Author Accepted Manuscript: Konstantina Stavrou and Yvonne McDermott, 'Digital Evidence' in William Schabas, Michelle Coleman and Caleb Wheeler (eds), *The Routledge Handbook of International Criminal Law* (2nd edn, Routledge 2027) (forthcoming)

Digital Evidence

Konstantina Stavrou and Yvonne McDermott

1. Introduction

The trial of the major war criminals at the International Military Tribunal at Nuremberg is often heralded as the first time video was ever introduced in the courtroom.[1] Whilst this bold claim is not entirely correct,[2] the showing of videos from liberated concentration camps was undoubtedly a turning point in the Nuremberg trial. As Telford Taylor recalled in his memoirs, the effect of the 'chillingly graphic film', showing the concentration camps at Dachau, Bergen-Belsen and Buchenwald as the Allied troops found them, was 'stunning', hardening sentiment against the defendants and changing the atmosphere in the courtroom.[3] Defendant Goëring was overheard remarking afterwards that 'then they showed that awful film, and it just spoiled everything.'[4]

International criminal tribunals have embraced new forms of evidence ever since, with the International Criminal Tribunal for the former Yugoslavia (ICTY) admitting satellite imagery, video, and intercept evidence. The Special Court for Sierra Leone (SCSL) admitted evidence from Facebook and Wikipedia, while the Special Tribunal for Lebanon's main prosecution case was centred around cellphone tower data showing the communication patterns and locations of networks of mobile phones.[5] In recent cases before the International Criminal Court (ICC), satellite imagery, videos, and images have played an important role.[6]

Konstantina Stavrou is a recipient of a DOC Fellowship of the Austrian Academy of Sciences at the Institute of Constitutional and Administrative Law at the Law Faculty of the University of Vienna, which supported the research on this chapter.

Yvonne McDermott's research on this chapter was conducted as part of the project, "Trust in User-generated Evidence: Analysing the Impact of Deepfakes on Accountability Processes for Human Rights Violations (TRUE)", selected for funding by the European Research Council and funded by UK Research and Innovation's Horizon Europe guarantee scheme (grant no. EP/X016021/1).

[1] Eg Lawrence Douglas, 'Films as Witness: Screening Nazi Concentration Camps Before the Nuremberg Tribunal', 105(2) The Yale Law Journal (1995) 449, 451 ('prior to Nuremberg, one can find no records of any court using graphic film of atrocities as proof of criminal wrongdoing').

[2] Lindsay Freeman and Raquel Vazquez Llorente, 'Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age' (2021) 19(1) JICJ 163, 164 provide some earlier examples from the US and UK in the 1920s and 1930s.

[3] Telford Taylor, *The Anatomy of the Nuremberg Trials* (1992) 202–203. See further, *Nuremberg Trial Proceedings Volume 3, Seventeenth Day (Tuesday, 11 December 1945) - Morning Session*; *Nuremberg Trial Proceedings Volume 2, Eighth Day (Thursday 29 November 1945) - Morning Session*.

[4] Taylor, ibid.

[5] James Hendry, 'Special Tribunal for Lebanon and Telecommunications Evidence' (2020) 4 PKI Global Justice Journal 34, <https://globaljustice.queenslaw.ca/news/special-tribunal-for-lebanon-and-telecommunications-evidence> accessed 16 December 2025.

[6] Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2018) 41(2) Fordham Int'l LJ 283.

This chapter focuses on the use of digital evidence in international criminal proceedings. It first defines digital evidence, as well as particular sub-categories of digital evidence that have gained prominence in recent years, such as open source and user-generated evidence. Through an historical examination of case law from the *ad hoc* tribunals, the ICC and domestic criminal courts, the chapter illustrates the progressive rise in the reliance on forms of digital evidence in international criminal proceedings. The analysis then highlights some of the unique benefits and challenges related to digital evidence. Finally, the chapter presents a detailed examination of how ICC proceedings have addressed the admissibility and weight of digital evidence to date.

2. Defining Digital Evidence

The literature on digital evidence reveals a lack of a coherent definition of the term.[7] Some authors refer to digital evidence as a broad category, encompassing all evidence in digital format.[8] The terms 'digital evidence' and 'electronic evidence' are broadly synonymous. For Schafer and Mason, 'electronic evidence refers to the digital information that can be used as proof in legal proceedings',[9] encompassing 'the output of analogue devices [and] data in digital form'.[10] Others distinguish between evidence that is created by digital devices and technology (so-called 'born-digital' or 'digitally derived' evidence) and digitised evidence, which incorporates, for example, an analogue document or artefact that is scanned and stored digitally for the purpose of legal proceedings.[11] According to the ICTR Trial Chamber I in *Musema*, digital evidence is a sub-category of documentary evidence, which is broadly defined as 'anything in which information of any description is recorded',[12] and includes 'documents in writing, maps, sketches, plans, calendars, graphs, drawings, computerized records, mechanical

[7] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Elsevier 2011) 7; David W Hagy, 'Glossary' in John D Nilsson (ed), *Digital Evidence in the Courtroom* (Nova Science Publishers 2010) 91; 'Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals', 3–4 <https://leiden-guidelines.com/> accessed 16 December 2025.

[8] Rafael Braga Da Silva, 'Updating the Authentication of Digital Evidence in the International Criminal Court' (2021) Int Crim L Rev 1, 2; Alexa Koenig et al, 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (Berkeley Human Rights Center, 2014) 1.

[9] Burkhard Schafer and Stephen Mason, 'The Characteristics of Electronic Evidence' in Stephen Mason and Daniel Seng (eds), *Electronic Evidence* (4th edn, IALS 2017) 19.

[10] ibid.

[11] International Bar Association Report, 'Evidence Matters in ICC Trials' (August 2016), <www.ibanet.org/document?id=Evidence-matters-in-icc-trials> accessed 16 December 2025, 19; Leiden Guidelines (n 7); Emma Breeze, 'Versions of the Truth: Disinformation and Prosecuting Atrocities', in Mark A Drumbl and Caroline Fournet (eds), *Sights, Sounds, and Sensibilities of Atrocity Prosecutions* (Brill 2024).

[12] *The Prosecutor v Musema* (Judgment and Sentence) ICTR-96-13-T (27 January 2000) [53].

records, electro-magnetic records, digital records, databases, sound tracks, audio-tapes, video-tapes, photographs, slides and negatives'.[13]

In this chapter, the term 'digital evidence' is understood as encompassing 'data, information or evidence that is created, manipulated, stored or communicated by any (digital) device, computer or computer system or transmitted over a communication system'[14] that a party to a case seeks to admit in legal proceedings. This definition covers all information in digital format, either born-digital or digitised.[15] In practice, however, the probative value of a piece of content that has been digitised for the purpose of proceedings, such as a scan of a document or record created in accordance with the ICC's E-Court Protocol, is unlikely to be as controversial as born-digital forms of digital evidence, including call data records, satellite imagery evidence, communications on social media platforms, and photographs and videos created on personal digital devices.

Two distinct but overlapping forms of digital evidence have gained prominence in recent years and require further definition at the outset. The first, open source evidence, is defined as 'publicly available information that any member of the public can observe, purchase or request' without specific permissions, which may be of evidentiary value in legal proceedings. [16] Akin to its parent category of digital evidence, scholarship on this form of evidence and investigation uses a dizzying array of closely-related terms and acronyms, including digital open source evidence (DOSI),[17] open source audio-visual content (OAVC),[18] open source research (OSR),[19] social media evidence,[20] and open source intelligence (OSINT),[21] amongst others. The difference in terminology between sub-categories of open source evidence tends to pertain to

[13] ibid.
[14] Koenig et al (n 8) fn 2.
[15] Freeman and Vazquez Llorente (n 2) 168.
[16] Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law 2020, para 14.
[17] Matthew Gillett and Wallace Fan, 'Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom' (2023) 21(4) JICJ 661.
[18] Dearbhla Minogue et al, 'Putting Principles into Practice: Reflections on a Mock Admissibility Hearing on Open Source Evidence' in Michael Lysander Fremuth, Andreas Sauermoser and Konstantina Stavrou (eds), *International Criminal Law before Domestic Courts: The Role of National Criminal Justice in the Prosecution of International Core Crimes* (MANZ Verlag 2024) 307–340.
[19] Daragh Murray, Yvonne McDermott, and K Alexa Koenig, 'Mapping the Use of Open Source Research in UN Human Rights Investigations' (2022) 14(2) Journal of Human Rights Practice 554.
[20] Franka Pues, 'Bridging the Evidentiary Gap: The Use of AI-Derived Social Media Open Source Evidence in International Criminal Prosecutions' (PhD thesis, Kings College London 2025) (on file with author).
[21] Sylvanna Falcón et al, 'Symposium on Fairness, Equality, and Diversity in Open Source Investigations: Democratizing OSINT – University-Based Lessons on Diversity and Inclusion' (*Opinio Juris*, 7 February 2023) <https://opiniojuris.org/2023/02/07/symposium-on-fairness-equality-and-diversity-in-open-source-investigations-democratizing-osint-university-based-lessons-on-diversity-and-inclusion/> accessed 16 December 2025.

the type of information (eg audio-visual or social media) or its use (ie as intelligence, information, or evidence). Closed source evidence, by contrast, encompasses 'information with restricted access or access that is protected by law, but which may be obtained legally through private channels, such as judicial processes, or offered voluntarily'.[22]

A second important sub-category of digital evidence, 'user-generated evidence', distinguishes between material based on its source.[23] User-generated evidence is understood as open or closed source information generated by ordinary users through their personal digital devices, which may be of evidentiary value and used in legal proceedings.[24] It may be open source, where it is available on the internet, for example, or it may be closed source, where it is sent directly to a party to the case or captured via a dedicated mobile phone application. The International Bar Association's 'Eyewitness to Atrocities' is one such application, which captures metadata and preserves the chain of custody of information from the point of its capture; by today, there are several applications of this nature. In this way, the sub-category of 'user-generated evidence' is broader than that of 'open source evidence', because it is not limited to publicly-available data. In another way, it is a narrower category because it excludes open source information such as journalistic reporting, satellite imagery, or public records. Other scholars distinguish between particular types of digital evidence which may be user-generated and/or open source; Jonathan Hak, for example, uses the term 'image-based evidence',[25] to capture images, video, digital reconstructions, earth observation data, and animations.

3. A History of the Use of Digital Evidence in International Criminal Proceedings

Using evidence created through technology is not new in international criminal law. Examples can be identified in the Nuremberg trials, during which data from IBM punched card

[22] Berkeley Protocol (n 16) para 14.
[23] Rebecca J Hamilton, 'User Generated Evidence' (2018) 57(1) Colum J Transnat'l L 1, 3.
[24] Konstantina Stavrou, 'User-Generated Evidence in International Criminal Proceedings before Domestic Courts: Is Seeing Always Believing?' in Michael L Fremuth, Andreas Sauermoser and Konstantina Stavrou (eds), *International Criminal Law before Domestic Courts: The Role of National Criminal Justice in the Prosecution of International Core Crimes* (Manz Verlag 2024) 344.
[25] Jonathan Hak, *Image-Based Evidence in International Criminal Prosecutions: Charting a Way Forward* (OUP 2024) xxiii.

technology, used by the Nazis to track the names of their victims, was relied upon, along with film and images.[26]

The establishment of the *ad hoc* tribunals for the former Yugoslavia and Rwanda in the 1990s marked an important point for the introduction of digital evidence in international criminal proceedings due to technological progress and digital transformation. Satellite imagery from the United States' spy planes[27] was, for instance, introduced in cases before the ICTY as evidence to demonstrate the existence of mass graves.[28] The ICTY also relied upon audio recordings of intercepted conversations in several cases, while the ICTR considered video footage of crime sites, rallies and meetings.[29] Additionally, user-generated evidence in the form of YouTube videos, Facebook pictures and messages was introduced before the International Residual Mechanism for Criminal Tribunals cases dealing with the crimes committed in the former Yugoslavia and Rwanda.[30] The Special Court for Sierra Leone also relied on novel forms of digital evidence in its proceedings. For instance, the defence in the *Taylor* case relied on a photograph from a Facebook page to indicate that a prosecution witness had attended a poor taste 'blood diamond' themed party.[31] The Special Tribunal for Lebanon was the first to rely primarily on digital technologies in trial proceedings as evidence against the accused in *Prosecutor v Ayyash et al*. In addition to video footage from surveillance cameras,[32] the

[26] See in general Edwin Black, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation-Expanded Edition* (Dialog Press 2012).

[27] Isabelle Delpla, 'The ICTY Investigations: Interview with Jean-René Ruez' in Isabelle Delpla, Xavier Bougarel and Jean-Louis Fourner (eds), *Investigating Srebrenica: Institutions, Facts, Responsibilities* (Berghahn Books 2012) 33. Controversially, this evidence was provided by the United States with instructions that the Prosecution was 'not authorized to discuss in courtroom proceedings any information relating to the technical or analytical sources, methods, or capabilities of the systems, organizations, or personnel used to collect, analyze, or produce these imagery-derived products': *Prosecutor v Tolimir* (Trial Judgment) IT-05-88/2-T (12 December 2012) [68]. See further, Aida Ashouri, Caleb Bowers, and Cherrie Warden, 'An Overview of the Use of Digital Evidence in International Criminal Courts', 11(0) Digital Evidence and Electronic Signature Law Review (2014) 115, 120–121.

[28] *Prosecutor v Radovan Karadžić* (Trial Judgment) IT-95-5/18-T (24 March 2016) [5512–5514]; *Prosecutor v Ratko Mladić* (Trial Judgment) IT-09-92-T (22 November 2017) [2700], [2752].

[29] Eg *Karadžić* Trial Judgment, ibid, [23]; *Prosecutor v Popović et al* (Decision on the Admissibility of Intercepted Communications) IT-05-88-T (7 December 2007); *Prosecutor v Bagosora et al* (Trial Judgment) ICTR-98-41-T (18 December 2008) [493], [518], [996], [1340], [1897], [1916], [2029].

[30] *Prosecutor v Zdravko Tolimir* (Transcript) IT-05-88/2-T (25 May 2011); *Prosecutor v Zdravko Tolimir* (Transcript) IT-05-88/2-T (26 May 2011); *Prosecutor v Radovan Karadžić* (Transcript) IT-95-5/18 (28 May 2013); *Prosecutor v Radovan Karadžić* (Transcript) IT-95-5/18 (31 May 2011); *Prosecutor v Ratko Mladić* (Transcript) IT-09-92-T (8 July 2014); *Prosecutor v Ratko Mladić* (Transcript) IT-09-92-T (7 July 2014); *Prosecutor v Ratko Mladić* (Transcript) IT-09-92-T (26 February 2013); *Prosecutor v Goran Hadžić* (Transcript) IT-04-75-T (7 May 2015); *Prosecutor v Goran Hadžić* (Transcript) IT-04-75-T (11 March 2015); *Prosecutor v Radovan Karadžić* (Transcript) IT-95-5/18 (2 February 2012); *Prosecutor v Marie Rose Fatuma et al* (Transcript) MICT-18-116-T (23 November 2020).

[31] *The Prosecutor v Charles Ghankay Taylor* (Trial Transcript) SCSL–2003–01–T (9 August 2010) 45783–45784.

[32] *The Prosecutor v Ayyash et al* (Judgment) STL-11-01/T/TC (18 August 2020) [1272–1273].

prosecution relied extensively on telecommunications data as evidence as a central pillar of its case.[33]

Video evidence in a digital format was introduced by the prosecution in the first ICC trial, *The Prosecutor v Thomas Lubanga Dyilo*, to support the charge of conscription and enlistment of child soldiers against Lubanga.[34] The Chamber considered that one video, showing Lubanga visiting a training camp in 2003, showed some 'recruits who were clearly under the age of 15'.[35] Intercepts and photographs have also been introduced as evidence in ICC jurisprudence.[36]

The *Al Mahdi* case, from the situation in Mali, and the *Al Werfalli* case, from the situation in Libya, marked two significant firsts for the Court's use of digital evidence. In *Al Mahdi*, the Court relied in its judgment for the first time on user-generated evidence in the form of videos.[37] The defendant was charged as a direct perpetrator of the war crime of destruction of cultural property in Timbuktu. Numerous videos were admitted as evidence, depicting the defendant destroying mosques, as well as overseeing others and ordering the destruction of mosques. In addition to videos, satellite imagery and geolocation data were tendered into evidence. The defendant made an admission of guilt and accepted the reliance on the evidence, which meant that the material was not challenged before the Court.[38] The following year, in *Al Werfalli*, Pre-Trial Chamber I issued an arrest warrant based largely on evidence found on social media.[39] The arrest warrant alleged the defendant's responsibility for 33 counts of the war crime of murder during seven incidents in the context of the Libyan conflict, either by personally killing the victims or ordering their execution. The proceedings were terminated following the suspect's death,[40] and, hence, the evidence was, similarly to *Al Mahdi*, not examined by the Court.

---

[33] STL, 'Primer on Telecommunications Evidence: Guide to Understanding the Testimony in Ayyash et al' (2018) <www.stl-tsl.org/sites/default/files/bulletin/Primer.pdf> accessed 16 December 2025.
[34] *The Prosecutor v Thomas Lubanga Dyilo* (Judgment Pursuant to Article 74 of the Statute) ICC-01/04-01/06-2842 (14 March 2012) [107].
[35] ibid [792]. The Chamber stated that it 'relied on video evidence in this context only to the extent that they depict children who are clearly under the age of 15.' [644].
[36] *The Prosecutor v Bemba et al* (Decision on 'Prosecution's Fifth Request for the Admission of Evidence from the Bar Table') ICC-01/05-01/13-1524 (14 December 2015); *The Prosecutor v Dominic Ongwen* (Trial Judgment) ICC-02/04-01/15 (4 February 2021) fns 4440 and 4622; *The Prosecutor v Bosco Ntaganda* (Judgment Pursuant to Article 74) ICC-01/04-02/06-2359 (8 July 2019) [282].
[37] *The Prosecutor v Ahmad Al Faqi Al Mahdi* (Judgment and Sentence) ICC-01/12-01/15-171 (27 September 2016) [29].
[38] ibid [29–30].
[39] *The Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli* (Warrant of Arrest) ICC-01/11-01/17-2 (15 August 2017) [3]; Alexa Koenig, 'Open Source Evidence and Human Rights Cases: A Modern Social History' in Sam Dubberley, Alexa Koenig and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (OUP 2019) 41.
[40] *The Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli* (Decision Terminating Proceedings against Mr Mahmoud Mustafa Busayf Al-Wefalli) ICC-01/11-01/17 (15 June 2022) [5].

Recent ICC jurisprudence confirms and further illustrates the Court's growing use of digital evidence in general and user-generated evidence in particular. In *Ongwen*, digital evidence, including intercepts of radio communications, videos and photographs, was tendered by the Prosecution and relied upon by the Court.[41] In *Al Hassan*, the evidentiary record included videos, audio recordings, and photographs to determine, among others, the perpetration of floggings and the destruction of mausoleums.[42] In *Yekatom and Ngaïssona,* Facebook material, such as private conversations, screenshots of posts, pictures and lists of Facebook friends, as well as Facebook business records, were introduced, for instance, by the Prosecutor to show Ngaïssona's coordinating role in the Anti-Balaka.[43]

In addition to proceedings before international criminal courts and tribunals, several prosecutions for core international crimes by domestic criminal courts, which have relied on user-generated evidence, have resulted in convictions.[44] Examples include cases from Germany, Sweden, the Netherlands and Finland.[45] The defendants in several of those cases were convicted of the war crime of outrages upon the personal dignity of the dead,[46] killing as a war crime, and the war crime of pillaging.[47]

4. The Value of Digital Evidence

The previous section illustrated the nascent importance of digital evidence – and, particularly, user-generated evidence – for criminal accountability proceedings both at the international and the domestic level. This section provides an overview of the beneficial effects of using digital evidence in international criminal proceedings.

---

[41] *The Prosecutor v Dominic Ongwen* (Trial Judgment) (n 36) [614] and fns 4440, 4622.

[42] *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (Trial Judgment) ICC-01/12-01/18-2594-Red (26 June 2024) [726], [838], [1031].

[43] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Trial Judgment) ICC-01/14-01/18-2784-Red (24 July 2025) [144], [435].

[44] For a full overview, see the database created by Anne Hausknecht of the TRUE project, <www.trueproject.co.uk/airtable> accessed 16 December 2025.

[45] ibid; European Union Network for Investigation and Prosecution of Genocide, Crimes against Humanity and War Crimes, 'Prosecuting War Crimes of Outrage upon Personal Dignity Based on Evidence from Open Sources – Legal Framework and Recent Developments in the Member States of the European Union' (1 February 2018) <https://www.eurojust.europa.eu/publication/prosecuting-war-crimes-outrage-upon-personal-dignity-based-evidence-open-sources-legal> accessed 16 December 2025.

[46] For a discussion on whether the corresponding Rome Statute provision covers the deceased and whether creating and sharing user-generated content depicting (body parts of) the deceased constitutes conduct amounting to this war crime, see Konstantina Stavrou, 'Committing War Crimes One Click at a Time? User-Generated Content and the War Crime of Outrages upon the Personal Dignity of the Dead at the International Criminal Court' (2025) Int Crim L Rev 1.

[47] TRUE project database (n 44); European Union Network for Investigation and Prosecution of Genocide, Crimes against Humanity and War Crimes, 'Overview of National Jurisprudence' (July 2024) <www.eurojust.europa.eu/sites/default/files/assets/files/case-law-compendium-2024.pdf> accessed 16 December 2025.

Digital content found online can generate leads that will assist with establishing that crimes falling within the court's jurisdiction may have been committed,[48] as a precondition for initiating investigations.[49] More specifically, forms of digital evidence can be used to answer the necessary 'who', 'what', 'where' and 'when' questions to determine the court's personal, material, geographic and temporal jurisdiction. For instance, videos and their geolocation can be used to identify the location depicted and confirm where specific incidents occurred.[50]

Such evidence can prove particularly useful when international investigators are denied access to sites where crimes have allegedly been committed.[51] In these instances, different forms of digital evidence may constitute the sole source of information regarding the potential commission of crimes in ongoing conflicts. As an illustration, photos, audio material and satellite imagery were key material for the ICC Office of the Prosecutor to file applications for arrest warrants in the Situation in the State of Palestine,[52] in light of Israel's impediments to access of international investigative bodies.[53]

Digital evidence can also assist in overcoming issues related to investigations initiated long after the occurrence of events and the cessation of hostilities. The ICC is a court of last resort, whose jurisdiction is determined based on the principle of complementarity. This means that the Court shall only exercise its jurisdiction if states are unwilling or unable to do so.[54] On some occasions, it may take years before the ICC can commence its investigations, which carries the risk that evidence may be lost or destroyed. Digital evidence, including user-generated evidence, can offer a contemporaneous account of events, minimising the risk of evidence loss or tampering.[55] Ultimately, this could expedite accountability proceedings.

---

[48] Jay D Aronson, 'The Utility of User-Generated Content in Human Rights Investigations' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (CUP 2018) 131.

[49] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) (hereinafter: Rome Statute) art 12.

[50] See eg Christiaan Triebert, 'Geolocating Libya's Social Media Executioner' (Bellingcat 4 September 2017) <www.bellingcat.com/news/mena/2017/09/04/geolocating-libyas-social-media-executioner/> accessed 16 December 2025 for a detailed analysis of the geolocation of the videos used in the *Al Werfalli* arrest warrants.

[51] Molly K Land and Jay D Aronson, 'The Promise and Peril of Human Rights Technology' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (CUP 2018) 9.

[52] ICC, 'Statement of ICC Prosecutor Karim A.A. Khan KC: Applications for Arrest Warrants in the Situation in the State of Palestine' (20 May 2024) <www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state> accessed 16 December 2025.

[53] As has been noted by the International Court of Justice: *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v Israel) (Request for the Modification of the Order of 28 March 2024: Order)* (24 May 2024) 649, 666; UNGA, 'Report of the Independent International Commission of Inquiry on the Occupied Palestinian Territory, Including East Jerusalem, and Israel' (A/79/232, 11 September 2024) 113(n).

[54] Rome Statute art 17(1)(a), 17(2) and 17(3).

[55] Rebecca J Hamilton, 'Social Media Platforms in International Criminal Investigations' (2020) 52(1) Case W Res J Intl'L 213, 218.

In the opposite scenario, investigations might begin while hostilities are ongoing, which carries significant risks for investigators accessing the ground and gathering relevant information. The issue of security has previously been raised in ICC proceedings, whereby, according to depositions of investigators, there was the feeling that it was dangerous to leave the United Nations-protected area.[56] Online digital content can minimise risks related to investigations while ensuring timely evidence collection.

Digital evidence – especially photographs and videos – can offer a visual account of the alleged crimes and the manner of their commission. At the same time, such content can help identify and link perpetrators to crimes.[57] Moreover, audio-visual evidence can provide cues on the potential affiliation of perpetrators based, for instance, on the uniforms worn or their demeanour.[58] Lastly, it can help ascertain the accused's *mens rea*.[59]

5. The Challenges of Digital Evidence

Despite these benefits, several challenges risk undermining the utility of digital evidence in international criminal trials. The volume of digital evidence, particularly open source and user-generated evidence, in the context of mass atrocity crimes is potentially enormous and unmanageable.[60] In an era of ever-increasing access to technology that enables people to document and share content online, terabytes of new information are created and shared every day.[61] In addition, access to satellite imagery, earth observation data and other forms of information have opened up new ways of knowing about international crimes. However, 'finding the signal in the noise', by sifting through this huge amount of information to identify and analyse the most relevant pieces of content that could produce investigative leads, or could be introduced as evidence in court one day, places a heavy burden on investigators, who simply will not have the resources or tools to search through every piece of content.[62]

---

[56] *Prosecutor v Thomas Lubanga Dyilo* (Judgment Pursuant to Article 74 of the Statute) (n 34) [153–155].

[57] Lindsay Freeman, 'Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court' in Sam Dubberley, Alexa Koenig and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (OUP 2019) 62–63.

[58] In *Case no 09/748003-18V* (The Hague District Court, 23 July 2019) section 4.3.2, for instance, the Court established the defendant's affiliation with the 'Islamic State' (IS) based on a photograph in which the defendant wears a piece of clothing carrying the IS logo, as well as on photographs in which he made a gesture attributed to the IS.

[59] See eg *Case no 09/748001-19* (The Hague District Court, 16 July 2021) 17 , in which the Court relied on video evidence to establish that the defendant 'consciously and closely cooperated in the execution' of the victims, playing a leading role, and negating the defence argument that the defendant acted out of fear for his life.

[60] Hamilton (n 23) 32–33.

[61] For example, approximately 20 million videos are uploaded to YouTube every day, while TikTok had 1.99 billion users globally in 2025. It is estimated that over 100 billion messages are sent each day on WhatsApp.

[62] Freeman and Vazquez Llorente (n 2) 170.

In modern armed conflicts, there has been a remarkable upsurge in civil society organisations that have been active in preserving digital evidence to document atrocities, which may ease the burden on prosecutors, if that information can be shared as information packages.[63] The Office of the Prosecutor recently created 'OTPLink', an online platform where information relevant to any situation under investigation can be uploaded.[64] The Office has apparently invested in artificial intelligence and machine learning tools to filter this content,[65] which raises issues of algorithmic bias,[66] where certain types of content might be incorrectly removed from human review.

More fundamentally, unlike the Prosecutor of the ICC,[67] the organisations and individuals sharing potential evidence have no legal duty to investigate exonerating and incriminating evidence equally. This may lead to allegations that the prosecution's case is the product of a biased investigation, where it relies heavily on evidence gathered by third parties.[68] The source of other forms of digital evidence, such as intercepted communications, may be an opposing party to the armed conflict, which may give rise to similar allegations of bias.[69] All of this means that at trial, the benefits of introducing digital evidence may be outweighed by the efficiency costs in doing so.[70] The source of this evidence, its chain of custody, and how it was authenticated or verified, will have to be explained, often through the testimony of an expert witness.[71] International criminal trials are known for their overwhelmingly large evidentiary records,[72] and to add more material to be considered may add to the duration of already lengthy proceedings.

---

[63] Eurojust, EU Genocide Network and ICC Office of the Prosecutor, 'Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations' (2022), foreword, 31–32.

[64] <https://otplink.icc-cpi.int/> accessed 16 December 2025.

[65] ICC, 'ICC Prosecutor Karim A.A. Khan KC Announces Launch of Advanced Evidence Submission Platform: OTPLink' (24 May 2023) <www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink> accessed 16 December 2025.

[66] Yvonne McDermott, Alexa Koenig and Daragh Murray, 'Open Source Information's Blind Spot: Human and Machine Biases in International Criminal Investigations' (2021) 19(1) JICJ 85.

[67] Rome Statute art 54(1).

[68] Freeman and Vazquez Llorente (n 2) 174.

[69] *The Prosecutor v Callixte Mbarushimana* (Decision on the Confirmation of the Charges) ICC-01/04-01/10-465-Red (16 December 2011) [74] noting 'the fact that there is no allegation of any bias or interest in the outcome of these proceedings or the events to which the charges relate on the part of the States which collected the intercept evidence'.

[70] Freeman (n 6) 313.

[71] See eg *The Prosecutor v Ali Muhammad Ali Abd-al-Rahman ('Ali Kushayb')* (Decision on the Defence Request to Admit Duncan Castellvi as an Expert Witness and to Introduce his Evidence under Rule 68(3) of the Rules) ICC-02/05-01/20-1132 (16 May 2024).

[72] Yvonne McDermott, 'Inferential Reasoning and Proof in International Criminal Trials: The Potentials of Wigmorean Analysis' (2015) 13(3) JICJ 507.

Storing digital evidence may also result in significant cost and staffing implications, as file types can become unreadable as technology advances.[73] Just as material stored on a floppy disk, once a common means of storage, will be almost impossible to access today, there is no guarantee that .jpeg images or .pdf files, or material stored on USB flash drives, will be readable ten years from now. Professional archivists will be needed to safely preserve evidentiary materials, as they do with hard copies and documents. The ephemeral nature of many types of digital evidence, coupled with the fact that information online may be removed at any time without notice, gives rise to additional vulnerabilities to be considered.[74] These will require back ups to be kept in different formats, again adding to storage costs and resource requirements.

Another vulnerability is the risk of misinformation and disinformation influencing digital evidence. The highly charged political contexts in which atrocity crimes occur can give rise to deliberate attempts to mislead through sharing manipulated, edited, or decontextualised material in digital form. It is also not uncommon for individuals to innocently share such material without realising that it is inauthentic, leading to the spread of misinformation. Thanks to advances in artificial intelligence, convincing 'deepfake' audio files, videos and images can now be created and edited quickly and at scale.[75] This broader information ecosystem in which digital evidence is created will invariably impact the consideration of digital evidence. There will be a greater need to ascertain the authenticity of digital evidence to prevent fake material from being introduced in court. Additionally, increased awareness of the risks of convincing fakes may also give rise to doubts around real content, and difficult questions around where the burden of proof should lie where one party alleges that the other side's evidence is fake. Digital evidence is also, by its nature, more susceptible to cyberattacks by malicious actors, who may seek to hack into the systems providing or storing this evidence, to delete or tamper with it.[76]

[73] Yvonne Ng, 'How to Preserve Open Source Information Effectively', in Sam Dubberley, Alexa Koenig, Daragh Murray and Yvonne McDermott (eds), *Digital Witness:* Using Open Source Information for Human Rights Investigation, Documentation and Accountability (2nd edn, forthcoming, OUP 2026), on file with authors.

[74] Hillary Hubley, 'Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations' (2022) 22 (5–6) Int Crim L Rev 989, 990.

[75] Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California L Rev 1755; Alexa Koenig, '"Half the Truth is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law' (2019) 113 AJIL Unbound 250, 252.

[76] Office of the Prosecutor, 'Draft Policy on Cyber-Enabled Crimes under the Rome Statute', para 79; Harriet Moynihan, Philippa Webb and Amal Clooney, *Legal Accountability for Malicious Cyber Operations*, Oxford Institute for Technology and Justice (2025), para 74.

6. Admissibility of Digital Evidence

The challenges outlined in the previous section make considerations around what evidence gets admitted to the record all the more pertinent. ICC Trial Chamber I in *Lubanga* established a three-step test for the admissibility of evidence other than direct oral testimony, derived from three factors mentioned in Article 69(4) of the Statute. The evidence should, first, be *prima facie* relevant to the trial; second, the Chamber should assess its probative value; and, third, its probative value should be weighed against its prejudicial effect.[77] This approach was also adopted later by Trial Chamber II in *Katanga and Ngudjolo*.[78]

i. Relevance

Relevance requires that evidence relates to matters examined by a Chamber.[79] It has been defined as the quality of making 'the existence of any fact that is of consequence to the determination of an issue in a case more or less probable'.[80] This determination depends on the purpose for which the evidence is adduced and is, thus, established on a case-by-case basis. Trial Chamber II in *Katanga and Ngudjolo* found that the relevance of audio-visual material depends on the recording date and/or location; thus, evidence needs to be provided about the time, date and location of the recording.[81] The Chamber added that if the relevance of a piece of evidence is not apparent from the item itself, the tendering party should explain the relevance of a 'specific factual proposition to a material fact of the case' and how the item at hand makes the proposition more or less likely.[82] This criterion aims to exclude irrelevant evidence from the trial and define the purpose of a specific evidentiary item in the proceedings.[83]

---

[77] *The Prosecutor v Thomas Lubanga Dyilo* (Decision on the Admissibility of Four Documents) ICC-01/04-01/06-1399 (13 June 2008) [26–32].
[78] *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) ICC-01/04-01/07-2635 (17 December 2010) [14].
[79] *The Prosecutor v Thomas Lubanga Dyilo* (Decision on the Admissibility of Four Documents) (n 77) [27].
[80] *The Prosecutor v Jean-Pierre Bemba Gombo* (Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo) ICC-01/05-01/08 (15 June 2009) [41]; *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) (n 78) [16]; *The Prosecutor v William Samoei Ruto, Henry Kiprono Kosgey and Joshua Arap Sang* (Decision on the Confirmation of Charges Pursuant to Article 61(7)(a) and (b) of the Rome Statute) ICC-01/09-01/11 (23 January 2012) [66]; *Prosecutor v Francis Krimi Muthaura, Uhuru Muigai Kenyatta and Mohammed Huseein Ali* (Decision on the Confirmation of Charges Pursuant to Article 61(7)(a) and (b) of the Rome Statute - Dissenting Opinion by Judge Hans-Peter Kaul) ICC-01/09-02/11-382-Red (23 January 2012) [79]; *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Bar Table Motion of the Defence of Germain Katanga) ICC-01/04-01/07-3184 (21 October 2011) [16].
[81] *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) (n 78) [24].
[82] ibid [16].
[83] ibid [16–18].

This role of the tendering party in explaining the relevance of a piece of evidence is particularly important in the case of user-generated evidence. For example, in *Bemba et al,* the defence noted that they felt 'ambushed' by the extensive admission of items whose relevance was 'never clearly pleaded in a timely manner' by the prosecution, as the prosecutor had failed to explain the relevance of each evidentiary item upon submission.[84] The defence in *Yekatom and Ngaïssona* raised similar arguments, expressing concern that the wholesale admission of Facebook messages that lacked relevance would unduly flood the evidentiary record and prejudice the fairness of proceedings.[85] This argument was rejected by the Single Judge, who found that the prosecution 'made submissions on the purported relevance of each evidence, in its entirety', adding that 'not every single Facebook message within the message threads has to have been discussed specifically with the witness for the Chamber to be in a position to assess the messages' probative value and relevance'.[86]

ii. Probative value

If the relevance of an item has been established, the chamber will then assess its probative value. At the outset, it is important to note that while probative value and evidentiary weight are similar concepts, they are distinct.[87] Probative value is a criterion for establishing the admissibility of a piece of evidence, while weight pertains to the importance a chamber may attach to that piece of evidence in reaching a judgment.[88] Several considerations about the 'inherent characteristics' of the evidence may be relevant for evaluating its probative value.[89] Generally, the probative value of a piece of evidence is assessed based on two key factors: the evidence's reliability and its significance.[90] The reliability may be indicated by factors such as the 'source or author, as well as their role in the relevant events, the chain of custody from the time of the item's creation until its submission to the chamber, and any other relevant

[84] *The Prosecutor v Bemba et al* (Public Redacted Judgment on the Appeals of Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jacques Mangenda Kabongo, Mr Fidèle Babala Wandu and Mr Narcisse Arido against the Decision of Trial Chamber VII Entitled "Judgment pursuant to Article 74 of the Statute") ICC-01/05-01/13-2275-Red (8 March 2018) [566].
[85] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Public Redacted Version of 'Yekatom Defence Response to Prosecution's Bar Table Motion of 17 February 2022', 31 March 2022, ICC-01/14-01/18-1341-Conf) ICC-01/14-01/18-1341-Red2 (3 June 2022) [25].
[86] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Decision on the Second Prosecution Submission Request from the Bar Table (P-0889)) ICC-01/14-01/18-1429 (24 May 2022) [15].
[87] *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) (n 78) [13].
[88] ibid.
[89] ibid.
[90] ibid [15]; *The Prosecutor v Thomas Lubanga Dyilo* (Decision on the Admissibility of Four Documents) (n 77) [28–30].

information'.[91] In *Ntaganda*, Trial Chamber VI found that the lack of information on the date, location and events depicted significantly lowered the material's probative value, resulting in its exclusion from the record.[92] Other factors may include an item's authenticity, whether it is an original or a copy, and whether it is 'signed, sealed, stamped or certified in any way'.[93] Trial Chamber II in *Katanga and Ngudjolo* found that, when establishing the admissibility of documentary evidence, authenticity is the first issue to be determined as part of the reliability assessment, as admitting unauthenticated evidence would 'unjustifiably burden the record of the trial with non-probative material'.[94]

An item's significance pertains to its ability to influence the chamber's inquiries either by significantly helping the chamber reach a conclusion about the existence of a material fact or by significantly assisting the chamber in assessing the reliability of other pieces of evidence in the record.[95] As elaborated by the ICC, there can be varying degrees of significance, depending on the impact the admission of a piece of evidence might have.[96] Accordingly, even though a piece of evidence may be relevant, it might still be declared inadmissible if its potential impact is limited.[97]

iii. Prejudicial effect

Lastly, the probative value of evidence must be weighed against its prejudicial effect.[98] Reflecting on this criterion in the case of digital evidence, the volume of such evidence admitted in proceedings could affect defendants' rights to be tried without undue delay.[99] In that regard, Trial Chamber II in *Katanga and Ngudjolo* found that the provision on the right to be tried without undue delay requires the exclusion of evidence 'if the time anticipated for its presentation - or subsequent evaluation by the Chamber - is disproportionate to its potential probative value'.[100] The volume of digital evidence can also raise concerns about equality of

[91] *The Prosecutor v Jean-Pierre Bemba Gombo* (Judgment pursuant to Article 74 of the Statute) ICC-01/05-01/08 (2016) [237].
[92] *The Prosecutor v Bosco Ntaganda* (Decision on Prosecution's Request for Admission of Documentary Evidence) ICC-01/04-02/06-1838 (28 March 2017) [68].
[93] *The Prosecutor v Édouard Karemera et al* (Decision on the Prosecutor's Motion for Admission of Certain Exhibits into Evidence) ICTR-98-44-T (25 January 2008) [8]; *The Prosecutor v Théoneste Bagosora et al* (Decision on Ntabakuze Motion to Deposit Certain United Nations Documents) ICTR-98-41-T (19 March 2007) [3]; *The Prosecutor v Augustin Ngirabatware* (Decision on Prosecution Motion for Admission of Documentary Evidence) ICTR-99-54-T (4 July 2012) [33].
[94] *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) (n 78) [22].
[95] ibid [34].
[96] ibid [35].
[97] ibid.
[98] Rome Statute art 69(4).
[99] ibid art 67(1)(c).
[100] *The Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecution's Bar Table Motions) (n 78) [41].

arms and the adequacy of time and resources when the defence lacks access to technologies that the prosecution has, for instance, to authenticate such evidence. A final concern may relate to the impact of bulk and/or late disclosure on the defendants' right to adequate facilities to prepare defence.[101]

7. Evaluation of Digital Evidence

The Rome Statute allows for a certain degree of flexibility in the admission and evaluation of evidence, as it provides that the presiding judge 'may give direction for the conduct of proceedings' including concerning the submission of evidence.[102] Building on this flexibility, Trial Chamber VII in *Bemba* determined that the assessment of relevance, probative value, and prejudicial effect, as well as the decision on objections on those grounds, can be deferred to the end of the trial, when all of the evidence submitted by the parties can be evaluated holistically.[103] The sole exception is when the objections raised relate to procedural bars, as in the case of challenges based on article 69(7) of the Rome Statute, or to the prerequisites of Rule 68 of the Rules of Procedure and Evidence.[104]

Even though the ICC adopted an 'admission' approach to the admissibility of evidence in its earlier jurisprudence,[105] whereby admissibility was determined at the point of submission, the Court has shifted to the 'submission' approach established in *Bemba* in all its recent trials.[106] Despite the shift to the submission approach, Chambers have maintained their discretion to

[101] See Sophie Rigney, *Fairness and Rights in International Criminal Procedure* (EUP 2022) 109ff, who discusses the impact of large volumes of material disclosed late on the rights of the accused, focusing on jurisprudence of the ICTY.
[102] Rome Statute art 64(8)(c).
[103] *The Prosecutor v Bemba et al* (Decision on Prosecution Requests for Admission of Documentary Evidence (ICC 01/05-01/13-1013-Red, ICC-01/05-01/13-1113-Red, ICC-01/05-01/13-1170-Conf)) ICC-01/05-01/13-1285 (24 September 2015) [9]; the approach was later confirmed by the appeals chamber *The Prosecutor v Jean-Pierre Bemba Gombo* (Judgment of 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') ICC-01/05-01/08-1386 (3 May 2011) [37].
[104] *The Prosecutor v Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Arido* (Judgment Pursuant to Article 74 of the Statute) ICC-01/05-01/13-1989-Red (19 October 2016) [191]
[105] For an overview of the approaches adopted by different ICC chambers, see Yvonne McDermott, *Proving International Crimes* (OUP 2024) 45–47; see also Fabricio Guariglia, ''Admission' v. 'Submission' of Evidence at the International Criminal Court: Lost in Translation?' (2018) 16 JICJ 315; Simon de Smet, 'All Roads Lead to Rome – Lifting the Veil on the ICC's Procedural Pluriformity' in Šturma Pavel (ed), *The Rome Statute of the ICC at its Twentieth Anniversary: Achievements and Perspectives* (Brill 2019) 193ff.
[106] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Trial Judgment) (n 43) [132]; *The Prosecutor v Dominic Ongwen* (Trial Judgment) (n 36) [237]; *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (Trial Judgment) (n 42) [23]; *The Prosecutor v Mahamat Said Abdel Kani* (Fourth Directions on the Conduct of Proceedings) ICC-01/14-01/21-932 (5 March 2025) [27]; *The Prosecutor v Ali Muhammad Ali Abd-al-Rahman ('Ali Kushayb')* (Directions on the Conduct of Proceedings) ICC-02/05-01/20-478 (4 October 2021) [25]; for an analysis of the strengths and weaknesses of the 'submission approach', see McDermott (n 105) 48ff.

decide on evidence admissibility upon its submission whenever necessary or appropriate to preserve the expeditiousness and fairness of proceedings, including upon request of the parties.[107] Indeed, while scarce, the ICC has rendered admissibility decisions on particularly important issues.[108]

Recent trial judgments give some indication of the factors to be taken into account when weighing digital evidence. While of course there is no formal requirement for corroboration in the ICC Statute, judgments indicate that whether the digital evidence is sufficiently corroborated by other evidence will be instructive. Corroboration may come in the form of expert analysis. In *Al Hassan*, for example, Trial Chamber X noted that videos had been examined by a geolocation expert 'who independently identified the likely locations at which the videos were filmed', and a metadata expert who indicated the 'file modification date/time' of the videos as well as corroboration through witnesses who identified the locations, and through other videos depicting the same scenesin finding videos to be reliable despite defence challenges to their authenticity and integrity.[109]

Authenticating audio-visual material includes requiring evidence of the item's originality and integrity and providing the whole recording instead of excerpts where possible.[110] Otherwise, chambers have stressed that recordings would need sufficient indicia that they are what they purport to be.[111] Witness testimony has been accepted as a means to authenticate photographs and video material.[112]

The chain of custody will also be a relevant factor in determining the weight to be given to digital evidence. Addressing defence challenges on the authenticity of Facebook material and call data records, Trial Chamber V in *Yekatom and Ngaïssona* was not persuaded by the argument that the lack of information 'concerning the domestic court processes and whether the materials were altered in any way' raised doubts about the material to render it inadmissible and was satisfied with its authenticity insofar as witnesses testified in Court on the

[107] *The Prosecutor v Laurent Gbagbo and Charles Blé Goudé* (Decision on the Submission and Admission of Evidence) ICC-02/11-01/15-405 (29 January 2016) [17].
[108] *The Prosecutor v Ali Muhammad Ali Abd-al-Rahman ('Ali Kushayb')* (Decision on the Defence Request to Admit Duncan Castellvi as an Expert Witness and to Introduce his Evidence under Rule 68(3) of the Rules (n 71).
[109] *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (Trial Judgment) (n 42) fn 2793, 3458.
[110] *The Prosecutor v Jean-Pierre Bemba Gombo* (Public Redacted Version of "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" of 6 September 2012) ICC-01/05-01/08-2299-Red (8 October 2012); *The Prosecutor v Jean-Pierre Bemba Gombo* (Public Redacted Version of "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" of 6 September 2012) ICC-01/05-01/08-2299-Red (8 October 2012) [120].
[111] ibid [122].
[112] *The Prosecutor v Dominic Ongwen* (Trial Judgment) (n 36) fn 4622; *The Prosecutor v Bosco Ntaganda* (Judgment Pursuant to Article 74) (n 36) [281]; *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (Trial Judgment) (n 42) fn 2793, 3458.

communications.[113] Indicia of authenticity of call data records may include corporate watermarks of the telecommunications provider, correspondence between the call logs and the number and the content of every communication in evidence, expert testimony on the call data records' origins, and information on the authenticity and chain of custody.[114] Factors that have been found to support call data records' reliability include the automated collection of the information 'in the ordinary course of business', that their collection and decoding are overseen by specialised staff, and that call data records in raw form cannot be altered, guaranteeing their authenticity.[115] However, this presumption of reliability can be rebutted 'by showing specific examples of irregularities in the collection, storing, formatting and/or transmission of the evidence'.[116]

Nevertheless, the completeness of digital evidence and what can realistically be inferred from it will be another key factor. For example, call data records may show that communications occurred, but they are of limited relevance in the absence of further evidence about the content and purpose of the concerned conversations.[117] In *Yekatom and Ngaïssona,* Trial Chamber V found that in the absence of a statement or testimony from an individual participating in Facebook communications, authoring a post, or otherwise having information about the contents, Facebook Material has little probative value.[118] Additionally, the Chamber expressed that it would not make any determinations of facts solely based on Facebook evidence.[119] Reflecting on the use of Facebook IP logs, the Chamber considered that – in the absence of a statement of testimony from a witness who participated in Facebook communications or authored a post – it also could not conclusively determine who participated in those exchanges or created the posts.[120] The Chamber additionally found that Facebook IP logs do not suffice for determining the location of individuals,[121] and that call data records are insufficient for attributing a phone number or handset to a given individual or for proving the occurrence of a conversation without corroborating information.[122]

---

[113] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Trial Judgment) (n 43) [148–149].
[114] *The Prosecutor v Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Arido* (Judgment Pursuant to Article 74 of the Statute) (n 104) [219–223].
[115] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Trial Judgment) (n 43) [170], [174].
[116] ibid [183].
[117] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Corrected Version of 'Decision on the Confirmation of Charges against Alfred Yekatom and Patrice-Edouard Ngaïssona') ICC-01/14-01/18-403-Corr-Red (28 June 2021) [180].
[118] *The Prosecutor v Alfred Yekatom and Patrice-Edouard Ngaïssona* (Trial Judgment) (n 43) [154].
[119] ibid [2130], [2180].
[120] ibid [151].
[121] ibid.
[122] ibid [188–189].

Some trial chambers have found that in-court authentication or authentication through witness testimony is not an absolute requirement for establishing the authenticity of audio-visual material.[123] However, Trial Chamber VI in *Ntaganda* found that documentary evidence should, where possible, be tendered through a witness and that the absence of authentication by a witness might impact the item's admissibility.[124] Even though failure to tender a document through a witness would not, in and of itself, prevent it from being tendered from the bar table, a party wishing to admit evidence without introducing it through a witness would need to provide the reasons for not doing so.[125] In *Al Hassan*, Trial Chamber X in its majority found that there are no requirements under the Rome Statute for the authentication of documentary material nor any obligation to submit it through a witness.[126] However, the majority also noted that the absence of evidence as to the circumstances of an audio recording's creation and the lack of opportunity to examine its source reduced the probative value of the piece of evidence.[127] In *Abd-Al-Rahman*, fairness considerations also led the Chamber to not rely on Facebook evidence. The Prosecution had sought to place this material on the record through its examination of a Defence expert witness. The Chamber found this approach unsatisfactory, as the witness had not been given advance notice of the material on which he was asked to comment.[128]

8. Conclusion

The foregoing analysis shows that digital evidence – broadly defined as material created, edited, stored or communicated through digital means – has played a crucial role in international criminal trials since Nuremberg. Newer forms of digital evidence, including satellite imagery, telecommunications data, and audio-visual content created by non-professionals, has come to the fore in recent years, with several ICC cases setting out principles for the admission and evaluation of this kind of evidence. Nevertheless, practice is patchy and inconsistent, not least owing to the different approaches to the admission of evidence taken by different chambers.

[123] *The Prosecutor v Jean-Pierre Bemba Gombo* (Public Redacted Version of "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" of 6 September 2012) (n 110) [120] ('recordings that have not been authenticated in court can still be admitted, as in-court authentication is but one factor for the Chamber to consider when determining an item's authenticity and probative value').
[124] *The Prosecutor v Bosco Ntaganda* (Decision on Prosecution's Request for Admission of Documentary Evidence) (n 92) [13].
[125] ibid [13–14].
[126] *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* (Trial Judgment) (n 42) fn 2793.
[127] ibid fn 2793.
[128] *The Prosecutor v Abd-Al-Rahman* (Trial Judgment) ICC-02/05-01/20-1240 (6 October 2025) [232–235].

Some have decided on the admissibility of evidence at the time of its introduction, while others have deemed all items presented by the parties to have been 'submitted', and only considering its relevance and admissibility at the end of trial.[129]

It is essential for the ICC to establish and implement rigorous standards and protocols for verifying the authenticity of different forms of digital evidence.[130] Such standards would give clarity to the parties to proceedings, and also to those civil society organisations preserving digital evidence in the hope that the material might be used in international criminal trials one day. It is also particularly necessary in an era of deepfakes and widespread misinformation, both to avoid judges from giving undue weight to a piece of fake evidence, but also to prevent real user-generated content from being unduly disregarded because of a fear of deception.[131] Relatedly, further guidance on expert witnesses is required and could be developed by the judges as an annex to the Chambers Practice Manual. This guidance could incorporate what kind of expert evidence may be needed to authenticate different types of (digital) evidence, what qualifications or experience are needed to qualify as an expert,[132] and whether the parties must 'put their case' to expert witnesses[133] and provide advance notice of questions and material to be produced in cross-examination, as was recently held in *Abd-Al-Rahman*.[134] Digital evidence has the capacity to transform international criminal trial, but its challenges must be carefully weighed against its benefits. Further guidance and standardised protocols, and training of legal professionals and judges, will copper-fasten the important role of digital evidence for years to come.

[129] See further, Guariglia (n 105); McDermott, *Proving International Crimes* (n 105) 39–64.
[130] See also, Hak (n 25); Maria-Paz Sandoval et al, 'Threat of Deepfakes to the Criminal Justice System: A Systematic Review' (2024) 13(41) Crime Science, 9.
[131] See Daragh Murray et al, 'Evaluating Digital Open Source Imagery: A Guide for Judges and Fact-Finders'(2024) <www.trueproject.co.uk/osguide> accessed 16 December 2025.
[132] Gillett and Fan (n 17).
[133] Grahame Aldous, 'Truth and Fairness: Challenging Evidence in International Justice and The Rule in *Browne v. Dunn'* (2025) 25(4) Int Crim L Rev 652.
[134] *The Prosecutor v Abd-Al-Rahman* (Trial Judgment) [232–235].