Indonesian Red Crescent Humanitarian Journal
published by Bulan Sabit Merah Indonesia

p-ISSN: 2829-8497, e-ISSN: 2829-8500
Vol.4, No.2 Suppl. 1 (2026), hal. 1-9
https://doi.org/10.56744/irchum.v4i2s1.109

Documenting Gaza Under Siege: Strengtening Digital Evidence Standards for Internasional Accountability

Meiske Iriyani*, Dendy Prasetyo Nugroho
Magister Hukum Universitas Islam Indonesia[1], CLDS FH UII[2]
Candirejo, Sardonoharjo, Kec. Ngaglik, Sleman, Daerah Istimewa Yogyakarta 55581, Indonesia
***Correspondence author:** Meiske Iriyani

Abstract. The ongoing attacks against civilians in Gaza occur in a closed investigative environment, where access for journalists, humanitarian organizations, and international investigators is systematically restricted due to blockade, infrastructure destruction, and risks of targeted violence. These conditions severely limit the collection of conventional forensic and testimonial evidence, making digital evidence, such as citizen-recorded videos, satellite imagery, communication data, and open-source media, central to documenting alleged violations of international humanitarian law and international criminal law. This paper aims to analyze the role, reliability, and admissibility challenges of digital evidence in efforts to prevent impunity for crimes committed in Gaza. Using a normative legal research method and comparative analysis of international soft law instruments, particularly the Berkeley Protocol on Digital Open Source Investigations and the Leiden Guidelines on Digital Evidence, this study examines how digital documentation may be strengthened to meet evidentiary thresholds applied by the International Criminal Court and United Nations fact-finding mechanisms. The findings indicate that although digital evidence enables continuous documentation under siege conditions, the absence of harmonized standards on authentication, verification, and chain of custody weakens its probative value in judicial proceedings. The paper concludes that harmonizing digital evidence standards from field documentation to courtroom evaluation is essential to ensure that documentation collected in Gaza can meaningfully support accountability processes and contribute to the prevention of impunity.

Keywords: digital evidence, primary evidence, Gaza

Introduction

The current development of digital technology in law enforcement shows its importance as instrument on the documentation of human rights violation and international crimes. Digital evidence has been used by various NGOs as well as United Nations Bodies/Agencies especially in the context where investigation access is very limited. The use of digital evidence, especially OSINT (Open Source Intelligence) can be more urgent in a situation where physical access to an area where violation occurred is structurally and systematically restricted by the authorities in power (closed investigative environment) (Berkeley, 2022). Such conditions, for example, are occurring in Gaza, Myanmar, and Syria, where international institutions including United Nations (UN) fact-finding missions, humanitarian organizations, and independent journalists are denied adequate access to conduct direct field investigations (Albanese, 2025; OHCHR, 2023; UN, 2016; UN Human Rights Council, 2018). This situation makes conventional evidence collection, forensic examinations, and direct witness interviews extremely difficult (Combs, 2010).

In Gaza, the land, sea, and air blockade has restricted the movement of residents and denied access to international investigators, including OHCHR investigative teams and other UN mechanisms (Albanese, 2025). Access restrictions are systematically implemented by the occupying government, Israel, including communication blackouts, targeting of journalists, and destruction of media infrastructure (*Over 210 Journalists Killed in Gaza*, 2025). As a result, digital evidence has become primary source of documentation of alleged international crimes, both for the purposes of record-keeping advocacy and potential accountability (Crawford-Holland et al., 2025).

Normatively, the ICC permits the use of digital evidence, stating that it cannot automatically reject certain types of evidence (Rome Statute of the International Criminal Court, 1998; Rules of Procedure and Evidence to the Rome Statute, 2001). Digital evidence can have recognized and testable probative value in international criminal courts, not just as supplementary evidence (*Prosecutor v. Ahmad Al Faqi Al Mahdi*, 2016). International courts such as the International Criminal Court apply stricter evidentiary standards, i.e. "beyond reasonable doubt," which require authenticity, integrity, and accountable reliability. In a closed investigative environment, these requirements are often difficult to meet due to the absence of a complete chain of custody, limitation in source verification, and the potential for manipulation or incomplete context. Thus digital evidence that can be used in UN fact finding reports cannot necessarily be used in cases before court.

The case of *Prosecutor v. Al Mahdi* at the ICC demonstrated that digital evidence played a key role in proving the defendant's involvement in the destruction historical sites in Timbuktu (*Prosecutor v. Ahmad Al Faqi Al Mahdi*, 2016). However, in that case, Al Mahdi pleaded guilty, so the examination of digital evidence during the trial was not given much weight. On the other hand in *Prosecutor v. Al Werfalli*, ICC issued an arrest warrant based on a video recording of an execution posted on Facebook showing the suspect directly or ordering the killing of detainees (*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, 2017). However, the case never went to trial because the de facto Libyan government refused to hand over the defendant, who then died in 2021 (ICC Public Affairs Unit, 2021). This means that the digital evidence used as the basis for the issuance of the arrest warrant was also never tested in court. The *Al Mahdi* and *Al Werfalli* case demonstrate that, in certain situations, the ICC can use digital evidence as a basis for prosecuting individuals.

Harmonizing evidentiary standards in the context of international crimes in closed door investigations is an urgent need. Such harmonization is crucial to ensure that the digital evidence obtained not only meets documentation and reporting requirement but also has probative value that can be legally accounted for. This article argues that under conditions of structural access denial, digital evidence may be relied upon as primary evidence, provided that its collection and evaluation are harmonized through existing soft-law instruments

Methods

This research is a qualitative research with a historical approach to trace the direction of the development of scientific evidence theory, as well as a conceptual approach to study and analyze various opinions and debates in the development of scientific evidence. This research is based on a literature study, where academic articles and relevant research documents regarding the theory of scientific evidence are analyzed in depth. The collected material is then analyzed prescriptively, to present a holistic picture of Documenting Gaza under Siege: Strengthening Digital Evidence Standards For International Accountability.

Result and Discussion

Gaza as a Closed Investigative Environment

Restricted access to evidence is a recurring feature in armed conflict, but not all situations of limited access constitute as a closed investigative environment. For the purpose of this article, a closed investigative environment refers to a situation in which; (i) territorial access for independent investigators is formally denied or rendered practically impossible for a sustained period; (ii) no feasible means exist to collect physical or forensic evidence within a timeframe compatible with evidentiary preservation; (iii) authorities exercising effective control over territory are unwilling or unable to cooperate; (iv) delay in evidence collection risks irreversible loss of material relevant to criminal accountability.

Gaza is a clear example of a closed investigative environment. Restriction in Gaza are structural, prolonged, and systematically enforced (OHCHR, 2023). Access for international investigators, journalists, forensic experts, and humanitarian organizations has been severely cut after the imposition of comprehensive land, sea, and air blockade (Amnesty International, n.d.). The condition is aggravated during period of intensified hostilities where there are security risks, destructions of infrastructure, and communication blackouts, making on-site investigation becomes very challenging, if not impossible. In this situation, physical crime scenes are frequently destroyed or altered because of continued bombardment before forensic examination can be conducted. Official documents, military orders, and internal communications relevant to command responsibility remain inaccessible due to classification and non-cooperation by authorities exercising effective control (Ambos, 2024). Witnesses are often displaced, injured, or killed and the one remaining face substantial risks of retaliation, undermining the feasibility of direct testimony (Amnesty International, n.d.).

The closed nature of investigative environment in Gaza thus has implications beyond evidentiary logistics. Access denial operates as an additional factor to impunity as it obstruct the collection of evidence supposedly required to meet judicial thresholds (Combs, 2010). When evidentiary frameworks fail to adapt to such environments, structural barriers to investigation risk transforming into legal barriers to accountability. Prolonged access denil has increasingly shifted documentation responsibilities to non-state actors and civil society organizations, whose digital records often constitute the primary contemporary account of alleged violations (Hellwig, 2021).

In closed investigative environment, judicial assessment of digital evidence cannot be detached from the structural conditions under which such evidence is produced. Formal recognition of sustained access denial, communication blackouts, and the absence of forensic alternative allows judges to evaluate probative value with contextual awareness, without lowering the applicable standard of proof or displacing the burden borne by the prosecution.

Evidentiary Theory and Digital Evidence in Criminal Law

In the investigation of international crimes, the use of digital evidence is crucial, especially when investigators are unable to access the area where the crime is suspected to have occurred. In fact, individuals, whether witnesses, victims, or even perpetrators, can upload photos or videos online (Irving, 2020). However, Laux (Johann Laux, 2018) notes that the evidentiary value of internet data remains a matter of debate in the legal realm, particularly in international courts. The main challenges include the complexity of source authentication and the potential inaccuracy of digital data (Lecorps et al., 2025).

There arefour fundamental parameters, namely: relevant, admissibility, exclusionary rules, and weight of proof. Relevant means the evidence submitted must be relevant to the

claim/charge indicted. Admissibility, in this case an evidence that is accepted as relevant. Exclusionary rules interpreted as a way to obtain evidence that is in accordance to the law. If evidence is obtained by illegal means or not in accordance with the applicable law, then evidence must not be taken into account in the examination in court. Weight of proof is every relevant and acceptable evidence must be evaluated by the judge (Hiariej, 2012). Judge should assess evidence and using them as a basis for the judge's consideration in their decision. In other words, the strength of evidence becomes the full authority of the judge (Hiariej, 2012).

Prosecutor has the burden of proof, thus they must present digital evidence that convinces the court that the perpetrator committed a crime (Louis Kaplow, 2012). Specifically, the prosecutor must be able to convince the judge beyond any reasonable doubt. As a result, prosecutor is more open to types of evidence, including digital evidence, than the defense in order to fulfill the burden of proof (Eric L. Talley, 2013).

ICC Evidentiary Framework

The evidentiary framework in the ICC is characterized by flexibility, however with rather demanding standards of proof. Article 69 of the Rome Statute gives the Court discretion to assess evidence based on relevance and probative value without imposing rigid admissibility rules (Rome Statute of the International Criminal Court, 1998; Schabas, 2011). This allows for the admission of wide range of evidentiary material, including digital evidence and open-source information.

Probative value assigned to evidence remains tied to conventional indicators of reliability, such as clear origin, identifiable chain of custody, and corroboration through physical or testimonial evidence. ICC jurisprudence demonstrates that while digital evidence may be admitted, its weight is often depending on confirmation through conventional investigative means (*Prosecutor v. Ahmad Al Faqi Al Mahdi*, 2016; *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, 2017). These evaluative practices reflect implicit assumptions regarding access to crime scenes, witnesses, and institutional cooperation. This assumption do not hold in closed investigative environment such as Gaza.

At the preliminary phase, digital evidence has proven to be sufficient to satisfy the "reasonable ground to believe" threshold, including arrest warrant grounded primarily in video recordings disseminated online (*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, 2017). At the trial stage, however, where the standard is "beyond reasonable doubt", the absence of physical corroboration and formal chain of custody present significant obstacles (Ambos, 2024). Digital material capable of establishing the occurrence of an attack may struggle to support findings concerning attribution, intent, or command responsibility in the absence of internal documents or direct testimony.

Braga da Silva observes that authentication at the ICC often relies on implicit judicial reasoning rooted in analogue evidentiary assumptions, resulting in fragmented and sometimes unclear assessment of reliability. This becomes consequential in context where digital evidence constitutes the primary source of documentation, as judicial discretion remains unguided by structures evaluative criteria (Braga Da Silva, 2021)

In Gaza, these challenges are worsened by the systemic non-cooperation and access denial. The ICC's evidentiary framework implicitly assumes the feasibility of obtaining documentary evidence from state authorities or conducting follow-up investigations on the ground (Schabas, 2011). Where such cooperation is absent, evidentiary expectations rooted in traditional investigative paradigms could be unattainable. This creates disconnection between the evidence that can realistically be collected and the standards against which it is assessed.

Indeed, caution toward digital evidence reflects legitimate concerns regarding manipulation, misattribution, and context loss (Berkeley, 2022; Leiden, 2022). However, an evaluative approach that treats digital evidence primarily as supporting evidence may inadvertently disadvantage situations where gathering supporting evidence through conventional means is structurally impossible. Thus, while digital evidence is formally admissible, its probative potential remains constrained by evaluative assumptions incompatible with closed investigative environments.

Admissibility in the Evidentiary System of Digital Evidence

The use of technology in the evidence-gathering process plays a strategic role in uncovering crimes, particularly in the realm of international crimes. Digital evidence has become a crucial instrument in the prosecution of international crimes, given the complexity of cases and its ability to bridge the limitations faced by international judges in the process of seeking material truth regarding events that occur far from the courtroom (Lecorps et al., 2025). Questions arise regarding its admissibility and reliability, as clarified by the jurisprudence of the ICC and other international criminal tribunals (Ragni, 2023). The use of digital evidence can also raise concerns about respect for due process standards (Packer, 1964) and the right to privacy.

The mechanism of the digital evidence admissibility process at the ICC currently has unique challenges due to the nature of data, i.e. vulnerable to manipulation and unclear sources. In this discussion the author divides the analysis of the admissibility of this evidence into three main frameworks, namely the ICC internal standards, the Berkeley Protocol and the Leiden Guidelines.

In practice, the ICC applies three stages of evaluation based on Article 69 (4) of the Rome Statute, namely determining the relevance of evidence *prima facie*, assessing the probative value through examination and chain of custody and considering the possible effects (prejudicial effectiveness) to ensure legal certainty in the trial (Sangari & Mohammadi, 2024).

The Berkeley Protocol, focuses primarily on Open Source Intelligence (OSINT). For digital evidence to be considered valid, this protocol emphasizes chain of custody standards, which include authentication, content verification, and preservation (Berkeley, 2022). Meanwhile, the Leiden Guidelines more specifically address the use of digital evidence in the context of international criminal law. These guidelines bridge the gap between high-tech and legal procedures in the courtroom. The standards in the Leiden Guidelines include relevance and evidentiary value, reliability, and balance of rights (Leiden, 2022)

Harmonization Model for Digital Evidence in a Closed Investigative Environment

There is a growing reliance on digital evidence in international criminal investigations and human rights violations that have been accompanied by the development of multiple soft law instruments aiming to address distinct stages of the evidentiary process. The Berkeley Protocol on Digital Open Source investigations provides guidance on the ethical and technical collection and verification of open-source information, while the Leiden Guidelines articulate principles for the judicial assessment of digital evidence in international criminal proceedings. Although these instruments play an important role in enhancing the reliability and legitimacy of digital evidence, they operate in parallel rather than as part of a coherent evidentiary framework (Berkeley, 2022; Leiden, 2022).

This fragmentation becomes particularly problematic in closed investigative environments, where digital evidence constitutes as primary, or even sole, means of documentation. In such context, the absence of physical access, forensic examination, and

institutional cooperation prevents investigators from supplementing digital material with conventional forms of corroboration. Yet, international criminal adjudication continues to assess probative value largely through evaluative assumptions rooted in traditional investigative conditions, including expectations of physical custody, identifiable authorship, and documentary corroboration (Schabas, 2011). The resulting disjunction potentially render digital evidence procedurally admissible but substantively insufficient.

The absence of a structured authentication doctrine, as identified inexisting analysis of ICC practices, underscore the need for a harmonized framework (Braga Da Silva, 2021). At the same time, empirical studies of contemporary conflict documentation demonstrate that digital evidence is already relied upon as a primary investigative resource in context of access denial (Hellwig, 2021)

This article proposes a harmonization model aimed at bridging the gap between field-level documentation practices and courtroom evidentiary evaluation. Rather than introducing new normative standards, the model operates as an interpretative framework that aligns existing instruments and practices across the evidentiary lifecycle. It is grounded in the discretionary authority granted to the ICC under Article 69(4) of the Rome Statute, which allows the Court to assess evidence on the basis of its relevance and probative value without rigid rules of admissibility (Rome Statute of the International Criminal Court, 1998).

Under the proposed harmonization model, the Berkeley Protocol functions as the baseline standard for evidentiary integrity at the collection and verification stage. This to ensure the digital materials are systematically sources, authenticated, and preserved (Berkeley, 2022). The Leiden Guidelines then, will operate as the interpretive bridge at the adjudicative stage, guiding courts in contextualizing and weighing such evidence in light of access denial and investigative severe limitation (Leiden, 2022). When applied together, these instruments enable digital evidence to be assessed as primary evidence where other feasible alternative is limited, without diluting established standards of proof.

The proposed harmonization model addresses the ‘linkage gap’ by operationalizing the discretionary authority of the ICC under Article 69(4). By aligning Berkeley’s technical verification with Leiden’s evaluative weight, the Court can recognize that the certainty of hashes and geo-located data provides a functional equivalent to physical forensics. This prevents access denial from becoming a de facto legal defense, ensuring that high-level command responsibility can be established even when the physical crime scene remains out of reach.

Through the Berkeley Protocol standard, every piece of digital data is hashed (a mathematical process that transforms a set of digital data) from the moment it is first acquired in the conflict zone. This addresses a classic challenge in ICC proceedings regarding data manipulation. Its novelty lies in the integration of hashing techniques with the legal assessment of the Leiden Guidelines, eliminating the need for judges to question the integrity of files, even those originating from highly isolated and disinformation-ridden regions.

Harmonization may further be supported through structured corroborative reasoning, where multiple independent digital indicators such as metadata consistency, geolocation analysis, satellite, or witness testimony, are assessed cumulatively. Such an approach does not impose numerical thresholds but assists judicial reasoning by making explicit the basis upon which reliability and probative value are inferred.

This harmonized approach preserves prosecutorial and judicial discretion. It does not mandate the acceptance of digital evidence as primary evidence in all cases, nor does it lower admissibility thresholds. It tries to provide evidentiary choice where access denial is formalized

and sustained. By aligning investigative rigidity with judicial evaluation, the model reduces the risk that evidentiary deficits caused by obstruction or siege conditions translate into impunity.

Importantly, the harmonization proposed in this article does not impose technical or legal obligations on civilians who document events under conditions of extreme risk. Standards of preservation, verification, and authentication are directed at receiving entities such as investigators, prosecutors, and fact finding bodies, to ensure that citizen-generated material is assessed responsibly rather than dismissed due to technical deficiencies beyond the control of its creators.

This harmonization serves as a defensive function within international criminal law. It ensures that existing evidentiary principles remain effective under conditions of structural access denial and prevents evidentiary formalism from becoming a tool through which accountability is evaded. While Gaza provides a critical case study for this approach, the harmonized model has broader relevance for ongoing investigations in similarly closed environments, for instance in Myanmar and Syria, where digital documentation increasingly constitutes the backbone of accountability efforts.

Conclusion

This article examined the role of digital evidence in situations where conventional investigative methods are structurally unavailable, using Gaza as paradigmatic example of a closed investigative environment. Prolonged access denial, destruction of infrastructures, and the absence of effective cooperation mechanisms fundamentally alter the evidentiary landscape. This situation render digital documentation central to accountability efforts. International criminal procedure, including ICC's evidentiary framework, does not preclude reliance on digital material as a principla evidentiary foundation, entrusting judges with assessing relevance, reliability, and probative value on case-by-case basis.

To address the vulnerabilities of digital evidence in such context, this article has proposed a harmonization model integrating the Berkeley Protocol's investigative thoroughness with the adjudicative guidance of the Leiden Guidelines. This approach does not lower evidentiary thresholds or alter burden of proof, but clarifies how reliability may be contructed during documentation and how probative value may be reasoned judicially. Digital evidence may therefore be relied upon as primary evidence under clearly defined conditions where no feasible alternative exists. While gaza serves as critical case study, the framework advanced here offers a principled option for accountability mechanisms in closed investigative environments more broadly. This will contribute to the prevention of impunity while remaining faithful to the core guarantees of international criminal justice.

References

Albanese, F. (2025). Report of the Special Rapporteur on theSituation of Human Rights in the Palestinian Territories Occupied Since 1967, Gaza Genocide: A Collective Crime (No. A/80/492). UN General Assembly.

Ambos, K. (2024). Treatise on International Criminal Law (2nd ed). Oxford University Press, Incorporated.

Amnesty International. (n.d.). Human rights in Israel and the Occupied Palestinian Territory. Amnesty International. Retrieved December 31, 2025, from

https://www.amnesty.org/en/location/middle-east-and-north-africa/middle-east/israel-and-the-occupied-palestinian-territory/report-israel-and-the-occupied-palestinian-territory/

Berkeley. (2022). Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. Human Rights Center UC Barkeley School of Law and OHCHR.

Braga Da Silva, R. (2021). Updating the Authentication of Digital Evidence in the International Criminal Court. International Criminal Law Review, 22(5–6), 941–964. https://doi.org/10.1163/15718123-bja10083

Combs, N. A. (2010). Fact-finding without facts: The uncertain evidentiary foundations of international criminal convictions. Cambridge university press.

Crawford-Holland, S., Smith, P. B., & Williams, A. (2025). Law's capture of human rights focused open-source investigation. London Review of International Law, 13(1), 93–113. https://doi.org/10.1093/lril/lraf007

Hellwig, K. (2021). The Potential and the Challenges of Digital Evidence in International Criminal Proceedings. International Criminal Law Review, 22(5–6), 965–988. https://doi.org/10.1163/15718123-bja10110

Hiariej, E. O. S. (2012). Teori dan Hukum Pembuktian (1st ed.). Erlangga.

ICC Public Affairs Unit. (2021). Statement on the Reported Death of Mahmoud Al-Werfalli.

Irving, E. (2020). Molly K. Land and Jay D. Aronson, New Technologies for Human Rights Law and Practice, 2018, Cambridge University Press, 330 pp, ISBN 9781107179639. Leiden Journal of International Law, 33(1), 249–252. https://doi.org/10.1017/S092215651900058X

Lecorps, Y., Naili, K., Obidzinski, M., Oytana, Y., & Toutounji, T. (2025). How is Digital Evidence Used in the International Criminal Court? A Theoretical and Empirical Approach. Working Papers AFED, Article 25–05. https://ideas.repec.org//p/afd/wpaper/2505.html

Leiden. (2022). Leiden Guidelines on the Use of Digitali Derived Evidence. Leiden University.

OHCHR. (2023). Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel (No. A/HRC/53/22). UN.

Over 210 journalists killed in Gaza: RSF and Avaaz call on media worldwide to stage major operation on 1 September | RSF. (2025, August 28). https://rsf.org/en/over-210-journalists-killed-gaza-rsf-and-avaaz-call-media-worldwide-stage-major-operation-1

Prosecutor v. Ahmad Al Faqi Al Mahdi (International Criminal Court September 27, 2016).

Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, No. ICC-01/11-o1/17 (ICC August 15, 2017).

Ragni, C. (2023). DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL PROCEEDINGS AND HUMAN RIGHTS CHALLENGES. 1–16. https://doi.org/10.25234/eclic/28255

Rome Statute of the International Criminal Court (1998).

Rules of Procedure and Evidence to the Rome Statute (2001).

Sangari, Z. N., & Mohammadi, A. M. (2024). Admissibility of Digital Evidence at the International Criminal Court. Journal of Criminal Law Research, 41–84.

Schabas, W. A. (2011). An introduction to the International criminal court (4th ed). Cambridge University Press.

UN. (2016). Commission of Inquiry on the Syrian Arab Republic. UN.

UN Human Rights Council. (2018). Independent International Fact-Finding Mission on Myanmar (No. A/HRC/39/64). UN.