or support the facts, provided that its authenticity has been verified. One of the most prominent examples of its use at the International Criminal Court is the case of Thomas Lubanga in the Democratic Republic of Congo, where videos and photographs showing the recruitment of child soldiers were used as supporting evidence to substantiate the charges¹⁰.

Such evidence is typically used to reconstruct events, such as documenting violations or determining the locations and times of crimes, particularly in cases where direct access to the crime scene is difficult.

C. Evidential Digital Platforms:

The International Criminal Court uses this evidence to present and organize digital evidence, such as photographs, videos and satellite imagery, within an interactive environment that aids in understanding the facts of the case. Their use was noted in the Al-Mahdi and Al-Hassan cases,

where they were used to present 'field' evidence in a visual manner that made it easier for judges to follow the locations of the crimes and link the evidence together¹¹.

In cases before the International Criminal Court, digital platforms are not merely tools for organizing and presenting evidence, they also add probative value by linking and interpreting evidence within an interactive context.

In addition to these categories, courts have developed evidentiary handling standards for specific forms of digital material. This is due to the significant expansion of technology use in the investigation of international crimes. The practices of these courts have produced clear guidelines regarding certain types of digitally derived evidence. It can be classified into:¹²

Video evidence: must be submitted as a single, unedited piece, and translated into the language of the court to preserve its evidentiary integrity.

Photographs: require verification of their authenticity regarding source, date, subjects, and the chain of custody.

Aerial and satellite imagery is made fully accessible and assessed for relevance to the facts in dispute, given their importance in establishing contextual and geographic elements of crimes.

Digital recordings: must be accurately translated and carefully analyzed with clear documentation of their origin and chain of custody to guarantee their probative value.

Call data records: should be examined by technical experts to confirm their accuracy and reliability. Their collection and transmission are considered lawful provided they are obtained on a valid legal basis and in compliance with applicable privacy safeguards.

Audio recordings: must be submitted in their entirety without any form of editing, to preserve their original context and prevent distortion of meaning.

Social media posts and emails have been used in international criminal proceedings. Case law has not explicitly addressed the issue of its admissibility or the specific evidentiary requirements applicable to it. This evidence has often been presented alongside other types of evidence, without being subjected to a separate analysis, which has prevented the derivation or formulation of clear and systematic guidelines regarding it¹³.

From the above, digital evidence has become an integral part of the work of the International Criminal Court, not only in terms of its collection and organization, but also in the way it is used within judicial proceedings. In the following section, the study examines how this evidence is managed

within the Court's systems, and how its role has evolved to influence judicial proceedings more broadly.

1-2-The Evolution of Digital Evidence before the International Criminal Court

Digital evidence before the International Criminal Court has undergone significant developments in terms of its management and the mechanisms for handling it within judicial proceedings, as well as its growing role in supporting criminal proof. This section aims to explain how such evidence is regulated within the Court and to highlight the most significant cases that have contributed to the development of the international judiciary's understanding of its value and how it is assessed.

1-2-1- Digital Evidence Processing in Judicial Proceedings

Criminal proceedings before the International Criminal Court proceed through a series of successive stages, including preliminary examination, investigation, the pre-trial phase to confirm the charges, and finally the trial to establish guilt, with the possibility of appeal and enforcement of the sentence¹⁴.

The Office of the Prosecutor (OTP) is responsible for gathering and securing most of the evidence. Since the Court has been in operation for more than a decade, specific systems and procedures have been developed for the collection, registration, and electronic disclosure of evidence¹⁵.

The growing reliance on digital evidence is impacting international criminal justice. Digital materials have become a key source of information for documenting international crimes and supporting judicial investigations.

While the exchange of evidence between the parties takes place directly between them, evidence to be submitted in judicial proceedings must first be filed with the Registry through the Court Management Section (CMS)¹⁶.

Any item to be admitted as evidence must satisfy some requirements: i) relevance to the case, which shall be assessed, according to Articles 69(9)(a) and 69(4) of the ICC Statute, considering how much the "evidence tendered makes the existence of a fact at issue more or less probable"; ii) probative value, which points to its utility in proving an important part of the case and to its relevance in determining a fact or issue;22 iii) both these conditions shall be balanced against any prejudicial effect that could be caused to the proceeding by the admission of the evidence.¹⁷

In this context, the Office of the Prosecutor is seeking to strengthen its capabilities to improve the efficiency of evidence collection, analysis, and management during judicial proceedings.

The Strategic Plan of the Office of the Prosecutor for 2023–2025 outlines how modern technologies will be leveraged to transform the performance of its functions and enhance its effectiveness at all levels¹⁸. The plan aims to modernize the Office of the Prosecutor by technology by leveraging modern digital tools to analyze evidence, establishing an electronic platform to streamline operations, and training staff in the use of these technologies.

Overall, digital evidence management at the International Criminal Court shows the growing role of technology in making judicial work more efficient and supporting court procedures.

1-2-2- Judicial Application of Digital Evidence in International Criminal Cases

This section examines the types of digital and technical evidence presented by the Office of the Prosecutor in three significant cases before international criminal courts, which have contributed to developing judges' understanding of how to admit digital evidence and assess its probative value in the future¹⁹. These cases can be summarized as follows:

A. Prosecutor v. Ayyash et al.

One of the most significant cases demonstrating the use of digital evidence to prove the existence of a conspiracy to commit terrorist acts was the case of Al-Ayash et al. before the Special Tribunal for Lebanon, where the court relied heavily on telecommunications data records and analysis of closed telephone networks. This evidence helped uncover interconnected telephone groups operating within secret, separate networks that were used to plan the 2005 attack targeting former Lebanese Prime Minister Rafik Hariri, thereby helping to prove the element of prior coordination among the defendants²⁰.

In this case, the important role of technical communications analysis in linking individuals to one another and identifying their communication patterns and roles within the network was highlighted, which reinforced the court's conclusion that there was an organized conspiracy that relied on indirect digital means of communication.

B. Prosecutor v. Al Mahdi

The case of The Prosecutor v. Al-Mahdi before the International Criminal Court is a prominent example of the use of digital evidence in international criminal proceedings, as the Court relied in its judgment on a variety of digital evidence, including satellite imagery particularly Google Earth imagery, as well as videos, photographs, and materials published online²¹.

Google Earth images helped document the affected sites and determine the nature of the destruction inflicted on cultural sites in Timbuktu, while

other visual evidence, such as videos and digital photographs, supported the process of verifying the facts and linking them to the accused. The Court affirmed that this type of evidence, when combined with witness testimony and expert reports, provides a strong basis for accurately establishing the facts²².

C. Prosecutor v. Bemba

The case of Bemba et al. before the International Criminal Court serves as an important example of the use of digital evidence in international criminal proceedings, as the Court relied on a wide range of evidence, including electronic money transfers (such as Western Union) used to track payments linked to witness tampering, as well as telephone records, metadata, and emails. The prosecution also seized the defendant's laptop and cell phone while he was in detention and extracted emails and other digital documents from them that supported the case²³.

This diversity of digital evidence helped reveal patterns of communication and coordination among the defendants and link them to acts of interference with the course of justice, while also sparking an important legal debate regarding the reliability of digital evidence, the chain of custody, and the protection of the right to privacy.

It can be concluded that these cases highlight the growing role of digital evidence in international criminal proceedings and the increasing reliance on technology to prove crimes and support judicial decisions.

2-Assessment of Digital Evidence before the International Criminal Court and Associated Challenges

This section examines the assessment and authenticity of digital evidence before the International Criminal Court, as well as the Court's approach under Article 69(4) of the Rome Statute. It also highlights the key developments in the Court's digital transformation and the main challenges associated with the use of digital evidence in international criminal proceedings.

2-1-Assessment of evidence and the authenticity of digital evidence

The assessment of digital evidence and the verification of its authenticity before the International Criminal Court are critical issues, particularly given the increasing reliance on this type of evidence in criminal proceedings. We will attempt to clarify the method the Court employs in evaluating evidence pursuant to Article 69(4) of the Rome Statute, as well as outline the key criteria it uses to verify the authenticity of digital evidence through internal and external indicators.

2-1-1-Evaluation of Evidence Before the International Criminal Court:

An analytical reading of Article 69(4) of the Rome Statute reveals that the International Criminal Court bases its evaluation of evidence on a three-part test: examining the relevance of the evidence to the case, assessing its probative value, and then weighing that value against the potential adverse impact of admitting it²⁴. Consequently, these rules are flexible in nature and apply to all types of evidence, including digital evidence.

A. Assessment of the prima facie relevance of evidence

Pursuant to Article 69(4) of the Rome Statute, the examination of evidence begins with a determination of its prima facie relevance to the subject matter of the case that is, the extent to which it relates to the facts underlying the charges and the issues before the Chamber, as well as matters concerning the rights and participation of victims. It follows that this standard is a preliminary one and constitutes a preliminary stage that does not amount to an assessment of the probative value of the evidence.

In this context, the Trial Chamber in the Katanga and Ngudjolo case clarified that relevance refers to whether the evidence presented makes the existence of the disputed fact probable. If the relevance of the evidence is not self-evident, the party presenting it must demonstrate how it contributes to proving a material fact or a related hypothesis. Thus, the relevance test aims to exclude irrelevant evidence while simultaneously determining the purpose of each piece of evidence in the proceedings²⁵.

Based on the foregoing, the test of prima facie relevance is a simple first step intended solely to ensure that the evidence is relevant to the case, without delving into an assessment of its strength or probative value.

B. Probative value of evidence

It appears from reviewing Article 69(4) of the Rome Statute that, when assessing evidence, the Trial Chamber does not merely consider the existence of the evidence but first examines its probative value on a prima facie basis. This assessment is not based on a single fixed standard, but rather on a set of factors that vary according to the nature and circumstances of each case.

Among the most important judicial precedents in this regard is the Aleksovski case, which shows that the reliability of evidence may be inferred from several indicators, such as its authenticity, its nature, and the circumstances under which it was produced, as well as whether it is direct or hearsay evidence. Furthermore, the absence of an opportunity to cross-examine the source of the evidence may affect the degree of confidence in it, but it does not automatically lead to its exclusion²⁶.

It can be said that probative value should not be understood as a fixed standard, but rather as a flexible element subject to the Chamber's discretion depending on the nature and circumstances of each piece of evidence, thereby ensuring a balance between the strength of the evidence on the one hand and the fairness of the proceedings on the other.

C-The probative value of the evidence against its prejudicial effect:

Under Article 69(4) of the Rome Statute, when evaluating evidence, the Chamber does not merely consider its probative value but proceeds to weigh that value against the potential adverse impact of the evidence on the administration of justice.

In the Katanga case, the International Criminal Court, when applying Article 69(4) of the Rome Statute, The Chamber first considers the strength and probative value of the evidence and then weighs its impact on the fairness of the proceedings²⁷.

Accordingly, we believe that this standard grants the court significant discretionary authority, allowing it to balance the pursuit of the truth on the one hand, with ensuring the fairness of proceedings and avoiding being influenced by evidence whose impact may outweigh its probative value on the other.

It is clear from the foregoing that Article 69(4) of the Rome Statute establishes a rigorous yet flexible approach to the assessment of evidence before the International Criminal Court, based on a clear progression that begins with verifying relevance, then assessing probative value, and finally weighing that value against the potential adverse impact.

2-1-2- Assessing the Authenticity of Digital Evidence:

Authenticity is determined by the extent to which the evidence corresponds to the claims made about it regarding its source or the entity that issued it. Evidence may be considered authentic if the party presenting it can prove that it is indeed what is claimed, which strengthens the court's confidence in the evidence and justifies reliance on it. In this context, the courts assess authenticity based on a set of indicators, whether internal related to the content of the evidence itself or externally related to the circumstances surrounding it²⁸.

A. Internal indicators of authenticity:

Internal indicators of the authenticity of digital evidence include features that help determine its source and authenticity. The Ntaganda case is the simplest example, where certain documents were deemed authentic because they bore a date, an official letterhead, and a signature, indicating that they were prepared in the normal course of business of the issuing entity²⁹.

The court has the discretion to determine whether evidence is reliable by looking for internal indicators of its authenticity. This is done by examining the integrity of the digital material itself such as metadata or source codes as well as reviewing metadata that reveals details such as the file's creation time, its content, and whether it has been modified³⁰.

B. External indicators of authenticity:

External indicators include witness testimony or information identifying the source of the evidence. For example, in the case of Prosecutor v. Karemera, the prosecution presented video evidence of a march accompanied by a written transcript of the related radio broadcast. The International Criminal Tribunal for Rwanda held that the radio broadcast transcript corroborated the date the video was recorded, thereby proving that the accused was present at that gathering³¹.

Similarly, in Prosecutor v. Bagosora, the combination of video footage and the radio broadcast transcript led the court to conclude that the accused held the position of Minister of Defense and thus exercised control over the army³².

It can therefore be said that external indicators play an important role in strengthening the weight of digital evidence by corroborating it with sources independent of the evidence itself, such as witness testimony, radio recordings, or the identification of the source of the digital material.

2-2-Digital Transformation and Challenges of Digital Evidence in the International Criminal Court

Digital evidence before the International Criminal Court has evolved significantly in terms of how it is collected, managed and used in court, and has become crucial in proving crimes.

In this section, we will examine the digital transformation of the court's evidence management system, alongside the key challenges associated with the use of digital evidence in international criminal proceedings.

2-2-1- Digital Transformation in the Processing of Evidence

The Office of the Prosecutor's Strategic Plan for 2023–2025 sets out how the Office intends to use modern technologies to develop its work in a more comprehensive and effective manner. For example, Strategic Objective 3 aims to make the Office a global leader in the field of technology³³.

This plan demonstrates a shift in investigative work before the International Criminal Court, reflecting a transition from traditional methods of evidence gathering to a fully integrated digital model based on the use of advanced technology. This decision demonstrated a clear desire to enhance the capacity to handle vast quantities of diverse digital evidence, including visual, audio and documentary data, through the

development of technological infrastructure and the adoption of cloud-based e-discovery platforms.

In this context, the Office of the Prosecutor has launched two major projects: the OTPLink platform for receiving digital evidence, and the Harmony project for the management and analysis of evidence using artificial intelligence. These projects form part of the Office's drive to promote digital transformation and modernise working practices within investigations.

A. The OTPLink platform for receiving reports and digital evidence

The OTPLink application, launched by the Office of the Prosecutor (OTP) of the International Criminal Court on 23 May 2023, enables witnesses and third parties to submit evidence and reports online and via email. This application replaces previous systems for receiving communications under Article 15 of the Rome Statute, providing two separate portals for anonymous users and authenticated users such as States Parties³⁴.

B. The Harmony Project for Evidence Management and Analysis using Artificial Intelligence

This is a system based on algorithms and artificial intelligence designed to store, manage and analyses evidence with high efficiency. It creates an advanced digital environment utilising cloud-based analysis and investigation tools. The project includes subsystems such as eDiscovery, which provides flexible and secure data storage, and the Evault system, which ensures the permanent preservation of digital evidence with backups and a comprehensive audit trail³⁵.

Both the OTPLink project and the Harmony project aim to accelerate data analysis processes through facial and voice recognition technologies, image and video analysis, automated transcription, and the linking of evidence, whilst ensuring the creation of a reliable and tamper-proof record of evidence collection and handling processes, as well as improving the speed at which reports are processed and categorised by the Bureau.

However, despite these technological advances, the growing reliance on digital systems has given rise to significant legal and technical challenges, which will be addressed in the following section.

2-2-2- Challenges of Digital Evidence in International Criminal Proceedings

The reliance on digital evidence in international criminal courts raises two main types of challenges. The first concerns the nature and reliability of digital evidence, such as its authenticity, source, chain of custody and susceptibility to tampering, whilst the second relates to the technical,

procedural and human rights challenges arising from the use of modern technologies in its collection and analysis. This section will outline the most significant of these challenges.

A- Reliability Challenges in Digital Evidence

Despite the importance of digital evidence in international criminal proceedings, it faces a significant challenge regarding its admissibility and reliability, particularly with regard to the authenticity of the evidence and the procedures used to gather it.

For example, in the Tolimir case, the accused challenged the reliability of satellite images on the grounds that insufficient information had been provided regarding their source, how they were produced or edited, or whether they had been submitted in their original form or after editing³⁶.

Similarly, in the Ongwen case, it emerged that most of the recordings contained significant gaps; the use of video recordings was also challenged on the grounds that it constituted a violation of human rights; and the Ayyash et al. case raised the issue of the admissibility of call logs as evidence, on the grounds that they constituted a violation of privacy³⁷. The vast amount of evidence available online places an increased workload on the parties involved in a case due to time-consuming processes³⁸ such as identifying, verifying, preserving and analyzing the evidence.

Digital evidence differs from traditional evidence in that it has no clear “original copy». It can be copied and stored in multiple locations simultaneously such as devices, servers and the cloud³⁹ which affect the process of verifying its authenticity and integrity and makes it more difficult to verify its source.

B-Technical Challenges in Digital Evidence

Algorithmic bias in the analysis of digital evidence at the International Criminal Court is considered one of the most significant challenges affecting the accuracy and reliability of findings. Furthermore, the use of modern technologies raises issues regarding the accuracy of evidence, particularly where data is stored outside the court’s jurisdiction⁴⁰.

The International Criminal Court lacks a clear and structured procedural framework for dealing with digital evidence, particularly regarding determining who is considered a qualified expert to analyze and verify it⁴¹. This is because it has relied primarily on traditional evidence and has not had to deal with the vast volume of digital evidence.

The potential for breaches of privacy is a critical challenge. Experts must ensure that the individuals appearing in the material have consented to the publication of their images, or that there is a legitimate criminal purpose justifying their display⁴². Therefore, the privacy and dignity of witnesses and victims must be respected.

Given the difficulty of detecting deepfakes⁴³, whether by humans or machines, concerns have arisen about their impact on criminal trials. The risk is not limited to the use of fake evidence, but extends to undermining confidence in all evidence, as anyone can claim that evidence is fake to evade responsibility “the liar’s advantage”, and this may also lead to increased scepticism even regarding genuine evidence “impostor bias”.⁴⁴

Therefore, the growing reliance on digital evidence in international criminal proceedings, whilst offering significant potential for detecting crimes and strengthening the case, also presents a complex set of challenges that affect criminal justice.

Conclusion

In conclusion, it can be said that digital evidence is one of the most significant developments in the proceedings of the International Criminal Court, as it is no longer merely a supplementary means of proof but has become an essential element in enhancing the Court’s ability to uncover the facts and accurately document crimes.

Considering the findings of this analysis, the most important conclusions can be summarized as follows:

- The diversity of digital evidence and the wide range of its applications before the International Criminal Court reflect an evolution in judicial practice, as this evidence includes communication records, open-source materials, digital platforms, and various electronic media.*
- The study also confirms that mechanisms for managing digital evidence before the International Criminal Court have evolved, contributing to increased efficiency in the collection, preservation, and organization of evidence, which has enhanced the effectiveness of judicial proceedings.*
- It is evident that the Office of the Prosecutor relies on modern technologies that enhance the accuracy of evidence, thereby supporting international criminal justice.*
- The study explains that the system for evaluating evidence before the International Criminal Court is based on Article 69(4) of the Rome Statute, under which the judicial chambers enjoy broad discretionary authority to balance the effectiveness of proof with fair trial guarantees.*
- The study also concluded that assessing the reliability of digital evidence relies on an approach that combines internal and external indicators. Internal indicators relate to the characteristics of the evidence itself, such as metadata and file integrity. External indicators relate to independent supporting elements such as testimonies, documents, and recordings, which reinforce the probative value of digital evidence.*

• *The study demonstrated that despite the growing importance of digital evidence in supporting the work of the International Criminal Court in uncovering and proving crimes, it continues to face challenges related to authenticity and reliability, in addition to algorithmic bias and deepfakes.*

In light of these findings, we will propose a set of recommendations aimed at strengthening digital evidence within the international criminal justice system, as follows:

- *A unified procedural framework for digital evidence must be developed within the International Criminal Court, precisely defining the rules for its collection and preservation, thereby ensuring that risks to its credibility are minimized.*
- *Train experts specialized in the analysis of digital evidence and modern technologies, while establishing precise standards for their certification to ensure the quality of their assessments.*
- *Verify the authenticity of digital evidence by adopting technical protocols that include metadata analysis and the use of deepfake detection tools.*
- *Protecting privacy when handling digital evidence by establishing precise legal controls to regulate the use and dissemination of data containing personal information.*
- *Mitigating the risk of data loss by developing a digital infrastructure within the International Criminal Court that ensures reliable data storage and processing.*

References:

1Wael Obeid, *Digital evidence and computer forensics*, United Nations Economic and Social Commission for Western Asia (ESCWA), 2014, p6.

2Eoghan Casey, *Digital evidence and computer crime: Forensic science, computers and the Internet*, Academic Press, 3rd ed, 2011, p7.

3National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, 2nd ed., 2008, p ix.

4Lindsay Freeman and Raquel Vazquez Llorente, *International Criminal Evidence and Procedure in the Digital Age*, *Journal of International Criminal Justice*, 2021, p165.

5Karolina Aksamitowska, *Digital Evidence in Domestic Core International Crimes Prosecutions*, *Journal of International Criminal Justice*, 2021, p198.

6Chiara Ragni, *Digital Evidence in International Criminal Proceedings and Human Rights Challenges*, *ECLIC*, Vol. 7 (Special Issue), 2023, p4.

7Marta Bo, *Artificial intelligence in the prosecution of international crimes*, *International Law Studies*, vol. 106, p9.

8Mahmoud Hussein Seref, *Digital Evidence before the International Criminal Court*, *International Journal*, Vol. 4, No. 1, 2024, p358.

9Ibid, p263.

- 10Nikita Mehandru and Alexa Koenig, *Open-Source Evidence and the International Criminal Court*, *Harvard Human Rights Journal*, 2019, accessed 05/06/2026, at 17:00, article published on,
<https://journals.law.harvard.edu/hrj/2019/04/open-source-evidence-and-the-international-criminal-court/>
- 11Anastasiia Liulina, *Evidentiary Digital Platforms: What the Al Mahdi and Al Hassan Cases Teach Us about Presenting Voluminous Digital Data*, *International Criminal Law Review*, Vol. 29, No. 1, 2025, p7.
- 12Leiden Guidelines, *Leiden Guidelines on the Use of Digitally Derived Evidence in ICC Trials*, 2022, p9.
- 13Ibid, p8.
- 14Yann Lecorps and AL., *How is digital evidence used in the International Criminal Court? A theoretical and empirical approach*, *CRESE*, 2025, p4.
- 15Mark Dillon and David Beresford, *Electronic Courts and The Challenges in Managing Evidence: A View from Inside the International Criminal Court*. *International Journal for Court Administration*, Vol. 6, No. 1, 2014, p6.
- 16Ibid., same page.
- 17Ibid., p8.
- 18Hanna Kuczyńska, *The ICC enters the future: the digital-evidence of revolution or evolution?* *International Criminal Procedure and International Legal Cooperation*, Vol. 10 No. 3, 2024, p10.
- 19Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, *Fordham International Law Journal*, Vol. 41, No. 2, p307.
- 20See *The Prosecutor v. Ayyash et al.*, *Decision Denying Sabra Defense Motion to Admit into Evidence Twenty Witness Statements*, STL-11-01/T/TC (Trial Chamber, 20 December 2017), available at: [World Courts, https://www.worldcourts.com/stl/eng/decisions/2017.12.20_Prosecutor_v_Ayyash_et_al.htm](https://www.worldcourts.com/stl/eng/decisions/2017.12.20_Prosecutor_v_Ayyash_et_al.htm)
- 21See *The Prosecutor v. Ahmad Al Faqi Al Mahdi*, *Judgment and Sentence*, ICC-01/12-01/15, Trial Chamber VIII, 27 September 2016.
- 22Ibid.
- 23See *The Prosecutor v. Jean-Pierre Bemba Gombo*, *Judgment pursuant to Article 74 of the Statute*, ICC-01/05-01/08, Trial Chamber III, 21 March 2016.
- 24ICC, *The Prosecutor v. Thomas Lubanga Dyilo*, *Decision on the admissibility of certain documents*, ICC-01/04-01/06, 20 January 2011, p16-17.
- 25Rafael Braga da Silva, *Updating the Authentication of Digital Evidence in the International Criminal Court*. *International Criminal Law Review*, Vol. 22, 2022, p943.
- 26ICC, *Prosecutor vs. Katanga*, *Decision on the prosecutor's Bar Table Motions*, ICC-01/04-01/07, 17 December 2010, p16.
- 27See Ibid.
- 28 Rafael Braga Silva, *op. cit.*, p945.
- 29Ibid, p946.
- 30Mahmoud Hussein Seref, *op.cit.*, p398.

31Aida Ashouri and AL, *an overview of the use of digital evidence in international criminal courts (Salzburg Workshop on Cyber Investigations working paper)*. Berkeley Human Rights Center, University of California, Berkeley, 2013, p4.

32Ibid., p5.

33International Criminal Court, Office of the Prosecutor, *Strategic Plan 2023–2025*, 2023, p14.

34Hanna Kuczyńska, *The ICC enters the future: the digital-evidence of revolution or evolution?* *International Criminal Procedure and International Legal Cooperation*, 2024, Vol. 10, No. 3, p7.

35Ibid., p7.

36Chiara Ragni, *op.cit.*, p3.

37Ibid., p4.

38McDermott, Y. and al., *new evidence, new challenges: ICC judges' perspectives on user-generated evidence and judging in an age of artificial intelligence*, *Oñati Socio-Legal Series*, Spain, 2026, p10.

39Lindsay Freeman and Raquel Vazquez Llorente, *op.cit.*, p167.

40Anne Hausknecht, *"The Impact of Deepfakes on Trust in User-Generated Evidence: Deepfakes and the Law: Challenges, Responses, and Critique"*, *SSRN Paper*, Swansea University, 2025, p18.

41 Matthew Gillett and Wallace Fan, *op.cit.*, p677.

42 Ibid., p685.

43It is generated using machine learning techniques to produce manipulated or fully synthetic audio, images, videos, text, or even real-time media, see Maria-Paz Sandoval, *Threat of deepfakes to the criminal justice system: a systematic review*, *Crime Science* 2024, Vol. 13, No. 1.

44 Anne Hausknecht, *op. cit.*, p18.