

Cyberactivism and Open Source Intelligence (OSINT): Normative Standards for the Evaluation of Citizen-Gathered Digital Evidence in International Criminal Justice

Maria Florencia Carballo Nieves, Ph.D.¹

¹ Orbis Iuris

Correspondence: florencia@florenciacarballo.com

Article Info

Article history:

Received Jul 27th, 2026

Revised Jul 28th, 2026

Accepted Aug 4th, 2026

Keyword:

Open source intelligence; digital evidence; International Criminal Court; authentication deficit; free proof; Berkeley Protocol

ABSTRACT

This article examines how the International Criminal Court evaluates citizen-gathered open source intelligence (OSINT). Through doctrinal legal research, it analyses the Rome Statute (Articles 21, 51–52, 64 and 66–69), the Rules of Procedure and Evidence (Rules 63–64, 69 bis, 79 and 81), ICC case law up to the 2025 Yekatom and Ngaïssona judgment and the 2026 Duterte decision on the e-Court Protocol, comparative regimes, and the epistemology of machine testimony. The central problem, it argues, lies not in admissibility but in an “authentication deficit”: the absence of binding standards for deciding whether digitally derived evidence, once admitted, is trustworthy enough to bear the weight placed on it. The article proposes a six-element framework: cryptographic hashing at capture, anchored with an entity independent of the collector; standardised, disclosable chain-of-custody documentation open to challenge by the defence; a permissive inference of authenticity, displaceable by any specific challenge and placing no persuasive onus on the accused, as Article 67(1)(i) requires; source-protection safeguards tested against Articles 67(1)(e), 67(2) and 68(1); a duty to give reasons when departing from the Berkeley Protocol and the Leiden Guidelines; and a best-evidence requirement that operates as a safety valve and never excludes evidence. The framework is distributed across the e-Court Protocol, Regulations of the Court under Article 52 and provisional Rules under Article 51(3). It would narrow the authentication deficit without displacing free proof or burdening the defence, although it cannot establish what an item depicts, where or when it was recorded, or who made it.



© 2026 The Authors. Published by Nusantara Society Lab. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

International criminal law has been slow to address one of its most pressing evidentiary questions. An activist with a smartphone can now record an attack, upload the footage to a social media platform and later see that material relied upon before an international court, and the volume of such material has grown faster than the instruments available to evaluate it.¹ In August 2017 the Pre-Trial Chamber issued an arrest warrant for Mahmoud Al-Werfalli that relied largely on videos of executions in Libya posted on social media.² On 24 July 2025 Trial Chamber V delivered its judgment in Yekatom and Ngaïssona. Resting on 19,590 items of evidence, among them approximately 943 items of Facebook material and 104 items of call data records, it contains the Court’s fullest treatment so far of digitally derived evidence.³ Between the two decisions, the Court’s engagement with this kind of evidence deepened considerably while the legal framework governing it remained unchanged.

¹See generally Sam Dubberley, Alexa Koenig, and Daragh Murray, eds., *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford: Oxford University Press, 2020), <https://doi.org/10.1093/law/9780198836063.001.0001>.

²*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, ICC-01/11-01/17-2, Warrant of Arrest (Pre-Trial Chamber I, August 15, 2017) (hereafter *Al-Werfalli*, First Warrant), paras. 11–22; Emma Irving, “And So It Begins... Social Media Evidence in an ICC Arrest Warrant,” *Opinio Juris*, August 17, 2017, <http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/>.

³*Prosecutor v. Yekatom and Ngaïssona*, ICC-01/14-01/18-2784-Red, Judgment (Trial Chamber V, July 24, 2025) (hereafter *Yekatom and Ngaïssona*, Trial Judgment), paras. 132 (19,590 items formally submitted), 144 (approximately 943 Facebook items), and 158 (approximately 104 items of call data records). All references in this article are to the public redacted version. For commentary, see Emma Irving and Sabrina Rewald, “Digital Evidence Before the ICC: Lessons from the Yekatom/Ngaïssona Judgment,” *Opinio Juris*, August 8, 2025, <https://opiniojuris.org/2025/08/08/digital-evidence-before-the-icc-lessons-from-the-yekatom-ngaissona-judgment/>.

The Rome Statute follows a model of free proof. Article 69 gives Chambers broad discretion over relevance and admissibility,⁴ and Rule 63(2) of the Rules of Procedure and Evidence empowers a Chamber, “in accordance with the discretion described in article 64, paragraph 9, to assess freely all evidence submitted in order to determine its relevance or admissibility in accordance with article 69,” a power the Yekatom Chamber expressly invoked.⁵ No exclusionary rule bars digital evidence. Nor, on the reading adopted here, does any provision of the Statute or the Rules govern the authentication of born-digital content, the preservation of metadata or the integrity of digital chains of custody. That silence was understandable when the Statute entered into force in 2002; it is considerably harder to justify in 2026.

Two soft-law instruments have partly filled the gap: the Berkeley Protocol on Digital Open Source Investigations, published by the UN Office of the High Commissioner for Human Rights and the Human Rights Center at the University of California, Berkeley,⁶ and the Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals.⁷ Neither has binding force. Synthetic media make it possible to fabricate convincing evidence and produce what has been called the “liar’s dividend,” the ability to dismiss genuine documentation as manipulated.⁸ Platforms enforcing their own community standards routinely remove content that may evidence international crimes, often before anyone has preserved it.⁹ The Court has responded through prosecutorial and technological measures, among them the OTPLink platform, Project Harmony and a Policy on Cyber-Enabled Crimes, rather than through its law of evidence; the cyber policy itself states that detailed questions of the collection, analysis, management and use of digital evidence “exceed the scope of this Policy.”¹⁰

This article argues that the central normative problem lies not in admissibility but in what it calls the authentication deficit: the absence of binding standards for deciding when digitally derived evidence is trustworthy enough to bear the weight that courts place on it.¹¹ Drawing on civil-society practice, comparative authentication regimes, the epistemology of machine testimony and the principles articulated in Yekatom, it develops a six-element framework, identifies an instrument capable of carrying each element, and shows that the framework imposes no onus of rebuttal on the accused, consistently with Article 67(1)(i) of the Rome Statute.

RESEARCH METHODS

The study uses doctrinal legal research, supplemented by secondary literature, to identify normative gaps and propose reform.¹² An empirical study was set aside because the Court’s limited case law makes

⁴Rome Statute of the International Criminal Court, art. 69, adopted July 17, 1998, entered into force July 1, 2002 (hereafter Rome Statute), <https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>.

⁵International Criminal Court, *Rules of Procedure and Evidence*, ICC-PIOS-LT-03-006/24_Eng (The Hague: International Criminal Court, 2024) (hereafter ICC RPE), rule 63(2); rules 63, 64, 79, 81, 87, and 88 have not been amended since their adoption. See also Rome Statute, art. 64(9)(a) (the Trial Chamber has the power to “[r]ule on the admissibility or relevance of evidence”); *Yekatom and Ngaissona*, Trial Judgment, para. 133. On the extension of this power beyond its literal object, see note 20.

⁶Office of the United Nations High Commissioner for Human Rights and Human Rights Center, UC Berkeley School of Law, *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*, HR/PUB/20/2 (New York and Geneva: United Nations, 2022), https://www.ohchr.org/sites/default/files/documents/publications/OHCHR_BerkeleyProtocol.pdf. The Protocol is a joint institutional publication and names no individual authors; its Coordinating Committee and other contributors are listed at vii.

⁷Sofia Aalto-Setälä et al., *Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals* (Leiden: Kalshoven-Gieskes Forum, Leiden University, 2022), <https://leiden-guidelines.com/guidelines/>. The document bears no printed date; 2022 is the date of the published file.

⁸Bobby Chesney and Danielle Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” *California Law Review* 107 (2019): 1785, <https://doi.org/10.15779/Z38RV0D15J> (“Hence what we call the liar’s dividend: this dividend flows, perversely, in proportion to success in educating the public about the dangers of deep fakes”); see also Yvonne McDermott, Stephen Sharp Queener, and Basile Simon, “Old Doubts, New Doubts: Evaluating Digital Open Source Imagery in the Courtroom,” *Opinio Juris*, June 26, 2024, <https://opiniojuris.org/2024/06/26/old-doubts-new-doubts-evaluating-digital-open-source-imagery-in-the-courtroom/>.

⁹Belkis Wille, “Video Unavailable”: *Social Media Platforms Remove Evidence of War Crimes* (Human Rights Watch, September 10, 2020), <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes>.

¹⁰On OTPLink (launched May 2023) and Project Harmony, see Tal Mimran and Lior Weinstein, “Digitalize It: Digital Evidence at the ICC,” *Articles of War*, August 14, 2023, <https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/>. See also International Criminal Court, Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute* (The Hague: International Criminal Court, December 2025), para. 29 (digital evidence) and n. 66 (OTPLink); its publication is welcomed in Assembly of States Parties, Resolution ICC-ASP/24/Res.6 (December 5, 2025), para. 71.

¹¹This article introduces the term “authentication deficit” to denote the absence of binding standards for evaluating the trustworthiness of digitally derived evidence once admitted. The term is preferred over broader alternatives such as “evidentiary gap” because the Rome Statute’s free-proof system does not exclude OSINT from admission.

¹²Terry Hutchinson and Nigel Duncan, “Defining and Describing What We Do: Doctrinal Legal Research,” *Deakin Law Review* 17, no. 1 (2012): 101, <https://doi.org/10.21153/dlr2012vol17no1art70>.

quantitative analysis premature, and comparative material is used as a source of ideas rather than of authority, in keeping with Rule 63(5). The primary sources are the Rome Statute (Articles 21, 51–52, 64, 66–69), the Rules of Procedure and Evidence (Rules 63–64, 69 bis, 79, 81 and 87–88) and six ICC cases: Al Mahdi (ICC-01/12-01/15), Al-Werfalli (ICC-01/11-01/17), Bemba (ICC-01/05-01/08), Ongwen (ICC-02/04-01/15), Al Hassan (ICC-01/12-01/18) and Yekatom and Ngaïssona (ICC-01/14-01/18). The Yekatom judgment was read in its full public redacted version, together with the January 2019 e-Court Protocol filed in that case, and the study also examines Trial Chamber III's decision of 28 September 2026 amending the e-Court Protocol applicable in Duterte (ICC-01/21-01/25). Comparative sources include decisions of the Special Tribunal for Lebanon and the European Court of Human Rights, the United States Federal Rules of Evidence, the EU eIDAS Regulation, the UNCITRAL Model Law on Electronic Commerce, the German Strafprozessordnung and ISO/IEC 27037 and 27042.

The analysis maps the existing architecture, identifies the doctrinal gaps, tests the proposed framework against the Statute's fair-trial guarantees and the principal counterarguments, and situates the proposal within the reform literature. It is limited to publicly available decisions.

RESULTS AND DISCUSSION

Free Proof and the Doctrinal Status of Authentication

A proposal to introduce authentication standards at the ICC must first meet the objection that authentication is the wrong doctrinal category. Authentication as a discrete evidentiary gate is a common-law construct, codified in the United States in Federal Rules of Evidence 901 and 902, and Rule 63(5) of the ICC Rules provides that Chambers "shall not apply national laws governing evidence, other than in accordance with article 21."¹³ The objection does not hold. Rule 63(5) excludes the application of national rules of evidence as such, not comparative reference or the use of analytical concepts shared across legal systems. Authenticity, moreover, already operates in ICC practice. In the second warrant of arrest for Al-Werfalli, the Pre-Trial Chamber referred to "sufficient indicia of authenticity,"¹⁴ and the Yekatom Chamber distinguished authenticity from reliability, finding that Defence submissions framed as challenges to the authenticity of call data records in fact concerned "whether the Prosecution CDR Material can be deemed sufficiently reliable or accurate."¹⁵

Article 69(3) permits the parties to submit evidence relevant to the case, and Article 69(4) allows the Court to rule on relevance or admissibility, taking into account probative value and prejudice.¹⁶ Practice treats this as a three-tiered test of relevance, probative value (assessed by reference to reliability, trustworthiness, credibility and authenticity) and prejudice.¹⁷ In Bemba, Trial Chamber III admitted the Prosecution's materials *prima facie* and deferred "the Chamber's future determination of the probative value to be given to the evidence" to the end of the case; the Appeals Chamber held that admitting every listed item on that basis, without individual assessment or reasons, fell outside the Court's legal framework.¹⁸ The Yekatom Chamber, by contrast, adopted a "submission approach," declining to rule on the admissibility of individual items and assessing all 19,590 of them freely under Rule 63(2) in its judgment.¹⁹ At the ICC, then, authenticity is not a gatekeeping category but part of reliability, which feeds into probative value and weight. This article uses the term in that internal sense, to denote whether a digital item is what it purports to be.

¹³ICC RPE, rule 63(5); Rome Statute, art. 21. On authentication in United States federal practice, see Fed. R. Evid. 901–902.

¹⁴*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, ICC-01/11-01/17-13, Second Warrant of Arrest (Pre-Trial Chamber I, July 4, 2018), para. 18, https://icc-cpi.int/CourtRecords/CR2018_03552.PDF. The video concerned the killings of January 24, 2018, at the Bi'at al-Radwan Mosque.

¹⁵*Yekatom and Ngaïssona*, Trial Judgment, para. 182.

¹⁶Rome Statute, art. 69(3)–(4).

¹⁷Mimran and Weinstein, "Digitalize It."

¹⁸*Prosecutor v. Bemba Gombo*, ICC-01/05-01/08-1022, Decision on the Admission into Evidence of Materials Contained in the Prosecution's List of Evidence (Trial Chamber III, November 19, 2010) (hereafter *Bemba*, Admission Decision), para. 9 (Majority; Judge Ozaki dissenting), reversed in *Prosecutor v. Bemba Gombo*, ICC-01/05-01/08-1386 OA 5 OA 6, Judgment on the Appeals of Mr Jean-Pierre Bemba Gombo and the Prosecutor against the Decision of Trial Chamber III Entitled "Decision on the Admission into Evidence of Materials Contained in the Prosecution's List of Evidence" (Appeals Chamber, May 3, 2011) (hereafter *Bemba*, Appeals Judgment), para. 2 ("By admitting into evidence all the items on the Revised List of Evidence based on a 'prima facie finding of admissibility,' without an item-by-item evaluation or giving reasons, the Trial Chamber acted outside the legal framework of the Court"). William A. Schabas, *The International Criminal Court: A Commentary on the Rome Statute*, 2nd ed. (Oxford: Oxford University Press, 2016), 1048, describes the appeal as finding that the burden of proof had been reversed; the Appeals Chamber in fact found that argument "misconceived" (para. 72) and upheld only a narrower complaint (para. 73).

¹⁹*Yekatom and Ngaïssona*, Trial Judgment, paras. 132–33.

Two textual difficulties arise. Read literally, Rule 63(2) confers the power of free assessment “in order to determine [the evidence’s] relevance or admissibility,” the very stage this article treats as unproblematic. Yet the Yekatom Chamber, having declined to rule on admissibility at all, recorded that it had “assessed freely all evidence in accordance with Rule 63(2).”²⁰ The provision has thus become a general power of evaluation without amendment, justification or criteria, which is itself an instance of the deficit discussed here.

The second difficulty concerns Rule 63(4), under which “[a] Chamber shall not impose a legal requirement that corroboration is required in order to prove any crime within the jurisdiction of the Court.”²¹ The first Yekatom principle discussed below, that authorship cannot be established from platform material alone, comes close to a corroboration requirement, but the two can be reconciled. Rule 63(4) forbids corroboration as a condition of *proving a crime*, whereas the Chamber’s holding concerns what a class of material can establish about *authorship* on its own. The framework proposed below respects that distinction by attaching consequences to the presence of integrity guarantees, never to the absence of a second source.

The existing framework therefore tells judges which questions to ask but gives them no binding criteria for answering them when the evidence is born-digital, gathered by an unidentified person, possibly stripped of metadata by platform compression, and submitted years after it was captured. That absence is the authentication deficit. The only rule that refers to the authenticity of evidence, Rule 69 bis, inserted in 2023, allows a Trial Chamber to take judicial notice of the authenticity of documentary evidence already finally determined in other proceedings of the Court; it presupposes an authentication standard rather than supplying one.²² Nor can careful reasoning fill the gap. Article 21(2) permits the Court to apply principles as interpreted in its previous decisions but does not require it to do so, so even a treatment as careful as that in Yekatom binds no later Chamber.²³

The Arc of ICC Jurisprudence: Expanding Use Without Expanding Standards

In *Al Mahdi* (2016), the Prosecution used an interactive digital platform that combined open-source videos, photographs taken by citizens and journalists, and satellite imagery of the Timbuktu sites before and after their destruction.²⁴ The platform produced no authentication doctrine. As Zarnsky observes, because the defendant admitted guilt, it “was never challenged as a piece of evidence before the Court,” and its creators “were also not called upon to testify their methodology.”²⁵

The *Al-Werfalli* warrants are doctrinally more significant. Irving noted that the first, of August 2017, gave no indication of the methods used to verify the videos on which it rested (see note 2), and the warrant itself describes no verification method.²⁶ The second, of 4 July 2018, found sufficient indicia of authenticity in a video of killings at a mosque on the strength of an independent expert report and a witness who confirmed the location (see note 14). The standard for an arrest warrant is, however, far lower than that for conviction, and the Pre-Trial Chamber terminated the proceedings on 15 June 2022, having found *Al-Werfalli*’s death established partly on the basis of social media material.²⁷ The authentication standard applied in the warrants was never tested adversarially.

²⁰*Bemba*, Admission Decision, para. 9; *Yekatom and Ngaïssona*, Trial Judgment, paras. 132–33. Neither decision addresses the tension between the literal object of rule 63(2) and the use made of it.

²¹ICC RPE, rule 63(4): “Without prejudice to article 66, paragraph 3, a Chamber shall not impose a legal requirement that corroboration is required in order to prove any crime within the jurisdiction of the Court, in particular, crimes of sexual violence.” On the procedure for raising questions of relevance or admissibility, see rule 64.

²²ICC RPE, rule 69 bis(1)–(2), inserted by Assembly of States Parties, Resolution ICC-ASP/22/Res.1, “Resolution on Amendments to the Rules of Procedure and Evidence of the International Criminal Court” (December 13, 2023). Rule 69 bis(4) allows a party to challenge the authenticity so noticed by referring to contradicting evidence or introducing evidence to the contrary.

²³Rome Statute, art. 21(2): “The Court may apply principles and rules of law as interpreted in its previous decisions.” The permissive “may” is what leaves the Yekatom principles without purchase on a later Chamber.

²⁴*Prosecutor v. Al Faqi Al Mahdi*, ICC-01/12-01/15-171, Judgment and Sentence (Trial Chamber VIII, September 27, 2016), paras. 7 and 27–30 (trial held August 22–24, 2016; admission of guilt); SITU Research, “ICC Digital Platform: Timbuktu, Mali,” accessed June 2, 2026, <https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali>. The judgment refers to video and photographic material only in its footnotes and does not discuss the platform.

²⁵Sarah Zarnsky, “Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law,” *Journal of International Criminal Justice* 19, no. 1 (2021): 215, <https://doi.org/10.1093/jicj/mqab048>.

²⁶*Al-Werfalli*, First Warrant, paras. 3 and 11–22. The only indication bearing on verification is a reference to data suggesting that one video was uploaded in the Benghazi area (para. 22).

²⁷*Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, ICC-01/11-01/17-24, Decision Terminating Proceedings (Pre-Trial Chamber I, June 15, 2022), paras. 4–5 (death established having considered “witness statements, photographs, and social media material”).

Al Hassan (2024) is the most instructive case. The trial is widely associated with a three-dimensional digital reconstruction of Timbuktu, and the Chamber convicted Mr Al Hassan of the crime against humanity of persecution on religious grounds,²⁸ yet the judgment does not discuss the reconstruction platform. It does treat at length, under dedicated headings, the authentication of handwritten Islamic Police reports, Islamic Court judgments and Hesbah reports, assessed with the help of a handwriting expert and an expert in document analysis whose methodology a Defence expert contested.²⁹ Contested video, by contrast, is addressed in a single footnote, where the Chamber found videos of the demolitions reliable by combining a witness's identification of the filming locations, an expert's geolocation analysis, another expert's metadata analysis and other authenticated videos of similar scenes.³⁰ For paper the Chamber set out a structured apparatus; for born-digital material it assembled, for the occasion, criteria that are sound in themselves but bind no later Chamber. Zarnsky adds a distributive dimension: where a private organisation donates technology and expertise to the prosecution but not to the defence, the resulting inequality of arms may engage the prejudice limb of Article 69(4).³¹

Yekatom and Ngaïssona (2025): Four Principles and One Caution

The judgment, now under appeal by the Prosecution and both Defence teams, is the Court's most extensive engagement with digitally derived evidence to date.³² Its treatment of Facebook material and call data records yields four principles and a caution.

Principle One: author testimony. Without a statement or testimony from a witness who took part in a Facebook exchange or wrote a post, the Chamber "cannot conclusively determine who effectively engaged in an exchange or who authored a specific post, based solely on the Facebook Material." In the absence of expert evidence, it likewise could not rely solely on Facebook IP addresses or logs to establish where a person was.³³ Social media content is thus not self-authenticating as to authorship, even where the platform itself supplied the account data.

Principle Two: no blanket presumption of unreliability. The Chamber declined to presume that "all messages are misinformation unless proven otherwise," preferring to determine reliability "on a case-by-case basis in light of the available evidence."³⁴ This is, in substance, a judicial answer to the scepticism that the liar's dividend encourages.

Principle Three: provenance through competent authorities. The Irish authorities had secured the Facebook material in response to requests for assistance and transmitted it to the Prosecution. The Chamber had "no reason to doubt" that it received what the authorities had obtained, held the material "overall authentic," and found it unnecessary to decide whether it was "self-authenticating." Allegations of alteration unsupported by any indicium were "mere submissions" that "are speculative."³⁵ The call data records, supplied through requests for assistance by the network operators Moov, Orange, MTN and Telecel, were treated in the same way: the Chamber saw "no reason to doubt" either their

²⁸*Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud*, ICC-01/12-01/18-2594-Red, Judgment (Trial Chamber X, June 26, 2024) (hereafter *Al Hassan*, Judgment), Disposition, Count 13 (guilty, by Majority, Judge Mindua dissenting, of the crime against humanity of persecution on religious grounds under art. 7(1)(h)). The judgment makes no reference to the digital reconstruction platform. For the platform itself, see SITU Research, "ICC Digital Platform and the Al Hassan Case," accessed June 2, 2026, <https://situ.nyc/research/projects/icc-digital-platform-and-the-al-hassan-case>; Anastasiia Liulina, "Evidentiary Digital Platforms: What the Al Mahdi and Al Hassan Cases Teach Us about Presenting Voluminous Digital Data," *International Criminal Law Review* 25, no. 5 (2025): 851 (the developers of the platforms were not called to testify in either case), 863, <https://doi.org/10.1163/15718123-bja10235>.

²⁹*Al Hassan*, Judgment, paras. 341–42 (Islamic Police reports), 345 (Islamic Court judgments), and 351 (Hesbah reports), under the headings on the authentication of each category, with expert evidence from a handwriting expert (P-0620) and an expert in document analysis (P-0621), and a contrary methodological critique from the Defence expert Nikolaos Kalantzis (D-0501).

³⁰*Al Hassan*, Judgment, para. 1031 and n. 3458 (noting that not all videos were shown to or authenticated by a witness, and relying on the evidence of P-0150, the geolocation analysis of P-0193, the metadata analysis of P-0075, and other authenticated videos).

³¹Zarnsky, "Why Seeing," 216, 220–22.

³²See Common Legal Representatives of the Victims of the Other Crimes, *Prosecutor v. Yekatom and Ngaïssona*, ICC-01/14-01/18-2884-Red, Consolidated Victims' Response to the Prosecution and Defence Appeals of the Judgment and Sentence against Mr Alfred Yekatom and Patrice-Edouard Ngaïssona (March 23, 2026), para. 1 and nn. 1–3. The only ground summarised there that touches the digital material concerns the weight given to call data records in assessing a Defence witness (paras. 90–92).

³³*Yekatom and Ngaïssona*, Trial Judgment, para. 151.

³⁴*Yekatom and Ngaïssona*, Trial Judgment, para. 154. The Chamber added that, absent a statement or testimony from a participant in the exchange or the author of a post, "the related Facebook Material has little probative value" (para. 154). Irving and Rewald, "Digital Evidence Before the ICC," read the passage as "a stance against the digital-era harm of the liar's dividend."

³⁵*Yekatom and Ngaïssona*, Trial Judgment, paras. 147–49; the passage on "mere submissions" is at para. 148 ("mere submissions on any alleged alteration of such material are speculative").

correspondence with what had been requested or “the validity of the respective chains of custody as reflected in the metadata.”³⁶

Principle Four: automated business records. Call data records, generated automatically in the ordinary course of business, “can be generally presumed reliable.” The Chamber gave four reasons: the information is generated automatically; its accuracy serves the networks’ commercial interests; it was stored and transmitted without evidence of tampering; and persons with sufficient knowledge or technical expertise were involved in producing it. The presumption “can be rebutted by the parties, for instance by showing specific examples of irregularities in the collection, storing, formatting and/or transmission of the evidence.”³⁷

The caution. The Chamber nonetheless held that “generally the probative value of the CDR and cell site items is low,” that it would rely on them “if at all” within its holistic approach, and that call data records alone cannot attribute a telephone number to an individual, for which “additional extrinsic evidence is necessary.”³⁸ An inference of authenticity is not an inference of probative weight, and the framework proposed below is drafted with that distinction in mind.

None of the material assessed in Yekatom was gathered by citizens: the Facebook records came from a platform through a national authority, and the call data records from licensed network operators. No ICC judgment has yet set out general criteria for authenticating citizen-gathered open-source material, and the reasons the Chamber gave for presuming call data records reliable were institutional ones that an activist recording in a conflict zone cannot offer. The approach proposed here replaces the institutional guarantee with a technical one, cryptographic hashing, and a procedural one, documented chain of custody. For citizen evidence, the hash performs the function that untampered storage and transmission performed for the call data records, within the limits set by the Chamber’s caution.

What the Soft-Law Instruments Require, and Where They Stop

The Berkeley Protocol is the more technical of the two instruments. Hash values, it explains, “are a unique form of digital identification that confirm, through the use of cryptography, that the content collected is unique and has not been modified since the time of collection,” and “[a]t the point of collection, open source investigators should manually add — or the collection tool should automatically add — a hash value.”³⁹ The Protocol defines chain of custody as “the chronological documentation of the sequence of custodians of a piece of information or evidence, and documentation of the control, date and time, transfer, analysis and disposition of any such evidence,”⁴⁰ and directs that, where removal of content is likely, “the most reliable known version of the content should be collected.”⁴¹

The Leiden Guidelines approach the problem from the courtroom. Guideline A6 provides that videos “can be admitted into evidence if relevance and prima facie authenticity is demonstrated by providing information about the date, the location, the events depicted, the author, the source, and/or the chain of custody.” Guideline E4 provides that the reliability of call sequence tables depends on the authenticity of the underlying call data records and must be proven through expert witnesses; its commentary adds that “the Court must be satisfied with the reliability of the underlying CDRs” and that the tendering party should provide contextual evidence on “the creation, storage, and retrieval of the CDRs.”⁴²

These instruments are of high quality. Guideline E4, drafted before Yekatom, anticipates much of what Trial Chamber V went on to hold about call data records. Neither instrument, however, provides what a Chamber confronted with citizen-gathered material needs. The Berkeley Protocol’s hashing provision is good practice addressed to investigators, and it is candid that a hash establishes only that content “has not been modified since the time of collection,” which is considerably less than authenticity. The Leiden Guidelines do not address cryptographic verification at all. Neither binds any Chamber, and under Article 21(2) a Chamber persuaded by them creates no obligation for the next. The gap is one of normative force rather than of knowledge.

³⁶Yekatom and Ngaïssona, Trial Judgment, paras. 161 and 182.

³⁷Yekatom and Ngaïssona, Trial Judgment, para. 183; on the automatic generation of call data records in the ordinary course of business, see para. 170.

³⁸Yekatom and Ngaïssona, Trial Judgment, paras. 186 and 188.

³⁹Berkeley Protocol, para. 155(b) and (h).

⁴⁰Berkeley Protocol, para. 167.

⁴¹Berkeley Protocol, para. 153.

⁴²Aalto-Setälä et al., *Leiden Guidelines*, Guideline A1 and commentary (10), Guideline A6 (16), and Guideline E4 and commentary (45–46).

Civil-Society Practice and Comparative Authentication Regimes

Civil-society verification and preservation practice has become sophisticated, and it is consistent with ISO/IEC 27037 and 27042, which set out guidelines for the collection and preservation of digital evidence and for its analysis and interpretation, respectively; both are suitable reference points for a binding framework.⁴³ Because provenance technologies are still evolving, the framework relies on functional criteria rather than on any single specification. Cryptographic authentication at capture has already reached the Office of the Prosecutor. In June 2022, Starling Lab and Hala Systems submitted an Article 15 communication on attacks on schools in Kharkiv, Ukraine, using cryptographically signed web archives whose files and metadata were registered and preserved on decentralised protocols.⁴⁴

Comparative regimes offer qualified guidance. The 2017 amendments that created Federal Rules of Evidence 902(13) and 902(14) permit the self-authentication of electronic records through certification by a qualified person, and the Committee Note to the 2017 amendment observes that such data are ordinarily authenticated by hash value.⁴⁵ Under eIDAS, qualified electronic seals and qualified electronic time stamps enjoy a presumption of integrity.⁴⁶ The UNCITRAL Model Law took a third path: a data message is not to be denied admissibility solely because it is in electronic form, and is to be given due evidential weight, without any presumption.⁴⁷ The presumption-based model thus originates in the law of trust services rather than in rules of criminal proof, which suggests adopting the certification mechanism of Rule 902(14) and the non-discrimination principle of the UNCITRAL Model Law while declining to import the eIDAS presumption into criminal proceedings.

Germany offers the closest civil-law analogue to Rule 63(2). Section 261 of the Strafprozessordnung, headed “Principle of judge’s free evaluation of evidence,” leaves it to the court “to decide on the result of the taking of evidence at its discretion and conviction based on the entire content of the hearing,”⁴⁸ yet the German system has long combined free evaluation with detailed procedural rules on how evidence is obtained, recorded and introduced. Free evaluation concerns the conclusions a court may draw, not the process by which material reaches it, so the objection that structured standards are incompatible with free proof misidentifies what the freedom covers.

Comparative Perspectives: Other International Jurisdictions

The European Court of Human Rights has faced the problem in a form very close to the one confronting the ICC. In *Ukraine and the Netherlands v Russia*, the respondent Government argued that the applicants had relied on “dubious digital material and reports from ‘so-called’ citizen journalists, such as Bellingcat and InformNapalm,” that such material “was susceptible to manufacture or manipulation,” and that circulation on social media “stripped the material of data necessary for proper forensic examination.”⁴⁹ This was, in effect, the liar’s dividend deployed as a litigation strategy, and the

⁴³International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (Geneva: ISO, 2012); International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27042:2015, Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence* (Geneva: ISO, 2015).

⁴⁴USC Shoah Foundation, “Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court,” June 10, 2022, <https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes>; Basile Simon, “New Evidence Techniques Document Bombed Ukrainian Schools for ICC,” *Starling Lab*, March 1, 2023, <https://starling.stanford.edu/case-studies/submission-icc-schools-kharkiv-evidence-case-study/> (web archives produced as cryptographically signed WACZ files; a second submission followed on January 17, 2023).

⁴⁵Fed. R. Evid. 902(13) (records generated by an electronic process or system) and 902(14) (data copied from an electronic device, storage medium, or file), added by the 2017 amendments effective December 1, 2017, accessed June 2, 2026, https://www.law.cornell.edu/rules/fre/rule_902. Both rules permit self-authentication through the certification of a qualified person. The Committee Note to the 2017 amendment observes that such data “are ordinarily authenticated by ‘hash value.’”

⁴⁶Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS), 2014 O.J. (L 257) 73, art. 35(2) (“A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked”) and art. 41(2) (“A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound”). Both paragraphs are unchanged in the consolidated version of October 18, 2024, following Regulation (EU) 2024/1183. eIDAS is a trust-services regulation and is not specific to criminal proof.

⁴⁷United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with Additional Article 5 bis as Adopted in 1998* (New York: United Nations, 1999) (hereafter UNCITRAL Model Law), art. 9 (admissibility and evidential weight of data messages).

⁴⁸Strafprozessordnung [StPO] [Code of Criminal Procedure], § 261, in the version published on April 7, 1987, as last amended by Article 2 of the Act of July 17, 2025, trans. Brian Duffett and Monika Ebinger, updated by Kathleen Müller-Rostin and Iyamide Mahdi, rev. Ute Reusch (Federal Ministry of Justice and Consumer Protection and Federal Office of Justice), https://www.gesetze-im-internet.de/englisch_stpo/.

⁴⁹*Ukraine and the Netherlands v. Russia*, App. nos. 8019/16, 43800/14, and 28525/20, Decision (Grand Chamber, European Court of Human Rights, November 30, 2022), para. 409.

Grand Chamber rejected it. Finding the authors of the reports “credible and serious,” it held that there were “no grounds upon which to reject the evidence of these reports as a category of evidence,” and reserved the respondent’s specific criticisms for consideration if and when weight came to be placed on particular reports.⁵⁰ The Yekatom Chamber adopted the same approach less than three years later, in a different system.

The Special Tribunal for Lebanon illustrates the limits of integrity guarantees. The evidence against all four accused in Ayyash was circumstantial, resting on “the cell activations of their attributed personal and network mobiles,” and the conviction of Mr Ayyash depended on connecting those activations with the movements of former Lebanese Prime Minister Rafik Hariri through the analysis of a single mobile, Red 741.⁵¹ The records were business records of licensed operators, of the kind the Yekatom Chamber would later presume reliable, and the contested issues arose only after integrity had been settled: whether a handset could be attributed to a person, and that person to an act. As the Yekatom Chamber’s caution also shows (see note 38), integrity is a precondition for probative reasoning rather than a substitute for it.

These examples point towards a convergence in treating digital evidence, including citizen-gathered material, as a legitimate part of the record, combined with a persistent lack of systematic authentication standards. The binding regimes that do exist, such as Federal Rules of Evidence 902(13)–(14) and eIDAS, are domestic or regional, and eIDAS was not designed for criminal proof. As the permanent international criminal court, the ICC is well placed to fill that gap.

The Epistemic Foundation: Machine Testimony and Digital Trust

A framework for evaluating digital evidence needs an account of why such evidence deserves trust. Roth’s analysis of machine testimony provides one, although her subject is machine conveyances such as breath analysers, whereas a citizen’s video is a human observation recorded by a device. The two can be separated. What a recording device asserts is that light of a certain description reached a sensor at a particular time and place; the claim that the images depict a crime is made by the person who recorded or tendered them, and integrity guarantees speak only to the first assertion. Machine conveyances, Roth argues, present dangers comparable to the credibility problems of human witnesses: what she calls falsehood by design, inarticulateness and analytical error. Rather than broad exclusion, she advocates layered safeguards, including pretrial disclosure and access to source code, authentication and reliability standards, and mechanisms for impeachment.⁵²

Cryptographic hashing does not show that a video depicts what it purports to depict, only that the file has not changed since the hash was generated. Chain-of-custody documentation does not show where a photograph was taken; it records the path the file has travelled. Both are necessary and neither is sufficient, as the Yekatom Chamber’s treatment of call data records illustrates: it presumed them reliable and still gave them little probative value. What these mechanisms provide is the precondition for meaningful evaluation, since they allow the Chamber and the defence to examine the process rather than simply accept its output.

The Proposed Framework: Six Elements and the Instruments That Can Carry Them

The choice of legal instrument matters as much as the content of the six elements, and no single instrument can carry them all.⁵³ An amendment to the Rules under Article 51(2) requires a two-thirds majority of the Assembly of States Parties; it carries the greatest authority and faces the greatest political difficulty. Provisional Rules under Article 51(3) are drawn up by the judges, by a two-thirds majority,

⁵⁰*Ukraine and the Netherlands v. Russia*, paras. 472–73. For commentary, see Eliot Higgins, “How Open Source Evidence Was Upheld in a Human Rights Court,” *Bellingcat*, March 28, 2023, <https://bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court>.

⁵¹*Prosecutor v. Salim Jamil Ayyash et al.*, STL-11-01/T/TC, Judgment (Trial Chamber, Special Tribunal for Lebanon, August 18, 2020), Summary, paras. 31–34.

⁵²Andrea Roth, “Machine Testimony,” *Yale Law Journal* 126, no. 7 (2017): 1972, 1989–93 (“falsehood by design,” “inarticulateness,” and “analytical error”), 2022–39 (testimonial safeguards), <https://www.yalelawjournal.org/article/machine-testimony>.

⁵³Rome Statute, art. 51(1)–(2) (the Rules of Procedure and Evidence enter into force upon adoption by a two-thirds majority of the members of the Assembly of States Parties, as do amendments); art. 51(3) (in urgent cases where the Rules do not provide for a specific situation, the judges may by a two-thirds majority draw up provisional Rules pending the next session of the Assembly); art. 52(1) (“The judges shall, in accordance with this Statute and the Rules of Procedure and Evidence, adopt, by an absolute majority, the Regulations of the Court necessary for its routine functioning”); and art. 52(3) (Regulations are circulated to States Parties and “[i]f within six months there are no objections from a majority of States Parties, they shall remain in force”).

in urgent cases where the Rules do not provide for a specific situation, and apply until the Assembly adopts, amends or rejects them. Regulations under Article 52(1) are adopted by an absolute majority of the judges but are confined to what is necessary for the Court's routine functioning, so they must be procedural in character; under Article 52(3), moreover, a Regulation remains in force only if a majority of States Parties does not object within six months. The fourth instrument, the e-Court Protocol, is the least conspicuous and probably the most useful. It governs how evidence is formatted, how metadata is recorded and how material is transmitted, and Braga da Silva identifies it as the appropriate place for metadata reform.⁵⁴ The Protocol is made under regulation 26(1) of the Regulations of the Court and updated through a consultation coordinated by the Registry; its text provides for no vote of the Assembly.⁵⁵ The version filed in Yekatom and Ngaïssona in January 2019 already requires, for electronic items, a "Digital Signature" field holding a cryptographic code "that may be used to verify authenticity of evidence, if authenticity is challenged," fixed at the MD5 standard, and a "Chain of Custody" field listing in chronological order every person or entity that has had custody of the item.⁵⁶ These fields serve record-keeping rather than evaluation: as far as the text shows, nothing turns on whether they are completed, and the hash is generated by the submitting participant rather than at the moment of capture. The Protocol can also change quickly. In Duterte, Trial Chamber III amended the e-Court Protocol applicable in that case at the parties' request in September 2026, adding a URL metadata field for open-source evidence but refusing a Defence request for an "Expert Verification" field, which would in effect have required expert verification reports for all open-source and user-generated evidence and "could well have the effect of causing a needless delay."⁵⁷ A Chamber can therefore amend the Protocol by a single decision, but without a general standard, verification is decided case by case. The analysis below is based on the January 2019 text.

The framework is therefore distributed across several instruments. Elements One, Two and Four concern how material is captured, documented, transmitted and disclosed, and belong in the e-Court Protocol, supplemented where necessary by a Regulation under Article 52. Element Three is an inference rule and, however modestly framed, forms part of the law of evidence; it belongs in a provisional Rule under Article 51(3) or, while practice develops, in the Chambers Practice Manual,⁵⁸ with an amendment under Article 51(2) as the eventual goal. Element Five belongs in a Regulation under Article 52 or, failing that, in a provisional Rule (see below), and Element Six, a best-evidence requirement coupled with a rule of non-exclusion, can accompany any of the others. Table 1 summarises the allocation.

Element One: cryptographic hashing at capture, independently anchored. Citizen-gathered digital evidence should be accompanied by a cryptographic hash generated at or near the time of capture, using an algorithm recognised by the Court and consistent with ISO/IEC 27037, as the Berkeley Protocol already recommends. Because the e-Court Protocol specifies MD5, an algorithm no longer acceptable where collision resistance is required,⁵⁹ the algorithm should be specified by reference to a maintained external standard. Hashing alone, however, is not enough. A hash generated and held by the collector shows only that the file has not changed since the collector generated it, and amounts to little more than

⁵⁴Rafael Braga da Silva, "Updating the Authentication of Digital Evidence in the International Criminal Court," *International Criminal Law Review* 22, nos. 5–6 (2022): 950–64, <https://doi.org/10.1163/15718123-bja10083>.

⁵⁵*Prosecutor v. Yekatom and Ngaïssona*, ICC-01/14-01/18-64-Anx, Unified Technical Protocol ("E-court Protocol") for the Provision of Prosecution, Witness and Victims Information in Electronic Form (January 23, 2019) (hereafter E-court Protocol), paras. 1–2 (regulation 26(1) of the Regulations of the Court) and 37–39 (updating of the Protocol). See International Criminal Court, *Regulations of the Court*, ICC-BD/01-03-11 (as amended November 2, 2011), reg. 26(1) ("a reliable, secure, efficient electronic system") and 26(2) (the Registry to take into account "the need to ensure authenticity, accuracy, confidentiality and preservation of judicial records and material"); later consolidated versions were not consulted. See also Braga da Silva, "Updating the Authentication," 958–59, 963, on the deficiencies of the current system in recording the metadata of tendered files.

⁵⁶E-court Protocol, para. 32 (Table 1: fields "Digital Signature," applying to e-files and email only, "Chain of Custody," and "Source Identity"); para. 16 (the collecting party is responsible for preserving the original electronic items); paras. 29–30 (excerpts of video).

⁵⁷*Prosecutor v. Duterte*, ICC-01/21-01/25-508, Decision on the Prosecution's and the Defence's Requests to Amend the E-Court Protocol (Trial Chamber III, September 28, 2026), paras. 2–4, 8, 11, 13–14, and disposition. The Protocol had been adopted in the Chamber's Directions on the conduct of proceedings on a proposal by the Registry following consultations with the parties and participants (para. 2).

⁵⁸International Criminal Court, "ICC Judges Update Chambers Practice Manual to Include Guidelines on Dissenting and Separate Opinions," press release, July 13, 2023, <https://www.icc-cpi.int/news/icc-judges-update-chambers-practice-manual-include-guidelines-dissenting-and-separate-opinions> (announcing the seventh edition and describing the Manual as "a living document which contains general recommendations and guidelines reflecting best practices identified by the judges"). Later editions have not been consulted.

⁵⁹E-court Protocol, para. 32 (Table 1, "Digital Signature": "The cryptographic hashing standard to be adopted is MD5"); S. Turner and L. Chen, *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*, RFC 6151 (Internet Engineering Task Force, March 2011), sec. 2 ("MD5 is no longer acceptable where collision resistance is required such as digital signatures"), <https://www.rfc-editor.org/rfc/rfc6151>.

the collector's own assertion, whereas the guarantees on which the Yekatom Chamber relied were all provided by third parties. Element One therefore requires the hash to be lodged, within a defined period after capture, with an entity independent of the collector, such as a qualified timestamping authority, a notarisation service, a distributed ledger, an institutional repository or the Court's own submission platform.⁶⁰ Where this is not done, the item is assessed on its merits under Element Six, without the benefit of the inference.⁶¹ The Starling Lab and Hala Systems communication shows what such anchoring looks like in practice (see note 44).

Element Two: standardised chain-of-custody documentation, disclosable and open to challenge. A standard-form record would follow the Berkeley Protocol's definition of chain of custody (see note 40) and the provenance indicators the Leiden Guidelines identify for the relevant type of material, and would be certified in the manner of Federal Rule 902(14); the existing "Chain of Custody" field in the Protocol is a natural starting point. The record should be disclosed to the defence as a matter of course, and the defence should be entitled to challenge the method it records and, where integrity is genuinely in issue, to examine the person who certified it. That entitlement responds to Roth's insistence that machine-derived evidence be open to impeachment, and it makes the inference under Element Three something the defence can contest rather than a presumption it must simply accept. The collector's identity is governed by Element Four.

Element Three: a permissive inference of authenticity, imposing no persuasive onus on the accused. This element requires the most careful formulation. Article 66 places the burden of proof on the Prosecutor, and Article 67(1)(i) guarantees that the accused shall not have imposed upon him or her any reversal of the burden of proof or any onus of rebuttal.⁶² The jurisprudence of the ad hoc tribunals cannot simply be transposed. The Čelebići Trial Chamber held that "[i]n every criminal act there is a presumption of sanity" and that the defence must be established "on the balance of probabilities,"⁶³ but the Defence in Ongwen submitted that the wording of Articles 66 and 67(1)(i) is "imperative and unequivocal" and that recourse to ad hoc jurisprudence is therefore unjustified.⁶⁴ Schabas observes that, because the Statute contains no typical reverse-onus provisions, the application of Article 67(1)(i) "to judge-made reverse onus provisions would seem to be the real purpose of the provision."⁶⁵ A framework intended for adoption by the judges falls squarely within that warning. In Bemba, the Appeals Chamber held that the burden in Article 67(1)(i) "refers to the burden on the Prosecutor to prove the case against the accused beyond reasonable doubt" and had not been shifted, but found that, because Rule 64(1) had not been given effect, the accused bore "the additional burden of disproving the admissibility of items on which the Chamber has already ruled."⁶⁶ A framework requiring the defence to disprove authenticity would therefore be incompatible with the Statute, and any proposal in this area must be tested against fair-trial guarantees rather than assumed to be procedurally neutral.⁶⁷

The answer lies in a distinction between two kinds of burden. Article 67(1)(i) prohibits imposing on the accused a *persuasive* burden, an obligation to prove or disprove a matter to any standard, with the risk of non-persuasion falling on the accused. It does not prohibit the ordinary requirement that a party advancing a contention identify some basis for it, which is simply a condition for the submission

⁶⁰This is where the present proposal departs from the *Berkeley Protocol*, which recommends hashing at the point of collection (see note 39) but not independent anchoring, and from the E-court Protocol, whose hash field is completed by the submitting participant (see note 56). The drafting would need to identify the acceptable anchoring mechanisms and the permissible interval between capture and anchoring.

⁶¹The requirement operates prospectively. Material preserved without contemporaneous hashing is neither excluded nor disadvantaged at admission and is assessed under the ordinary free-assessment power, but the inference under Element Three is unavailable to it. That difference tracks a genuine epistemic difference, and Element Six prevents it from hardening into a de facto exclusionary rule.

⁶²Rome Statute, arts. 66(2)–(3) and 67(1)(i) ("Not to have imposed on him or her any reversal of the burden of proof or any onus of rebuttal").

⁶³*Prosecutor v. Delalić et al.* ("Čelebići"), IT-96-21-T, Judgment (Trial Chamber, International Criminal Tribunal for the former Yugoslavia, November 16, 1998) (hereafter *Delalić et al.*, Judgment), paras. 1157, 1158, and 1172; see also para. 78, recording the Trial Chamber's earlier determination to the same effect.

⁶⁴*Prosecutor v. Ongwen*, ICC-02/04-01/15-1423, Defence Motion on the Burden and Standard of Proof for Defences under Article 31(1)(a) and (d) (Trial Chamber IX, January 28, 2019) (hereafter *Ongwen*, Defence Motion), paras. 13 and 15. The Single Judge granted leave to reply, noting that the burden and standard of proof for these defences was "an issue of first impression for the Court": *Prosecutor v. Ongwen*, ICC-02/04-01/15-1455, Decision on Defence Request for Leave to Reply to Prosecution and CLRV Responses on the Burden and Standard of Proof Applicable to Articles 31(1)(a) and (d) of the Rome Statute (Trial Chamber IX, February 19, 2019), para. 5.

⁶⁵Schabas, *International Criminal Court*, 1048–49 (commentary on art. 67(1)(i)), citing *Delalić et al.*, Judgment, paras. 1157–60.

⁶⁶*Bemba*, Appeals Judgment, paras. 72–73.

⁶⁷See generally María de Arcos Tejerizo, "Digital Evidence and Fair Trial Rights at the International Criminal Court," *Leiden Journal of International Law* 36, no. 3 (2023): 758 (chain of custody as key to prima facie authenticity), 764 (Chambers require digital material tendered from the bar table to be accompanied by information supporting its authenticity and reliability—a practice applied case by case, not a binding standard), <https://doi.org/10.1017/S0922156523000031>.

to be considered at all. The structure of the Statute and the Rules presupposes this distinction: grounds for excluding criminal responsibility under Article 31 are raised by the accused and notified under Rule 79 without any shift in the burden of proof, as the Defence in Ongwen took care to argue.⁶⁸

The distinction already operates at the Court. The Yekatom presumption for call data records yields to “specific examples of irregularities” (see note 37), and unsupported allegations of alteration were dismissed as speculative (see note 35). In Duterte, Trial Chamber III likewise made the Defence “primarily responsible to identify and raise” admissibility issues for individual items (see note 57). Under Article 21(2) these decisions bind no one and serve as illustrations rather than authority; the argument rests on the text and structure of the Statute. What the Yekatom Chamber required of a party seeking to displace its presumption was specificity, not proof.

The framework therefore creates no presumption of the kind Article 67(1)(i) forbids. Compliance with Elements One and Two permits, but does not require, a Chamber to infer that an item is what it purports to be. The inference concerns authenticity alone and has no bearing on probative value; it is displaced by any challenge that identifies a specific indication of irregularity; and the Prosecutor retains throughout the burden of proving every element of the offence beyond reasonable doubt. The accused is never required to prove anything, only to point to something specific, which the disclosure and challenge entitlement under Element Two makes possible. That entitlement is therefore a structural condition of this element’s legitimacy.

Element Four: integrated source-protection safeguards, tested against the rights of the accused. Article 68 requires the protection of victims and witnesses, yet open-source methodology depends on transparency and reproducibility, and those who gather the material are often in danger. This is also the only element that operates to the disadvantage of the accused. Withholding the identity of a person whose work has contributed to the evidentiary record engages Article 67(1)(e), the right to examine witnesses, and Article 67(2), which governs disclosure, and it is constrained by Article 68(1), under which protective measures must be “not prejudicial to or inconsistent with the rights of the accused and a fair and impartial trial.”⁶⁹ Setting those provisions aside would reproduce, to the detriment of the defence, an asymmetry of the kind Zarmisky identified (see note 31).

The element therefore proposes a tiered model with a fixed minimum. The method is always disclosed, including the capture tool, the anchoring mechanism and its timing, the chain-of-custody record and any processing applied. The collector’s identity may be withheld on application where the conditions of Article 68 are met, and the Protocol’s “Source Identity” field already allows a reference number “as authorized by the Chamber” to replace a protected person’s name (see note 56). Identity is then verified ex parte by the Chamber or the Registry’s Victims and Witnesses Unit, the defence may apply for counsel-only disclosure under the existing regime of protective measures, and the Chamber must take the withholding into account in assessing the weight the item can bear.⁷⁰ Attention to what the Berkeley Protocol calls the “mosaic effect, whereby public data, even when anonymized, may become vulnerable to reidentification if enough data sets containing similar or complementary information are released or combined,” would be mandatory,⁷¹ since redacting a name achieves nothing if the surrounding methodological detail identifies the collector. Anonymity thus comes at the cost of weight, not of the defence’s ability to test the process.

Element Five: reason-giving on existing soft-law instruments, within the limits of Article 21. The Berkeley Protocol and the Leiden Guidelines cannot be declared authoritative: Article 21 defines the Court’s sources exhaustively, and neither instrument is a treaty, a principle of international law or a

⁶⁸On the distinction, see *Ongwen*, Defence Motion, paras. 2 and 13 (the accused is “only under an evidential obligation to raise the defence,” while “the legal burden of proof remains at all times on the Prosecutor”); and Schabas, *International Criminal Court*, 641 (commentary on art. 31), suggesting that art. 67(1)(i) “may compel the less onerous requirement that the accused only raise a reasonable doubt.” ICC RPE, rule 79(1)(b), requires the defence to notify the Prosecutor of its intent to raise a ground for excluding criminal responsibility under art. 31(1), specifying the witnesses and other evidence relied on, and rule 79(3) provides that failure to give notice does not limit the right to raise it; the Rules say nothing about the burden of proof, which remains governed by arts. 66(2) and 67(1)(i).

⁶⁹Rome Statute, arts. 67(1)(e), 67(2), and 68(1). Article 68(1) requires that measures taken to protect victims and witnesses “shall not be prejudicial to or inconsistent with the rights of the accused and a fair and impartial trial.”

⁷⁰The mechanism draws on the existing protective-measures regime rather than creating a new one: ICC RPE, rules 81(3)–(4) and 87–88, the latter tied to the protection under art. 68 of victims, witnesses, and other persons at risk. The proposal is that the regime be applied to collectors of digitally derived material on the same terms as to other protected persons, and that the consequence for weight be stated expressly rather than left implicit.

⁷¹*Berkeley Protocol*, para. 28. On the risk to those who post such material, see Alexa Koenig, Jessica Peake, and Sylvanna Falcón, “Power and Humility in Open Source Investigations,” *Human Rights Review* 27, no. 1 (2026): 85, <https://doi.org/10.1007/s12142-026-00758-1>.

general principle derived from national legal systems.⁷² An instrument adopted by the judges can, however, guide the exercise of a discretion already conferred. Element Five provides that a Chamber evaluating digitally derived evidence shall have regard to those instruments as the prevailing technical standards in the field and shall give reasons when it departs from them. This creates no new source of law and does not alter what may be proved, by whom or to what standard, so it can be placed in a Regulation under Article 52; should that characterisation be rejected, Element Five can be adopted together with Element Three as a provisional Rule under Article 51(3).

Element Six: best evidence reasonably obtainable, operating as a safety valve. The first limb is a genuine requirement. A party tendering digitally derived evidence should tender the most complete and least degraded version reasonably available to it, such as the original file rather than a re-encoded copy, and should explain why nothing better was available when it tenders something less. This reflects the Berkeley Protocol's instruction to collect "the most reliable known version of the content" (see note 41), the e-Court Protocol's rule that an excerpt of a video may be provided only in exceptional circumstances and must display its original time-coding (see note 56), and Leiden Guideline A1, under which a party tendering excerpts should "clearly indicate whether the full footage was available and who extracted the segments of the video" (see note 42). The UNCITRAL Model Law expresses the same idea, providing that a data message is not to be denied admissibility on the ground that it is not in its original form "if it is the best evidence that the person adducing it could reasonably be expected to obtain."⁷³ The second limb is the safety valve itself: material that does not satisfy Elements One or Two, or the first limb of this element, remains fully admissible and is assessed on its merits under the ordinary power of free assessment. The framework never requires exclusion.

Table 1 Proposed Framework for the Evaluation of Digitally Derived Evidence at the ICC

No	Element	Content and Legal Basis
1	Cryptographic Hashing, Independently Anchored	Hash generated at or near capture with a recognised algorithm, consistent with ISO/IEC 27037 and the Berkeley Protocol (see notes 43 and 39), and lodged within a defined period with an entity independent of the collector (see note 60). Prospective operation (see note 61). <i>Instrument:</i> e-Court Protocol ("Digital Signature" field); Regulation under art. 52.
2	Chain-of-Custody Record, Disclosable	Standard-form record following the Berkeley Protocol's definition (see note 40) and the Leiden provenance indicators (see note 42), certified as under Fed. R. Evid. 902(14) (see note 45). Disclosed as of course; method open to challenge; certifier examinable where integrity is in issue. <i>Instrument:</i> e-Court Protocol ("Chain of Custody" field); Regulation under art. 52.
3	Permissive Inference of Authenticity	Compliance permits, but does not compel, an inference that the item is what it purports to be. Bears on authenticity only, not on weight (see note 38). Displaced by any specific indication of irregularity. Evidential, not persuasive, burden, compatible with arts. 66 and 67(1)(i) (see notes 62 and 68); cf. Yekatom (see note 37). <i>Instrument:</i> Provisional Rule under art. 51(3); Chambers Practice Manual in the interim.

⁷²Rome Statute, art. 21(1). On the limits of what an instrument adopted by the judges may do, see art. 52(1) and note 53 above.

⁷³UNCITRAL Model Law, art. 9(1)(b); see also art. 9(2), which directs that evidential weight have regard to "the reliability of the manner in which the integrity of the information was maintained." Article 9 concerns admissibility and evidential weight rather than functional equivalence (arts. 6–8); the safety valve in Element Six reflects the non-discrimination rule in art. 9(1).

No	Element	Content and Legal Basis
4	Source-Protection Safeguards	Method always disclosed; identity withheld only on application under art. 68, with ex parte verification, possible counsel-only disclosure and an express consequence for weight (see note 70). Tested against arts. 67(1)(e), 67(2) and 68(1) (see note 69). Mandatory mosaic-effect analysis (see note 71). <i>Instrument:</i> e-Court Protocol (“Source Identity” field); Regulation under art. 52.
5	Reason-Giving on Soft-Law Standards	Chambers to have regard to the Berkeley Protocol and the Leiden Guidelines and to give reasons for departing from them. No new source of law under art. 21 (see note 72). <i>Instrument:</i> Regulation under art. 52, or art. 51(3) together with Element Three.
6	Best Evidence Reasonably Obtainable	Most complete and least degraded version reasonably obtainable, or an explanation why not (see note 41). Non-compliant material remains admissible and is assessed on its merits; no exclusion (see note 73). <i>Instrument:</i> Any of the instruments above.

Anticipating Objections

Four objections call for a response. The first is that the drafters of the Statute deliberately chose evidentiary minimalism, so that introducing standards would betray that choice or would appear to judges from other traditions as common-law formalism. The framework, however, creates no exclusionary rule, Element Six ensures that it cannot operate to exclude evidence, and Element Three is expressly permissive so as to avoid the categorical quality that civil-law practitioners rightly resist. It gives structure to an evaluation that Chambers already carry out, as the Yekatom Chamber did at length, building its criteria from first principles because none had been laid down. Nor is unstructured free proof beyond criticism: Murphy has argued that the indiscriminate admission of evidence is a serious flaw in international criminal trials.⁷⁴

The second objection is over-formalisation: technical requirements may lead to the exclusion of probative evidence of atrocities where citizen witnesses cannot meet the ideals of chain-of-custody practice. Element Six is designed to meet this objection, since non-compliant material suffers no penalty at the admission stage. For the same reason, the framework is consistent with Pfefferkorn’s argument that “imposing a heightened bar for authentication of video evidence is unwarranted” and that courts “will be able to handle the challenges posed by deepfakes as they have handled potentially inauthentic evidence in the past.”⁷⁵ It raises no bar to admission and treats no video as suspect by default. What it adds is something her argument takes for granted, namely settled procedures on which courts can rely. The domestic systems she examines have them; the ICC does not.

The third objection is that a framework which allocates no persuasive burden, says nothing about weight and penalises no non-compliance at admission is merely declaratory. It changes three things. First, it changes what a Chamber must do: rather than developing criteria for the occasion, as in Yekatom, or resolving the matter in a footnote, as in Al Hassan, a Chamber would have to take stated standards into account and give reasons for departing from them, which makes appellate review and informed criticism possible. Second, it changes what a party may ask for, since a defence confronted with an unanchored and undocumented item could invoke a standard rather than rely on intuition. Third, and most significantly, it gives collectors a reason to anchor and document their material. The authentication deficit is less a matter of what judges do with the record than of what the record contains by the time it reaches them.

⁷⁴Peter Murphy, “No Free Lunch, No Free Proof: The Indiscriminate Admission of Evidence Is a Serious Flaw in International Criminal Trials,” *Journal of International Criminal Justice* 8, no. 2 (2010): 539–40, <https://doi.org/10.1093/jicj/mqq029>.

⁷⁵Riana Pfefferkorn, “‘Deepfakes’ in the Courtroom,” *Boston University Public Interest Law Journal* 29, no. 2 (2020): 248; see also 266–67 (“The current rules for authentication are adequate as-is”) and 255, 270–71 (anticipating a “reverse CSI effect” among jurors).

The fourth objection concerns implementation. Many items will never carry contemporaneous hashes, and expert interpretation of digital open-source material raises its own difficulties concerning the neutrality and qualifications of analysts.⁷⁶ The prospective operation of Element One and the safety valve in Element Six address the first difficulty; the second lies beyond the scope of this article.

Situating the Proposal

Braga da Silva observed that ICC Chambers have applied methods developed for verifying physical documents to digital evidence, and proposed a taxonomy of internal and external indicators of authenticity, an e-Court Protocol that records the metadata of tendered files, and training for judges and staff (see note 54). Al Hassan bears out his diagnosis (see notes 29–30). The present proposal takes his agenda further by identifying legal instruments, grounding the framework in an account of machine testimony, and addressing directly whether its central mechanism is compatible with Article 67(1)(i). Freeman and Vazquez Llorente concluded that most of the procedural adaptations that digital evidence requires could be achieved through updated interpretation and practice rather than through amendment of the Statute or the Rules.⁷⁷ This article accepts that much of the work lies in practice, but argues that the evaluation of citizen-gathered material needs a binding point of reference. Aksamitowska's study of how domestic courts in Germany, Sweden, Finland and the Netherlands have handled digital evidence in core international crimes cases offers comparative rather than directly applicable guidance.⁷⁸

CONCLUSION

Citizen-gathered open-source intelligence has become indispensable to international criminal accountability, yet its evaluation at the ICC still rests on judicial discretion and non-binding guidance. This article has argued that the precise doctrinal problem is not admissibility, which the free-proof system resolves generously, but the authentication deficit: the lack of binding criteria for deciding whether a digital item is what it purports to be. It has also argued that authentication is already a category internal to ICC practice, and not an importation barred by Rule 63(5).

The Yekatom and Ngaïssona judgment supplies four principles on which standards can be built, together with a caution that a presumption of reliability is compatible with low probative value. None of the material assessed in that case was gathered by citizens, however, and the Al Hassan Chamber dealt with contested video in a single footnote. The Berkeley Protocol and the Leiden Guidelines supply much of the technical knowledge a Chamber would need, but they bind no one, and under Article 21(2) neither does a carefully reasoned judgment. Extending the Yekatom principles to citizen-gathered evidence therefore requires substitutes for the guarantees that institutions provide.

The six-element framework proposes those substitutes: independently anchored hashing and disclosable chain-of-custody documentation; a permissive inference of authenticity, displaced by any specific indication of irregularity; source protection that affects the weight of an item rather than the defence's ability to test the process; a duty to give reasons when departing from the soft-law instruments; and a safety valve that keeps non-compliant material admissible. The elements concerning capture, documentation and disclosure fit the e-Court Protocol, which, as Duterte shows, a Chamber can amend by a single decision, supplemented where necessary by a Regulation under Article 52. The inference of authenticity belongs in a provisional Rule under Article 51(3), with an amendment under Article 51(2) as the eventual goal.

The framework is deliberately limited. Its central mechanisms show only that an item has not changed since it was anchored, and support an inference that it is what it purports to be. They do not establish what the item depicts, where or when it was recorded, or who made it; the attribution problems in Ayyash illustrate the last point. The inference carries no implication as to probative value, creates no exclusionary rule and places no persuasive onus on the accused; presumption-based models such as that of eIDAS derive from the law of trust services, and Article 67(1)(i) rules out the burden-shifting they

⁷⁶Matthew Gillett and Wallace Fan, "Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom," *Journal of International Criminal Justice* 21, no. 4 (2023): 671, 686–91, <https://doi.org/10.1093/jicj/mqad050>.

⁷⁷Lindsay Freeman and Raquel Vazquez Llorente, "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age," *Journal of International Criminal Justice* 19, no. 1 (2021): 184–88, esp. 184 ("this does not necessarily require amending the Statute or the Rules"), <https://doi.org/10.1093/jicj/mqab023>.

⁷⁸Karolina Aksamitowska, "Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands," *Journal of International Criminal Justice* 19, no. 1 (2021): 210–11, <https://doi.org/10.1093/jicj/mqab035>.

would entail. The framework is accordingly offered as a defensible first step rather than a complete solution. The analysis is also limited to public decisions, the Yekatom judgment remains under appeal, and the neutrality and qualifications of the experts who interpret open-source material deserve separate study.

More is at stake than procedural refinement. Synthetic media are making fabrication easier and the liar's dividend more potent, while platform moderation removes evidence before it can be preserved. The credibility of citizen-gathered evidence depends on standards that are transparent, technically grounded and institutionally recognised, and the safety of those who gather it depends on protections built into the evidentiary framework itself. International criminal justice has long relied on individuals willing to bear witness, often at considerable personal risk. They, and the accused, whose rights deserve equal protection, are owed a framework that does justice to the evidence brought before the Court.

REFERENCES

Cases and Court Documents

- Prosecutor v. Al Faki Al Mahdi*. ICC-01/12-01/15-171. Judgment and Sentence. Trial Chamber VIII, September 27, 2016.
- Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud*. ICC-01/12-01/18-2594-Red. Judgment. Trial Chamber X, June 26, 2024.
- Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*. ICC-01/11-01/17-2. Warrant of Arrest. Pre-Trial Chamber I, August 15, 2017.
- Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*. ICC-01/11-01/17-13. Second Warrant of Arrest. Pre-Trial Chamber I, July 4, 2018.
- Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*. ICC-01/11-01/17-24. Decision Terminating Proceedings. Pre-Trial Chamber I, June 15, 2022.
- Prosecutor v. Salim Jamil Ayyash et al*. STL-11-01/T/TC. Judgment. Trial Chamber, Special Tribunal for Lebanon, August 18, 2020.
- Prosecutor v. Bemba Gombo*. ICC-01/05-01/08-1022. Decision on the Admission into Evidence of Materials Contained in the Prosecution's List of Evidence. Trial Chamber III, November 19, 2010.
- Prosecutor v. Bemba Gombo*. ICC-01/05-01/08-1386 OA 5 OA 6. Judgment on the Appeals of Mr Jean-Pierre Bemba Gombo and the Prosecutor against the Decision of Trial Chamber III Entitled "Decision on the Admission into Evidence of Materials Contained in the Prosecution's List of Evidence." Appeals Chamber, May 3, 2011.
- Prosecutor v. Delalić et al*. IT-96-21-T. Judgment. Trial Chamber, International Criminal Tribunal for the former Yugoslavia, November 16, 1998.
- Prosecutor v. Duterte*. ICC-01/21-01/25-508. Decision on the Prosecution's and the Defence's Requests to Amend the E-Court Protocol. Trial Chamber III, September 28, 2026.
- Prosecutor v. Ongwen*. ICC-02/04-01/15-1423. Defence Motion on the Burden and Standard of Proof for Defences under Article 31(1)(a) and (d). Trial Chamber IX, January 28, 2019.
- Prosecutor v. Ongwen*. ICC-02/04-01/15-1455. Decision on Defence Request for Leave to Reply to Prosecution and CLRV Responses on the Burden and Standard of Proof Applicable to Articles 31(1)(a) and (d) of the Rome Statute. Trial Chamber IX, February 19, 2019.
- Prosecutor v. Yekatom and Ngaïssona*. ICC-01/14-01/18-64-Anx. Unified Technical Protocol ("E-court Protocol") for the Provision of Evidence, Witness and Victims Information in Electronic Form. January 23, 2019.
- Prosecutor v. Yekatom and Ngaïssona*. ICC-01/14-01/18-2784-Red. Judgment. Trial Chamber V, July 24, 2025.
- Prosecutor v. Yekatom and Ngaïssona*. ICC-01/14-01/18-2884-Red. Consolidated Victims' Response to the Prosecution and Defence Appeals of the Judgment and Sentence against Mr Alfred Yekatom and Patrice-Edouard Ngaïssona. March 23, 2026.
- Ukraine and the Netherlands v. Russia*. App. nos. 8019/16, 43800/14, and 28525/20. Decision. Grand Chamber, European Court of Human Rights, November 30, 2022.

Treaties, Legislation, and Other Instruments

- Aalto-Setälä, Sofia, Luca Caroli, Julia Freytag, Maria F. Jaramillo Gomez, and Joshua Lim. *Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals*. Leiden: Kalshoven-Gieskes Forum, Leiden University, 2022. <https://leiden-guidelines.com/guidelines/>.
- Assembly of States Parties. Resolution ICC-ASP/22/Res.1, “Resolution on Amendments to the Rules of Procedure and Evidence of the International Criminal Court.” December 13, 2023.
- Assembly of States Parties. Resolution ICC-ASP/24/Res.6, “Strengthening the International Criminal Court and the Assembly of States Parties.” December 5, 2025.
- Federal Rules of Evidence (United States). Rules 901–902, including Rules 902(13)–(14) as amended effective December 1, 2017. Accessed June 2, 2026. https://www.law.cornell.edu/rules/fre/rule_902.
- International Criminal Court. *Regulations of the Court*. ICC-BD/01-03-11, as amended November 2, 2011.
- International Criminal Court. *Rules of Procedure and Evidence*. ICC-PIOS-LT-03-006/24_Eng. The Hague: International Criminal Court, 2024.
- International Criminal Court, Office of the Prosecutor. *Policy on Cyber-Enabled Crimes under the Rome Statute*. The Hague: International Criminal Court, December 2025.
- International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: ISO, 2012.
- International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27042:2015, Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*. Geneva: ISO, 2015.
- Office of the United Nations High Commissioner for Human Rights and Human Rights Center, UC Berkeley School of Law. *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*. HR/PUB/20/2. New York and Geneva: United Nations, 2022.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS). 2014 O.J. (L 257) 73. Consolidated version of October 18, 2024.
- Rome Statute of the International Criminal Court. Adopted July 17, 1998, entered into force July 1, 2002.
- Strafprozessordnung [StPO] [Code of Criminal Procedure]. Version published on April 7, 1987, as last amended by Article 2 of the Act of July 17, 2025. Translated by Brian Duffett and Monika Ebinger, updated by Kathleen Müller-Rostin and Iyamide Mahdi, revised by Ute Reusch. Federal Ministry of Justice and Consumer Protection and Federal Office of Justice. https://www.gesetze-im-internet.de/englisch_stpo/.
- Turner, S., and L. Chen. *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*. RFC 6151. Internet Engineering Task Force, March 2011. <https://www.rfc-editor.org/rfc/rfc6151>.
- United Nations Commission on International Trade Law. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with Additional Article 5 bis as Adopted in 1998*. New York: United Nations, 1999.

Books and Journal Articles

- Aksamitowska, Karolina. “Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands.” *Journal of International Criminal Justice* 19, no. 1 (2021): 189–211. <https://doi.org/10.1093/jicj/mqab035>.
- Braga da Silva, Rafael. “Updating the Authentication of Digital Evidence in the International Criminal Court.” *International Criminal Law Review* 22, nos. 5–6 (2022): 941–64. <https://doi.org/10.1163/15718123-bja10083>.

- Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107 (2019): 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>.
- de Arcos Tejerizo, María. "Digital Evidence and Fair Trial Rights at the International Criminal Court." *Leiden Journal of International Law* 36, no. 3 (2023): 749–69. <https://doi.org/10.1017/S0922156523000031>.
- Dubberley, Sam, Alexa Koenig, and Daragh Murray, eds. *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford: Oxford University Press, 2020. <https://doi.org/10.1093/law/9780198836063.001.0001>.
- Freeman, Lindsay, and Raquel Vazquez Llorente. "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age." *Journal of International Criminal Justice* 19, no. 1 (2021): 163–88. <https://doi.org/10.1093/jicj/mqab023>.
- Gillett, Matthew, and Wallace Fan. "Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom." *Journal of International Criminal Justice* 21, no. 4 (2023): 661–93. <https://doi.org/10.1093/jicj/mqad050>.
- Hutchinson, Terry, and Nigel Duncan. "Defining and Describing What We Do: Doctrinal Legal Research." *Deakin Law Review* 17, no. 1 (2012): 83–119. <https://doi.org/10.21153/dlr2012vol17no1art70>.
- Koenig, Alexa, Jessica Peake, and Sylvanna Falcón. "Power and Humility in Open Source Investigations." *Human Rights Review* 27, no. 1 (2026): 77–99. <https://doi.org/10.1007/s12142-026-00758-1>.
- Liulina, Anastasiia. "Evidentiary Digital Platforms: What the Al Mahdi and Al Hassan Cases Teach Us about Presenting Voluminous Digital Data." *International Criminal Law Review* 25, no. 5 (2025): 840–68. <https://doi.org/10.1163/15718123-bja10235>.
- Murphy, Peter. "No Free Lunch, No Free Proof: The Indiscriminate Admission of Evidence Is a Serious Flaw in International Criminal Trials." *Journal of International Criminal Justice* 8, no. 2 (2010): 539–73. <https://doi.org/10.1093/jicj/mqq029>.
- Pfefferkorn, Riana. "'Deepfakes' in the Courtroom." *Boston University Public Interest Law Journal* 29, no. 2 (2020): 245–76.
- Roth, Andrea. "Machine Testimony." *Yale Law Journal* 126, no. 7 (2017): 1972–2053. <https://www.yalelawjournal.org/article/machine-testimony>.
- Schabas, William A. *The International Criminal Court: A Commentary on the Rome Statute*. 2nd ed. Oxford: Oxford University Press, 2016.
- Zarmsky, Sarah. "Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law." *Journal of International Criminal Justice* 19, no. 1 (2021): 213–25. <https://doi.org/10.1093/jicj/mqab048>.

Reports, Blogs, and Online Sources

- Higgins, Eliot. "How Open Source Evidence Was Upheld in a Human Rights Court." *Bellingcat*, March 28, 2023. <https://bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court>.
- International Criminal Court. "ICC Judges Update Chambers Practice Manual to Include Guidelines on Dissenting and Separate Opinions." Press release, July 13, 2023. <https://www.icc-cpi.int/news/icc-judges-update-chambers-practice-manual-include-guidelines-dissenting-and-separate-opinions>.
- Irving, Emma. "And So It Begins... Social Media Evidence in an ICC Arrest Warrant." *Opinio Juris*, August 17, 2017. <http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/>.
- Irving, Emma, and Sabrina Rewald. "Digital Evidence Before the ICC: Lessons from the Yekatom/Ngaïssona Judgment." *Opinio Juris*, August 8, 2025. <https://opiniojuris.org/2025/08/08/digital-evidence-before-the-icc-lessons-from-the-yekatom-ngaissona-judgment/>.
- McDermott, Yvonne, Stephen Sharp Queener, and Basile Simon. "Old Doubts, New Doubts: Evaluating Digital Open Source Imagery in the Courtroom." *Opinio Juris*, June 26, 2024.

- <https://opiniojuris.org/2024/06/26/old-doubts-new-doubts-evaluating-digital-open-source-imagery-in-the-courtroom/>.
- Mimran, Tal, and Lior Weinstein. "Digitalize It: Digital Evidence at the ICC." *Articles of War*, August 14, 2023. <https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/>.
- Simon, Basile. "New Evidence Techniques Document Bombed Ukrainian Schools for ICC." *Starling Lab*, March 1, 2023. <https://starling.stanford.edu/case-studies/submission-icc-schools-kharkiv-evidence-case-study/>.
- SITU Research. "ICC Digital Platform and the Al Hassan Case." Accessed June 2, 2026. <https://situ.nyc/research/projects/icc-digital-platform-and-the-al-hassan-case>.
- SITU Research. "ICC Digital Platform: Timbuktu, Mali." Accessed June 2, 2026. <https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali>.
- USC Shoah Foundation. "Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court." June 10, 2022. <https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes>.
- Wille, Belkis. "Video Unavailable": *Social Media Platforms Remove Evidence of War Crimes*. Human Rights Watch, September 10, 2020. <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes>.