المجلة المغربية للدراسات القانونية والاقتصادية
ISSN(P) : 1142-2489
V2, Numéro 25, MARS 2026
REMEJE
المجلد 2، العدد 25، مارس 2026
ISSN(E) : 3085-4555
Revue Marocaine des Eudes Juridiques et Economiques

The Use of Digital Evidence and Open-Source Intelligence (OSINT) in International Criminal Investigations and Prosecutions

Almoatuz A. Munsoor
Associate Professor of Public International Law University of Jeddah,
e.mail: aaadam@uj.edu.sa

ملخص

أحدث التطور التكنولوجي تحولاً جذرياً في مجال العدالة الجنائية الدولية، إذ أدخل منهجيات متطورة لجمع الأدلة وتحليلها، لم تكن لتخطر على بال أحد قبل عقدين من الزمن. يبحث هذا البحث في الاعتماد المتزايد على الأدلة الرقمية ومعلومات المصادر المفتوحة في التحقيق في الجرائم الدولية ومقاضاة مرتكبيها، بما في ذلك الإبادة الجماعية، والجرائم ضد الإنسانية، وجرائم الحرب، والإرهاب. ومن خلال تحليل شامل لقضايا حديثة أمام المحاكم الدولية والمحاكم المختلطة، تُبين هذه الدراسة كيف أصبحت معلومات المصادر المفتوحة والأدلة الجنائية الرقمية أدوات لا غنى عنها في توثيق الفظائع الجماعية وتحديد المسؤولية الجنائية الفردية. يستكشف البحث الأطر القانونية التي تحكم قبول الأدلة الرقمية، والتحديات التقنية المرتبطة بالمصادقة والتحقق، والاعتبارات الأخلاقية المتعلقة بالخصوصية وحماية البيانات. وبالاستناد إلى السوابق القضائية للمحكمة الجنائية الدولية، والمحكمة الجنائية الدولية ليوغوسلافيا السابقة، ومحاكم محلية مختلفة تمارس اختصاصاً عالمياً، يكشف هذا العمل عن الإمكانات التحويلية والقيود الكامنة في جمع الأدلة بوساطة التكنولوجيا. تشير النتائج إلى أنه على الرغم من أن الأدلة الرقمية قد عززت بشكل كبير قدرات الادعاء، لا سيما في مناطق النزاع حيث يتعذر إجراء التحقيقات التقليدية، إلا أن تحديات كبيرة لا تزال قائمة فيما يتعلق بسلسلة الحفظ، والتحقق من البيانات الوصفية، والفجوة الرقمية التي تؤثر على إمكانية الوصول إلى الأدلة. يساهم هذا البحث في المناقشات الجارية حول معايير الأدلة في القانون الجنائي الدولي، ويقترح توصيات لتطوير أطر عمل متينة توازن بين الابتكار التكنولوجي وحماية الحقوق الأساسية.

الكلمات المفتاحية: الأدلة الرقمية، الاستخبارات مفتوحة المصدر، القانون الجنائي الدولي، جرائم الحرب، المحكمة الجنائية الدولية، الأدلة الجنائية الرقمية، أدلة وسائل التواصل الاجتماعي، المصادقة، المقبولية.

Abstract

The evolution of technology has fundamentally transformed the landscape of international criminal justice, introducing sophisticated methodologies for evidence collection and analysis that were unimaginable merely two decades ago. This research examines the increasing reliance on digital evidence and open-source intelligence in investigating and prosecuting international crimes, including genocide, crimes against humanity, war crimes, and terrorism. Through comprehensive analysis of recent cases before international tribunals and hybrid courts, this study demonstrates how OSINT and digital forensics have become

indispensable tools in documenting mass atrocities and establishing individual criminal responsibility. The research explores the legal frameworks governing the admissibility of digital evidence, the technical challenges associated with authentication and verification, and the ethical considerations surrounding privacy and data protection. Drawing upon case law from the International Criminal Court, the International Criminal Tribunal for the former Yugoslavia, and various domestic courts exercising universal jurisdiction, this work reveals both the transformative potential and inherent limitations of technology-mediated evidence gathering. The findings indicate that while digital evidence has significantly enhanced prosecutorial capabilities, particularly in conflict zones where traditional investigations prove impossible, substantial challenges remain regarding chain of custody, metadata verification, and the digital divide affecting evidence accessibility. This research contributes to ongoing discussions about evidence standards in international criminal law and proposes recommendations for developing robust frameworks that balance technological innovation with fundamental rights protections.

Keywords: digital evidence, open-source intelligence, OSINT, international criminal law, war crimes, ICC, digital forensics, social media evidence, authentication, admissibility

1. Introduction

The proliferation of digital technologies and the exponential growth of information available through open sources have revolutionized criminal investigations across all jurisdictions, yet nowhere has this transformation been more profound than in the realm of international criminal justice. International crimes, by their very nature, present unique investigative challenges that distinguish them from ordinary domestic offenses. These crimes typically occur during armed conflicts or systematic campaigns of violence, often in territories where state structures have collapsed or where governments themselves are perpetrators. Traditional investigative methods, which rely heavily on physical evidence collection, witness interviews, and cooperation from local authorities, frequently prove inadequate or entirely impossible in such contexts (Dubberley et al., 2020).

The emergence of digital evidence and open-source intelligence has fundamentally altered this investigative paradigm. Millions of individuals now possess smartphones capable of capturing high-resolution images and videos, which are instantly uploaded to social media platforms accessible worldwide. This democratization of information has created an unprecedented documentary record of human rights violations and international crimes as they unfold. Simultaneously, satellite imagery, communication intercepts, and digital metadata provide investigators with tools to establish patterns of violence, command responsibility, and geographic scope of atrocities with precision previously unattainable (Freeman, 2020).

The importance of this research lies in addressing the critical gap between technological capabilities and legal frameworks. While digital evidence has been utilized in various international criminal proceedings, comprehensive analysis of its admissibility standards, authentication requirements, and evidentiary weight remains underdeveloped in academic literature. Furthermore, the rapid pace of technological advancement continually introduces new forms of digital evidence and investigative techniques that challenge existing legal doctrines developed in analog contexts.

This study examines three interconnected dimensions of digital evidence and OSINT in international criminal justice. First, it analyzes the technical aspects of collecting, preserving, and authenticating digital evidence from diverse sources including social media platforms, satellite imagery, and communication data. Second, it explores the legal frameworks governing admissibility of such evidence before international tribunals, examining relevant case law and procedural rules. Third, it investigates the practical challenges and ethical considerations that arise when utilizing digital evidence, including issues of privacy, security of sources, and potential manipulation.

The research methodology employs doctrinal legal analysis of international criminal law instruments, jurisprudence from international and hybrid tribunals, and examination of technical standards developed by forensic experts and human rights organizations. Case studies of specific prosecutions illuminate how digital evidence has been deployed in practice and reveal emerging trends in judicial interpretation of admissibility criteria.

The contemporary relevance of this research cannot be overstated. Recent conflicts in Syria, Ukraine, Myanmar, and Ethiopia have generated massive volumes of digital

documentation of alleged war crimes and crimes against humanity. Organizations such as the Syrian Archive, Bellingcat, and Mnemonic have pioneered methodologies for preserving and analyzing this material, creating databases that support accountability mechanisms (Koettl, 2018). The International Criminal Court has increasingly relied upon digital evidence in its investigations, while domestic courts exercising universal jurisdiction have admitted social media posts and satellite imagery as proof of international crimes. Understanding the evidentiary standards, technical requirements, and legal principles governing such evidence is essential for practitioners, scholars, and policymakers engaged in international criminal justice.

2. Conceptual Framework and Definitions

Understanding the application of digital evidence and OSINT in international criminal proceedings requires precise definition of key concepts and establishment of analytical frameworks that distinguish these evidentiary categories from traditional forms of proof.

Digital evidence encompasses any information stored or transmitted in binary form that may be relied upon in legal proceedings. In international criminal contexts, this definition extends to photographs and videos captured on smartphones, communications transmitted through messaging applications, geolocation data from mobile devices, documents stored on computers or servers, metadata embedded in digital files, and information extracted from social media platforms (Casey, 2011). The International Organization for Standardization defines digital evidence more technically as data stored or transmitted using a computer system that a party seeks to introduce to support or refute a position in legal proceedings (ISO/IEC 27037:2012).

The distinguishing characteristic of digital evidence lies not merely in its format but in its inherent properties that differ fundamentally from physical evidence. Digital information is extraordinarily volatile, easily altered without leaving obvious traces, and requires specialized technical expertise for proper collection and preservation. Unlike physical evidence, digital files can be perfectly replicated, exist simultaneously in multiple locations, and may be recovered even after apparent deletion (Sommer, 2008). These properties create both opportunities and challenges for international criminal investigations, necessitating development of specific protocols for handling such material.

Open-source intelligence represents a distinct but overlapping category, referring to information collected from publicly available sources that is analyzed to produce actionable intelligence. The NATO Open Source Intelligence Handbook defines OSINT as intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (NATO, 2001). In international criminal investigations, OSINT sources include news reports, social media posts, satellite imagery available through commercial providers, public government documents, academic publications, and information shared on online forums and platforms.

The relationship between digital evidence and OSINT merits careful delineation. While all OSINT is digital in contemporary practice, not all digital evidence originates from open sources. Communications obtained through lawful interception, data seized from

electronic devices, and information requiring authentication credentials for access constitute digital evidence but not open-source intelligence. Conversely, a video of an alleged war crime uploaded to YouTube represents both digital evidence and OSINT, as it is publicly accessible yet requires digital forensic analysis for authentication and interpretation (Alexa Koenig et al., 2014).

International crimes, the substantive focus of this research, possess specific definitions under international law. The Rome Statute of the International Criminal Court defines four categories of crimes within the Court's jurisdiction: genocide, crimes against humanity, war crimes, and the crime of aggression (Rome Statute, 1998). Each category encompasses specific prohibited acts with distinct elements that prosecution must establish beyond reasonable doubt. Genocide requires proof of acts committed with intent to destroy, in whole or in part, a national, ethnical, racial, or religious group. Crimes against humanity involve widespread or systematic attacks directed against civilian populations. War crimes encompass grave breaches of the Geneva Conventions and other serious violations of laws and customs applicable in armed conflict.

The evidentiary requirements for proving these crimes create particular demands upon investigative methodologies. Establishing the contextual elements of crimes against humanity, for instance, necessitates demonstrating that individual acts occurred within a widespread or systematic attack, requiring evidence of scale, organization, and patterns that digital sources can uniquely illuminate (Prosecutor v. Katanga, 2014). Similarly, proving command responsibility requires evidence of superior-subordinate relationships, knowledge of subordinate crimes, and failure to prevent or punish, elements that may be established through digital communications and organizational documentation (Prosecutor v. Bemba, 2016).

The integration of digital evidence into international criminal proceedings builds upon established evidentiary principles while adapting them to technological realities. Traditional concepts such as relevance, probative value, and reliability remain fundamental, yet their application to digital materials requires new interpretative approaches. The principle of "best evidence," which historically preferred original documents over copies, must be reconceptualized when dealing with digital files that exist only as data patterns on storage media (Chaffee, 2018).

3. Evolution of Digital Evidence in International Criminal Justice

The trajectory of digital evidence in international criminal proceedings reflects broader technological transformations in society while revealing the adaptive capacity and limitations of international legal institutions. Tracing this evolution illuminates how contemporary practices emerged and identifies persistent challenges requiring resolution.

The International Criminal Tribunal for Rwanda and the International Criminal Tribunal for the former Yugoslavia, established in the 1990s, conducted their investigations and prosecutions predominantly using traditional evidence gathering methodologies. Witnesses provided oral testimony, documentary evidence consisted of paper records, and photographic evidence was submitted in physical format. The technological infrastructure of these tribunals reflected their era, with limited capacity for handling electronic materials

(Wald, 2002). Nevertheless, these institutions laid crucial groundwork for later developments by establishing flexible evidentiary rules that would prove adaptable to digital materials.

The ICTY's Rules of Procedure and Evidence adopted a relatively liberal approach to admissibility, permitting any relevant evidence with probative value unless its admission would be antithetical to the rules or rights of the accused (ICTY RPE, Rule 89). This flexible framework, created primarily to accommodate the civil law and common law traditions represented among tribunal judges, inadvertently created space for innovative evidence forms as technology advanced (May & Wierda, 2002).

Early instances of digital evidence in international proceedings involved relatively simple materials such as computer-generated documents and databases compiled by investigators. In Prosecutor v. Kordić and Čerkez, the ICTY admitted evidence derived from computer analysis of witness statements and documents, establishing that electronically stored information could be treated similarly to traditional documentary evidence provided proper authentication (Prosecutor v. Kordić and Čerkez, 2004). These initial steps were tentative, focusing on digital storage of conventional information rather than distinctively digital evidence forms.

The establishment of the International Criminal Court in 2002 coincided with the acceleration of digital technology adoption globally, yet the Rome Statute and ICC Rules of Procedure and Evidence contained no specific provisions addressing digital evidence. The Rules replicated the flexible admissibility standard pioneered by the ad hoc tribunals, providing that the Court may consider evidence it deems relevant and necessary while possessing discretion to reject evidence if its probative value is substantially outweighed by prejudicial effect (ICC RPE, Rule 69). This intentional flexibility has permitted the ICC to adapt its evidentiary practices as digital materials have become increasingly central to investigations.

The Syria conflict, which began in 2011, marked a watershed moment for digital evidence in international criminal accountability efforts. Unlike previous conflicts, Syria witnessed unprecedented documentation by civilians equipped with smartphones and internet connectivity. Syrians uploaded hundreds of thousands of videos and images depicting alleged war crimes and crimes against humanity to social media platforms, creating a vast digital archive of human rights violations (Bellingcat Investigation Team, 2021). This material presented both extraordinary opportunities and novel challenges for accountability mechanisms.

Traditional investigation in Syria proved largely impossible due to lack of territorial access and absence of government cooperation. International commissions of inquiry, human rights organizations, and nascent accountability units within European prosecution services turned to digital evidence as their primary investigative tool. The Syrian Archive, established in 2014, pioneered methodologies for preserving and verifying social media documentation, collecting over 3.5 million videos and developing protocols for authentication and cataloging (Syrian Archive, 2021).

European domestic courts exercising universal jurisdiction became testing grounds for admissibility of this new evidence. German courts, particularly active in prosecuting Syrian

nationals for international crimes, admitted social media videos, photographs, and communications as evidence in several landmark cases. In the trial of Eyad A. before the Koblenz Higher Regional Court, prosecutors relied substantially upon digital evidence including videos the defendant had shared on social media and communications recovered from his devices (Koblenz Higher Regional Court, 2021). The court's acceptance of this material, subject to rigorous authentication, established important precedents for digital evidence admissibility.

The ICC's approach to digital evidence evolved substantially during this period. In Prosecutor v. Bemba et al., charges were brought regarding witness tampering and presentation of false evidence, with prosecution relying heavily on digital communications and call data records to establish the alleged conspiracy (Prosecutor v. Bemba et al., 2016). Although the Appeals Chamber ultimately reversed the convictions on substantive grounds, the case demonstrated the Court's capacity to handle complex digital evidence requiring technical expertise for interpretation.

Satellite imagery emerged as another crucial digital evidence form, particularly valuable for establishing large-scale patterns of destruction and documenting attacks on civilian infrastructure. The ICC utilized satellite imagery extensively in its investigation of crimes in Darfur, employing analysis by the American Association for the Advancement of Science to document village destruction (AAAS, 2012). Commercial satellite providers offering high-resolution imagery created new possibilities for remote monitoring of conflict zones, enabling investigators to track developments without territorial access.

The development of specialized organizations focused on digital evidence preservation and analysis represents another significant evolution. Bellingcat, founded in 2014, demonstrated the potential of open-source investigation techniques through groundbreaking work identifying perpetrators of the MH17 downing over Ukraine using publicly available materials including social media posts, satellite imagery, and photographic analysis (Bellingcat, 2016). Their methodologies, combining technical expertise with traditional investigative techniques, established new standards for OSINT-based accountability research.

The establishment of the Independent Investigative Mechanism for Myanmar in 2018 and the International, Impartial and Independent Mechanism for Syria in 2011 reflected institutional recognition that conflicts characterized by limited territorial access required new investigative approaches centered on digital evidence collection. These mechanisms prioritized building capacity for analyzing vast quantities of digital material, employing data scientists and digital forensic experts alongside traditional investigators (IIIM, 2020).

The ICC's Policy on Children reinforced the importance of digital evidence while highlighting associated risks, noting that digital technologies create new opportunities for documenting crimes affecting children but also pose dangers of re-traumatization through circulation of exploitative material (ICC, 2016). This policy demonstrated growing sophistication in balancing evidentiary value against protection concerns specific to digital materials.

Recent developments include increasing use of blockchain technology for evidence preservation, ensuring immutability and creating verifiable chains of custody for digital

materials. Organizations such as Hala Systems have deployed sensor networks in conflict zones that automatically record airstrikes and attacks, generating data with embedded authentication features (Hala Systems, 2019). Artificial intelligence and machine learning applications are being developed to analyze massive digital evidence collections, identifying patterns and relevant materials that would be impossible to detect through manual review.

4. Technical Aspects of Digital Evidence Collection and Preservation

The technical dimensions of digital evidence in international criminal investigations encompass specialized methodologies for identification, collection, preservation, and analysis of electronic materials. Understanding these technical aspects is essential for evaluating evidentiary reliability and developing appropriate legal standards for admissibility.

Digital evidence collection begins with identification of relevant sources. In contemporary conflicts, potential sources include social media platforms hosting user-generated content, commercial satellite imagery providers, telecommunications companies maintaining call detail records, internet service providers logging connection data, cloud storage services, messaging applications, and devices seized from suspects or crime scenes (Molina, 2020). Each source presents distinct technical challenges and requires specialized collection techniques.

Social media platforms constitute increasingly important evidence sources, yet their architecture complicates collection efforts. Content uploaded to platforms such as YouTube, Facebook, Twitter, and Telegram may be deleted by users or removed by platform administrators, either immediately or years after posting. Platforms regularly modify their interfaces and application programming interfaces, affecting collection tool functionality. Terms of service restrictions may prohibit automated data collection, creating legal and practical obstacles for investigators (Roberts, 2017).

Organizations addressing these challenges have developed sophisticated preservation systems. The Syrian Archive's methodology involves identifying relevant content through keyword searches and geolocation parameters, downloading videos with associated metadata, calculating cryptographic hash values to ensure file integrity, and storing materials in secure repositories with multiple backups (Syrian Archive, 2021). Hash values, generated through algorithms such as SHA-256, create unique digital fingerprints for files, enabling verification that content has not been altered during storage or transmission.

Metadata preservation represents a critical technical consideration often overlooked in early digital evidence collection efforts. Metadata includes information about when files were created, who created them, what devices were used, geographic coordinates where images were captured, and modification history (Turner, 2019). This contextual information may prove as valuable as content itself for establishing authenticity and relevance. However, metadata can be easily lost through improper handling, stripped when files are converted between formats, or deliberately falsified to deceive investigators.

Satellite imagery introduces distinct technical considerations. Commercial providers such as Maxar Technologies, Planet Labs, and Airbus Defence and Space offer imagery at resolutions sufficient to identify individual vehicles, structures, and military equipment. Effective utilization requires expertise in remote sensing, geospatial analysis, and

understanding of satellite orbital mechanics (Marx & Goward, 2013). Analysts must account for factors affecting image interpretation including atmospheric conditions, sensor limitations, viewing angles, and temporal resolution. Synthetic aperture radar imagery, which penetrates cloud cover, requires specialized interpretation techniques but enables monitoring of regions with persistent cloud coverage.

Authentication of digital materials presents fundamental technical challenges distinct from those encountered with physical evidence. Digital files can be perfectly duplicated, making concepts of "original" and "copy" problematic. Files may be edited using sophisticated software that leaves no obvious traces of manipulation. Deep fake technologies can generate synthetic images and videos of events that never occurred, with detection requiring advanced forensic analysis (Chesney & Citron, 2019).

Digital forensic experts employ multiple techniques to authenticate materials and detect manipulation. Examination of metadata fields may reveal inconsistencies indicating alteration, such as creation dates preceding device manufacture dates or software version numbers incompatible with file formats. Analysis of compression artifacts in images and videos can identify signs of editing, as repeated compression leaves detectable patterns. Examination of error level analysis reveals areas within images that have been saved at different quality levels, suggesting selective editing (Farid, 2016).

Geolocation verification represents another crucial authentication dimension. Videos and images purporting to depict specific locations must be verified to ensure they actually show claimed areas. Techniques include matching architectural features, vegetation patterns, terrain characteristics, signage, and landmarks visible in materials against reference imagery from verified sources such as Google Street View or satellite imagery. Shadow analysis can verify time of day and season, while celestial positioning can determine possible dates and locations (Brown, 2020).

Chain of custody documentation, fundamental in all criminal investigations, assumes heightened importance with digital evidence given ease of alteration. Comprehensive documentation must track who accessed materials, when access occurred, what actions were performed, and what controls prevented unauthorized access or modification. Forensic imaging of devices creates exact bit-by-bit copies using write-blocking hardware that prevents alteration of original media. Hash values calculated at each transfer point verify that files remain unchanged through investigative processes (Carrier, 2005).

Encryption presents significant technical obstacles to evidence collection. Suspects may encrypt device storage or communications using strong cryptographic algorithms that are effectively unbreakable without access to decryption keys. Investigators may employ forensic techniques to recover encryption keys from device memory, attempt to obtain keys through legal process, or utilize vulnerabilities in encryption implementations, yet increasingly robust encryption technologies limit these approaches (Kerr, 2018).

Cloud storage introduces jurisdictional and technical complexities. Digital evidence may be physically stored on servers in multiple countries, subject to various legal regimes governing access. Cloud service providers may lack technical capability to retrieve specific user data if end-to-end encryption is employed. International legal assistance procedures for

obtaining cloud-stored evidence are often cumbersome and time-consuming, potentially allowing evidence destruction before collection (Daskal, 2015).

The volume of digital evidence in international criminal investigations creates substantial technical challenges. Syrian conflict documentation exceeds several petabytes, far beyond human capacity for manual review. Investigators employ database systems, content management platforms, and increasingly artificial intelligence tools to organize, search, and analyze massive collections. Machine learning algorithms can classify content, identify relevant materials based on training data, and recognize patterns invisible to human reviewers (Skelton, 2020).

Quality assurance protocols must address risks of data loss, corruption, or misidentification. Redundant storage systems, regular integrity checks using hash verification, and documented preservation workflows minimize these risks. Organizations such as the Human Rights Data Analysis Group have developed specialized software tools for human rights evidence management, incorporating features specifically designed for international criminal investigation requirements (Ball, 2020).

5. Legal Frameworks Governing Admissibility of Digital Evidence

The admissibility of digital evidence in international criminal proceedings is governed by legal frameworks that balance procedural flexibility with fundamental fairness requirements. These frameworks have evolved through interpretation of general evidentiary rules originally drafted without specific contemplation of digital materials, creating both opportunities for innovation and risks of inconsistent application.

The Rome Statute establishes the International Criminal Court's foundational admissibility principles without differentiating between evidence types. Article 69(3) provides that the Court shall have authority to request submission of all evidence that it considers necessary for determination of truth, while Article 69(4) permits the Court to rule on relevance or admissibility of evidence, taking into account inter alia the probative value and any prejudice that such evidence may cause to a fair trial (Rome Statute, 1998). This broad formulation delegates substantial discretion to judges in evaluating whether particular evidence should be admitted.

Rule 63(2) of the ICC Rules of Procedure and Evidence reinforces procedural flexibility, stating that a Chamber shall not apply national laws governing evidence except as specified in the Rules. Rule 69(4) authorizes the Court to assess freely all evidence submitted in order to determine its relevance or admissibility. This departure from strict adherence to common law or civil law evidentiary traditions reflects the Court's hybrid character and enables adaptation to emerging evidence forms (Ambos, 2015).

The threshold question for any evidence, including digital materials, involves relevance. Evidence is relevant if it tends to prove or disprove a fact in issue or affects the credibility of witnesses. Digital evidence may establish elements of crimes, demonstrate patterns of conduct, corroborate witness testimony, impeach witness credibility, or prove contextual circumstances necessary for crime characterization (Hamdani & Maldonado, 2020). A video depicting destruction of religious buildings may be relevant to proving

persecution as a crime against humanity, while geolocation data from a mobile device may be relevant to establishing presence at crime scenes.

Beyond relevance, admissibility requires sufficient probative value. Probative value depends upon evidence reliability and its tendency to prove matters of consequence to the case. For digital evidence, reliability hinges substantially on authentication, whether the evidence is what its proponent claims it to be. Authentication may be established through various means including testimony of witnesses with knowledge of evidence origin, expert analysis of technical characteristics, comparison with authenticated specimens, or distinctive characteristics combined with circumstances (ICC RPE, Rule 64).

The International Criminal Tribunal for the former Yugoslavia developed important jurisprudence regarding authentication standards applicable to digital evidence. In Prosecutor v. Popović et al., the Trial Chamber addressed authentication of intercepts of military communications, holding that authentication could be established through testimony of intercept operators, technical evidence regarding recording equipment and procedures, content analysis showing distinctive terminology and speech patterns, and corroboration through other evidence (Prosecutor v. Popović et al., 2010). This multi-factorial approach, emphasizing convergence of authentication indicia rather than requiring any single type of proof, has influenced subsequent treatment of digital evidence authentication.

The ICC has similarly adopted flexible authentication standards while requiring rigorous foundational showings for contested materials. In Prosecutor v. Katanga, the Trial Chamber admitted videos downloaded from the internet after prosecution provided evidence regarding when and how materials were obtained, hash values establishing file integrity, and expert analysis confirming metadata consistency with claimed date and location (Prosecutor v. Katanga, 2014). The Chamber emphasized that authentication required showing, on balance of probabilities, that evidence was what it purported to be, but authentication standards should not be so rigid as to exclude probative evidence merely because some uncertainty remained.

The probative value assessment must weigh potential prejudice against evidentiary worth. Digital evidence may carry particular prejudicial risks including inflammatory content that might improperly influence judges, privacy violations, or risks to witness security if materials reveal information about protected individuals (Zawati, 2014). Rule 69(4) of the ICC Rules specifically requires consideration of potential prejudice to fair trial, providing authority to exclude evidence even if relevant and reliable when prejudicial effect substantially outweighs probative value.

Hearsay considerations apply distinctively to digital evidence in international criminal proceedings. Unlike many domestic systems that strictly regulate hearsay, international criminal tribunals generally admit out-of-court statements, assessing their reliability and weight rather than excluding them categorically. The ICTY Appeals Chamber in Aleksovski held that hearsay evidence is not inadmissible per se, with the Trial Chamber required to assess whether the evidence is reliable for the purpose for which it is tendered (Prosecutor v. Aleksovski, 2000). This approach permits admission of social media posts, videos uploaded by unknown individuals, and other digital materials containing statements not subject to cross-examination.

The weight accorded to digital hearsay depends upon indicia of reliability. Corroboration through independent sources, internal consistency, technical authentication, and circumstantial evidence regarding likely accuracy all affect evidentiary weight. A video uploaded anonymously showing alleged atrocities might carry substantial weight if multiple independent sources captured similar events from different angles, technical analysis confirmed the video was recorded at the claimed location and time, and satellite imagery corroborated destruction visible in the video.

Expert evidence plays a crucial role in digital evidence admissibility and interpretation. Technical experts may testify regarding authentication, explaining forensic analysis of metadata, satellite imagery interpretation, or geolocation verification. Rule 68 of the ICC Rules governs expert evidence, permitting parties to submit written expert reports and requiring experts to assist the Court impartially (ICC RPE, Rule 68). The rapid evolution of digital forensic techniques creates challenges in establishing expert qualifications and evaluating reliability of novel methodologies not yet broadly accepted within relevant technical communities.

Disclosure obligations intersect with digital evidence in complex ways. The ICC Statute requires prosecution to disclose to defense evidence in prosecution possession or control that tends to show innocence of the accused or mitigate guilt (Rome Statute, Article 67(2)). When prosecution possesses massive digital evidence collections, identifying exculpatory material becomes technologically and practically challenging. The Katanga Trial Chamber addressed this issue by requiring prosecution to employ search methodologies designed to identify potentially exculpatory evidence within large databases, though not requiring manual review of every item (Prosecutor v. Katanga, 2013).

Privacy and data protection considerations increasingly affect digital evidence admissibility. The ICC Regulations of the Court recognize that evidence collection must respect internationally recognized human rights, including privacy rights (ICC Regulations, Regulation 46). Materials obtained through unlawful surveillance, hacking, or other rights violations may be excluded even if relevant and reliable. However, international criminal courts balance privacy interests against the serious nature of crimes under investigation, generally permitting admission of evidence obtained by third parties even if collection methods raised privacy concerns, while excluding evidence obtained through serious rights violations by investigators themselves (Cryer et al., 2019).

6. Open-Source Intelligence Methodologies in International Criminal Investigations

Open-source intelligence has evolved from supplementary investigative technique to central methodology in international criminal investigations, driven by technological developments that have made vast information resources publicly accessible while creating new analytical challenges requiring specialized expertise.

OSINT methodologies in international criminal contexts encompass systematic collection, verification, analysis, and preservation of publicly available information relevant to alleged crimes. The scope of available sources has expanded dramatically with internet

proliferation. Traditional OSINT sources included published news reports, government statements, academic publications, and public records. Contemporary OSINT additionally encompasses social media platforms, video sharing sites, photographic databases, satellite imagery, mapping services, online forums, messaging applications with public channels, flight tracking services, maritime vessel tracking, weapons identification databases, and numerous specialized data sources (Caligiuri & Torres Soriano, 2018).

Social media platforms serve as particularly rich OSINT sources for conflict documentation. Individuals present in conflict zones upload real-time documentation of events, often without awareness that materials may serve evidentiary purposes. Platforms host millions of videos and images depicting armed conflicts, attacks on civilians, destruction of property, and other conduct potentially constituting international crimes. The Syrian Archive alone has preserved over 3.5 million videos from the Syrian conflict, representing an unprecedented historical record (Syrian Archive, 2021).

Effective exploitation of social media OSINT requires sophisticated collection strategies. Manual searching proves inadequate given the volume of relevant content. Investigators employ automated collection tools that monitor specific hashtags, keywords, geographic locations, and user accounts. Application programming interfaces provided by platforms enable programmatic access to content, though API limitations and platform policies restrict collection capabilities. Collection must occur promptly, as users frequently delete content and platforms remove materials deemed violative of community standards (Golovchenko et al., 2020).

Verification constitutes the critical challenge in OSINT utilization for criminal accountability. Anyone can upload content to the internet claiming it depicts particular events, yet without verification such materials lack evidentiary value. Verification methodologies combine technical analysis with traditional investigative techniques. Geolocation verification involves identifying the precise location where images or videos were captured through analysis of distinctive features. Investigators compare architectural details, terrain, vegetation, signage, landmarks, and other observable characteristics against reference materials including satellite imagery, street view photography, and verified photographs of locations (Silverman et al., 2020).

Chronolocation establishes when content was created or when depicted events occurred. Metadata embedded in digital files may include creation timestamps, though such data can be falsified or lost through file processing. Alternative chronolocation techniques include shadow analysis using sun position calculations, verification that weather conditions visible in materials match meteorological records, identification of seasonal vegetation states, analysis of visible clothing, and cross-referencing with dated events visible in content such as news broadcasts or newspaper front pages (Godbole, 2019).

Source verification assesses who created content and their credibility. Investigators analyze account creation dates, posting patterns, follower networks, and content history to evaluate source reliability. Accounts created immediately before uploading dramatic content, accounts with small follower bases and minimal activity, and accounts posting exclusively content favorable to particular parties merit skepticism. Conversely, accounts with long

histories, substantial organic follower bases, and diverse content suggesting authentic individual operation increase credibility (Roberts, 2020).

Content verification examines whether materials have been manipulated or misrepresented. Images and videos may be authentic recordings of real events yet decontextualized, presented as depicting different times, locations, or circumstances than actually shown. Reverse image searches identify whether materials appeared previously online with different claims attached. Analysis of compression artifacts, error level analysis, and examination of metadata fields can detect editing. Comparison of multiple sources depicting the same events from different perspectives provides powerful verification (Farid, 2018).

Bellingcat, perhaps the most prominent open-source investigative organization, has pioneered OSINT methodologies applied to international crimes and human rights violations. Their investigation of the MH17 downing demonstrated OSINT's potential, identifying the specific Buk missile launcher used in the attack, its movement from Russia into Ukraine, perpetrators involved in transportation, and launch location, entirely through analysis of social media posts, photographs, videos, and satellite imagery (Bellingcat, 2016). This investigation, subsequently validated by official Dutch investigators, established precedents for OSINT reliability in high-stakes investigations.

Satellite imagery represents another crucial OSINT category, increasingly accessible through commercial providers offering high-resolution imagery to public and private purchasers. Planet Labs operates constellations of small satellites providing near-daily imagery of the entire Earth at three-meter resolution, with selected areas imaged at sub-meter resolution (Planet Labs, 2020). This temporal frequency enables before-and-after analysis documenting destruction, movement of military equipment, development of mass graves, and other developments relevant to international crimes.

Interpreting satellite imagery requires specialized expertise. Analysts must distinguish between object types based on size, shape, shadow patterns, spectral signatures, and contextual clues. Damage assessments classify destruction levels based on visible indicators such as roof damage, wall collapse, and burn patterns. Temporal analysis tracks changes across image series, identifying when developments occurred within windows defined by image acquisition dates (Aronson, 2018).

The integration of OSINT with traditional investigative techniques yields synergistic benefits. OSINT can identify witnesses, locations, and events requiring further investigation through conventional means. Conversely, witness testimony and physical evidence can corroborate or contradict OSINT findings. The Independent Investigative Mechanism for Syria employs integrated approaches, combining OSINT collection and analysis with interview-based investigation and examination of documentary evidence (IIIM, 2020).

Specialized databases and analytical tools have been developed to manage OSINT collections for international criminal investigations. The Berkeley Protocol on Digital Open Source Investigations provides comprehensive guidance on OSINT methodology, addressing collection, verification, preservation, and presentation of digital open-source information (Human Rights Center, 2020). The Protocol emphasizes documentation of investigative steps,

maintenance of chains of custody, and ethical considerations including protection of sources and respect for victims.

Artificial intelligence and machine learning technologies increasingly augment OSINT analysis. Algorithms can classify vast image collections, identifying content depicting weapons, military vehicles, destruction, or other relevant subject matter. Natural language processing enables analysis of textual content in multiple languages, identifying relevant materials within massive databases. Computer vision systems detect objects, faces, and scenes, though their use raises ethical concerns regarding privacy and potential misidentification (Greenberg, 2020).

Challenges in OSINT methodology include information overload, with relevant materials buried within vast quantities of irrelevant content. Platform policies and interface changes affect collection capabilities unpredictably. Legal restrictions on data collection vary across jurisdictions, creating compliance complexities. The digital divide means conflicts in regions with limited internet connectivity generate less open-source documentation, creating geographic biases in available evidence.

Adversarial manipulation represents an emerging threat to OSINT reliability. State and non-state actors increasingly understand that conflict documentation may serve accountability purposes, leading to deliberate disinformation campaigns. Fabricated videos, staged scenes, and coordinated posting of false information aim to pollute the evidentiary record. Sophisticated detection techniques and source verification protocols help address these threats but cannot eliminate risks entirely (Wardle & Derakhshan, 2017).

7. Case Studies of Digital Evidence and OSINT Application

Examination of specific cases where digital evidence and OSINT have been central to international criminal investigations illuminates practical applications, reveals how legal principles operate in context, and identifies patterns in evidentiary standards and judicial reasoning.

The prosecution of Eyad A. before the Koblenz Higher Regional Court in Germany represents a landmark case in which social media evidence proved decisive. Eyad A., a former member of Syrian government intelligence services, was charged with crimes against humanity for his involvement in torture and arbitrary detention (Koblenz Higher Regional Court, 2021). The case relied substantially on photographs and videos that Eyad A. himself had posted on social media depicting his presence at detention facilities and his associations with other intelligence personnel.

Prosecutors utilized these digital materials to establish Eyad A.'s membership in the intelligence unit implicated in systematic detention and torture, his presence during relevant time periods, and his knowledge of conditions within detention facilities. Authentication involved analysis of metadata confirming posting dates, geolocation verification matching visible architectural features with identified facilities, and corroboration through witness testimony from former detainees who recognized Eyad A. from his social media photographs (Kaleck & Kroker, 2021).

The court admitted the social media evidence after rigorous examination of authentication and reliability. Defense challenged the materials' authenticity and

interpretation, arguing photographs showing presence at locations did not prove criminal conduct. The court's reasoning emphasized that evidence need not be conclusive on its own but must be evaluated in context with other evidence. When combined with witness testimony and documentary evidence of systematic crimes occurring at the facilities where Eyad A. was present, the social media materials contributed to proof beyond reasonable doubt of his criminal participation.

This case established important precedents for social media evidence admissibility in domestic prosecutions of international crimes under universal jurisdiction. It demonstrated that materials defendants themselves posted publicly do not raise insurmountable authentication challenges, as their posting establishes a connection between the defendant and the content. It also illustrated how OSINT can compensate for lack of territorial access and limited traditional investigative capabilities in ongoing conflict zones.

The International Criminal Court's investigation of crimes in Darfur, Sudan, extensively utilized satellite imagery as OSINT evidence, though the resulting arrest warrants against Sudanese officials have not led to trials due to non-execution. The ICC Prosecutor's office collaborated with the American Association for the Advancement of Science to analyze satellite imagery documenting village destruction in Darfur (AAAS, 2012). Sequential imagery showed villages intact in earlier images and completely destroyed in later images, with burning visible in intermediate images indicating deliberate arson.

This satellite imagery supported charges of crimes against humanity and war crimes including murder, extermination, forcible transfer, torture, and rape. The imagery provided direct evidence of widespread destruction establishing the scale of attacks on civilian populations, an essential element of crimes against humanity. Expert analysis quantified destruction, identifying thousands of destroyed residential structures across multiple villages, demonstrating the systematic nature of attacks (Bromley & Andersen, 2012).

The Darfur investigation demonstrated satellite imagery's value for establishing contextual elements of international crimes when traditional investigation proves impossible. Sudan refused to cooperate with ICC investigations, preventing territorial access by Court investigators. Satellite imagery enabled remote monitoring and documentation of ongoing crimes, creating an evidentiary record despite these constraints. The investigation revealed both satellite evidence's potential and its limitations, as imagery alone could not establish individual criminal responsibility without evidence linking specific perpetrators to documented destruction.

The Dutch investigation of MH17 represents perhaps the most sophisticated integration of OSINT methodologies into a major international criminal investigation. Malaysia Airlines Flight 17 was shot down over eastern Ukraine in July 2014, killing 298 people. The Dutch-led Joint Investigation Team combined traditional investigative techniques with extensive OSINT analysis to identify perpetrators and weapons used (JIT, 2016).

Bellingcat's open-source investigation ran parallel to official efforts, using social media posts, photographs, videos, and satellite imagery to track a Buk missile launcher transported from Russia into Ukraine, positioned near the launch location, and returned to Russia immediately after the downing (Bellingcat, 2016). The investigation identified specific

individuals involved in transporting the weapon system through photographic analysis and comparison with verified photographs of Russian military personnel. Metadata analysis, geolocation verification, and chronolocation techniques established the timeline and movement route.

Official investigators subsequently validated Bellingcat's findings and conducted additional investigation including intercepted communications, missile fragment analysis, and radar data. The convergence of OSINT findings with classified intelligence and traditional evidence demonstrated OSINT's reliability when proper verification methodologies are employed. Prosecutors in the Netherlands brought charges against specific individuals based substantially on this evidence, with trial proceedings ongoing (Public Prosecution Service, 2019).

This case established important precedents for OSINT admissibility in hybrid international-domestic proceedings. The Dutch court admitted extensive OSINT evidence after prosecution established verification procedures and authentication through expert testimony. The court's acceptance of Bellingcat's methodologies, including geolocation verification and source analysis, validated OSINT investigative techniques previously considered experimental or uncertain.

The Syrian conflict has generated numerous cases involving digital evidence, with European prosecutors particularly active in exercising universal jurisdiction. The trial of Anwar R. before the Koblenz court, a senior official in Syrian intelligence services, relied on combinations of witness testimony, documentary evidence, and digital materials (Wiebke, 2021). Unlike the Eyad A. case involving the defendant's own social media posts, the Anwar R. prosecution incorporated videos and photographs uploaded by third parties documenting conditions in detention facilities under Anwar R.'s authority.

Prosecutors utilized videos showing overcrowded cells, evidence of torture, and deplorable conditions to corroborate witness testimony from survivors. Authentication involved analysis by experts who geolocated facilities visible in videos, compared architectural features with established detention center layouts, and analyzed metadata. Witnesses provided additional verification by recognizing specific rooms and corridors visible in videos as locations where they were detained.

The court admitted this third-party digital evidence, finding authentication sufficiently rigorous despite unknown identities of original video creators. The decision emphasized that circumstantial authentication evidence including geolocation verification, architectural feature matching, and witness corroboration collectively established authenticity on balance of probabilities. The court noted that requiring identification of original creators would effectively exclude valuable evidence from conflict zones where anonymity is necessary for source protection.

The International Criminal Court's Al-Werfalli case, though not reaching trial due to the suspect's death, involved novel use of social media evidence in arrest warrant proceedings. Al-Werfalli, a Libyan military commander, was charged with war crimes based primarily on videos circulated on social media showing him personally executing prisoners (ICC, 2017).

Seven distinct videos depicted summary executions, with Al-Werfalli clearly identifiable conducting killings.

The Pre-Trial Chamber issued an arrest warrant based substantially on these videos, finding reasonable grounds to believe Al-Werfalli committed war crimes. The decision represented the first ICC arrest warrant based predominantly on social media evidence, establishing that such materials, when properly authenticated and contextualized, can satisfy even the initial threshold for arrest warrants without extensive corroboration from traditional sources (Kersten, 2017).

The Chamber's reasoning emphasized the videos' self-authenticating qualities given their depiction of events that appeared genuine and could not reasonably be explained as staged or fabricated. The visible identification of Al-Werfalli, the clear depiction of summary executions, and the consistency across multiple videos created mutually reinforcing authentication. This case demonstrated that compelling digital evidence can establish probable cause independently, though the lack of trial proceedings prevented fuller exploration of admissibility standards at trial stage.

These cases collectively illustrate several patterns in digital evidence and OSINT application. Courts require rigorous authentication but employ flexible, multi-factorial approaches rather than demanding specific authentication methods. Corroboration through independent sources significantly enhances evidentiary weight. Expert testimony regarding technical authentication processes proves crucial for establishing reliability. Materials originating from multiple independent sources carry greater weight than single-source evidence. Judicial willingness to admit digital evidence correlates with the seriousness of charges and the difficulty of obtaining evidence through traditional means.

8. Challenges and Limitations of Digital Evidence in International Criminal Justice

Despite the transformative potential of digital evidence and OSINT in international criminal investigations, substantial challenges and inherent limitations affect their utilization and constrain their evidentiary impact. These challenges span technical, legal, ethical, and practical dimensions, requiring careful consideration by investigators, prosecutors, and judicial decision-makers.

Authentication remains the paramount technical challenge. Unlike physical evidence bearing unique characteristics difficult to replicate, digital files can be perfectly copied, easily edited, and entirely fabricated with minimal traces. Sophisticated image and video manipulation tools enable creation of convincing forgeries, while deep fake technologies using artificial intelligence can generate synthetic videos of individuals appearing to say or do things they never actually did (Chesney & Citron, 2019). As these technologies become increasingly accessible and sophisticated, distinguishing authentic from fabricated materials grows progressively more difficult.

Detection of manipulation requires specialized forensic expertise and sophisticated analytical tools. Yet forensic techniques race against advancing manipulation technologies in a perpetual arms race. Methods effective for detecting current editing techniques may prove

obsolete as new manipulation technologies emerge. Compression artifacts analysis, metadata examination, and error level analysis can identify many manipulations but cannot guarantee detection of all forgeries, particularly those created using state-of-the-art techniques (Farid, 2016).

The chain of custody challenges for digital evidence differ fundamentally from those affecting physical evidence. Physical evidence can be sealed in tamper-evident containers and stored securely with access logs documenting handling. Digital evidence requires copying for analysis and dissemination, creating multiple versions whose equivalence must be verified. Files may be processed through various software tools during investigation, each potentially altering metadata or file characteristics. Maintaining comprehensive documentation of all handling becomes essential yet burdensome (Casey, 2011).

Establishing original sources for digital materials presents particular difficulties. Videos appearing on social media platforms may be re-uploads of content originally posted elsewhere. Users download materials and re-post them, often with altered context or cropped to remove attribution information. Tracing materials to original sources requires extensive investigation that may prove impossible when original uploads were deleted or when materials circulated through multiple platforms (Golovchenko et al., 2020).

The volume of digital evidence creates practical challenges that overwhelm traditional investigative capacities. The Syrian conflict documentation numbers in millions of videos and images, representing thousands of hours of content. Human review of such collections is impossible within reasonable timeframes. While artificial intelligence tools can assist with classification and analysis, these technologies remain imperfect and may miss relevant materials or misclassify content (Skelton, 2020).

Verification of massive evidence collections strains organizational resources. Each item ideally requires geolocation verification, chronolocation assessment, source analysis, and content verification. Investigators must prioritize verification efforts, focusing on materials most directly relevant to specific cases while accepting that vast portions of collections cannot receive detailed verification. This selectivity creates risks that important evidence may be overlooked or that verified materials may not represent the full evidentiary picture.

Legal ambiguities regarding OSINT collection persist despite growing jurisprudential guidance. Different jurisdictions maintain varying legal standards for collecting publicly available digital information. Some activities that investigators consider ordinary OSINT collection might violate computer fraud laws, unauthorized access statutes, or platform terms of service in certain jurisdictions (Roberts, 2017). International criminal investigations operating across multiple legal systems must navigate these complexities, potentially limiting collection activities to avoid legal violations.

Privacy and data protection concerns create ethical tensions in digital evidence utilization. Videos and images uploaded to document human rights violations inevitably capture identifiable individuals, including victims, witnesses, and innocent bystanders. Circulation of this material for investigative and evidentiary purposes potentially violates privacy rights and creates safety risks for depicted individuals. Striking appropriate balances

between accountability imperatives and privacy protection proves challenging (Dubberley et al., 2020).

Content involving minors presents particularly acute ethical challenges. Children appear in conflict documentation as victims, witnesses, and occasionally perpetrators. International standards require special protections for children, yet effective criminal accountability may require using materials depicting child victims. The ICC has developed policies requiring careful assessment of necessity before using such materials, yet tension between child protection and accountability requirements persists (ICC, 2016).

The digital divide affects evidence availability and creates geographic biases. Conflicts in regions with robust internet connectivity and high smartphone penetration generate extensive digital documentation, while conflicts in areas with limited connectivity may produce minimal digital evidence. This disparity means accountability mechanisms relying on digital evidence may function more effectively for certain conflicts than others, creating potential inequities in international criminal justice (Silverman, 2014).

Platform policies and terms of service create practical obstacles. Social media companies regularly modify content policies, remove materials deemed violative of community standards, and ban accounts for policy violations. Content documenting violence, even when valuable for accountability purposes, often violates platform policies against graphic violence. Platforms remove such material, often without adequate notice, resulting in evidence loss. While preservation organizations attempt to archive content before removal, deletion often occurs before preservation (Syrian Archive, 2021).

Platform cooperation with investigations varies substantially. Some platforms provide limited legal assistance processes enabling investigators to request preservation or disclosure of materials, while others offer minimal cooperation. The lack of standardized procedures across platforms complicates investigations that require evidence from multiple sources. Platforms headquartered in jurisdictions unsympathetic to international criminal justice may resist cooperation entirely.

Metadata reliability presents ongoing challenges. Timestamps, geolocation coordinates, and other metadata fields can be falsified or may be automatically generated based on incorrect device settings. Users may alter device clocks, disable GPS functionality, or employ applications that strip metadata from files before upload. Investigators cannot simply accept metadata at face value but must verify information through independent means, substantially increasing verification complexity (Turner, 2019).

Language barriers complicate OSINT analysis when materials involve languages unfamiliar to investigators. Machine translation tools assist with basic comprehension but may miss nuances, translate idioms incorrectly, or fail to convey contextual meanings. Ensuring investigation teams possess necessary language capabilities requires resources that may be unavailable, particularly for less commonly spoken languages.

The contextualization challenge affects interpretation of digital evidence. Images and videos show specific moments from particular perspectives but cannot capture complete context. A video showing armed individuals in civilian areas might depict legitimate self-defense, unlawful attacks, human shielding, or numerous other scenarios depending on

broader context not visible in the footage. Investigators must gather extensive additional information to properly contextualize materials, yet such information may be unavailable (Godbole, 2019).

Source credibility assessment remains inherently uncertain for anonymously posted materials. Accounts may be operated by individuals with direct knowledge, by parties attempting to spread propaganda, or by anyone in between. Determining motivation and credibility of unknown sources challenges even experienced investigators. While analysis of posting patterns and account history provides some insight, absolute certainty about source credibility is often impossible.

The adversarial information environment complicates verification. Parties to conflicts increasingly recognize that digital documentation may serve accountability purposes, leading to deliberate disinformation campaigns. Fabricated materials, staged events, and coordinated dissemination of false claims aim to pollute the evidentiary record and discredit authentic documentation. Sophisticated disinformation operations require sophisticated counter-measures, creating additional verification burdens (Wardle & Derakhshan, 2017).

Legal uncertainty regarding admissibility standards persists despite developing jurisprudence. Different international tribunals and domestic courts may apply varying authentication standards, creating unpredictability regarding which materials will be admitted. Lack of binding precedent in international criminal law means decisions by one court may not bind others, resulting in potentially inconsistent approaches.

Defense challenges to digital evidence can be particularly effective given authentication complexities. Defense counsel can raise reasonable doubts by highlighting the ease of manipulation, questioning verification methodologies, identifying gaps in chains of custody, or proposing alternative explanations for materials. Prosecution must be prepared to address these challenges through comprehensive authentication evidence and expert testimony, substantially increasing litigation burdens.

9. Ethical Considerations and Human Rights Implications

The utilization of digital evidence and OSINT in international criminal investigations raises profound ethical questions regarding privacy, consent, source protection, victim dignity, and the balance between accountability imperatives and fundamental rights protection. These considerations require careful analysis to ensure that pursuit of justice does not itself create injustice.

Privacy rights intersect with digital evidence collection in complex ways. The International Covenant on Civil and Political Rights protects privacy, stating that no one shall be subjected to arbitrary or unlawful interference with privacy, family, home, or correspondence (ICCPR, Article 17). Yet international criminal investigations necessarily involve examining private information to establish criminal responsibility. The European Convention on Human Rights similarly protects privacy while recognizing that interference may be justified when necessary for prevention of crime and protection of rights of others (ECHR, Article 8).

Balancing these interests requires careful assessment of necessity and proportionality. Collection of digital evidence should be limited to materials genuinely relevant to

investigations, avoiding indiscriminate gathering of private information. When materials contain information about individuals not implicated in crimes, investigators should implement redaction and anonymization measures to protect privacy while preserving evidentiary value (Dubberley et al., 2020).

Social media content presents particular privacy complexities. Materials posted publicly might seem to carry reduced privacy expectations, yet individuals posting conflict documentation rarely envision their materials being utilized in criminal proceedings. Cultural contexts affect privacy expectations, with sharing among particular communities not necessarily intended as publication to global audiences. Moreover, public posting may result from ignorance of privacy settings rather than intentional disclosure.

The principle of informed consent proves difficult to apply in OSINT contexts. Individuals captured in videos or photographs typically have not consented to documentation, let alone to use in criminal investigations. Obtaining retrospective consent is often impossible when individuals are deceased, displaced, or unreachable. Proceeding without consent may be justified by accountability imperatives, yet this rationale requires careful ethical analysis to avoid instrumentalizing victims for institutional purposes (Aronson, 2011).

Secondary traumatization concerns arise when graphic materials depicting violence and suffering are repeatedly viewed during investigation, legal proceedings, and public trials. Victims and family members may experience re-traumatization through forced engagement with documentation of their suffering. The ICC has developed protocols for handling sensitive evidence, including in-camera proceedings for particularly graphic materials and restrictions on public disclosure, yet these measures incompletely address traumatization risks (ICC, 2016).

Source protection represents a critical ethical obligation when individuals face danger for providing information. OSINT sources who upload documentation from conflict zones may face severe reprisals if identified by parties to conflicts. Even apparently anonymous posts may be traceable through technical analysis or contextual investigation. Investigators must implement protective measures including anonymizing source information, securely storing materials preventing unauthorized access, and carefully considering risks before public disclosure of evidence revealing source identities (Koenig et al., 2014).

The Berkeley Protocol on Digital Open Source Investigations emphasizes source protection as a fundamental ethical requirement, recommending that investigators assess potential harm to sources before collection, implement technical and procedural safeguards preventing unauthorized disclosure, obtain informed consent where feasible, and maintain ongoing risk assessment as circumstances evolve (Human Rights Center, 2020).

Children's rights warrant special attention given their vulnerability and the distinctive harms digital evidence may inflict. The UN Convention on the Rights of the Child requires that children's best interests be primary considerations in actions concerning them. Using evidence depicting child victims in prosecutions may serve children's interests by providing accountability for crimes against them, yet it simultaneously risks harm through exposure of their identities and traumatic experiences (CRC, Article 3).

The ICC's Policy on Children requires assessment of necessity before using materials depicting children, implementation of special protective measures including image anonymization, closed sessions during testimony involving children, and provision of psychosocial support to child victims and witnesses. The Policy emphasizes that children should never be subject to further harm through justice processes (ICC, 2016).

Dignity concerns extend beyond children to all victims. Graphic documentation of atrocities, while potentially valuable evidence, may violate victim dignity through exposure of their suffering. International humanitarian law's fundamental principle of respect for human dignity applies throughout investigations and prosecutions, requiring that evidence handling preserves dignity even when depicting undignified treatment (ICRC, 2015).

Balancing competing ethical imperatives proves challenging when dignity protection conflicts with evidentiary necessity. Completely excluding graphic materials might undermine prosecutions by failing to demonstrate crime severity, yet unrestricted use violates victim dignity. Compromise approaches including redaction of identifying features, use of still images rather than videos where sufficient, and restricting graphic evidence to closed proceedings partially address these tensions.

Cultural sensitivity requires recognition that privacy norms, dignity concepts, and attitudes toward documentation vary across cultures. Investigators and institutions rooted in Western legal traditions may insufficiently appreciate cultural contexts of evidence subjects. Meaningful engagement with affected communities and incorporation of diverse perspectives within investigative teams can enhance cultural sensitivity (Ní Aoláin, 2012).

The risk of misuse of collected evidence extends beyond criminal proceedings. Digital evidence collected for accountability purposes might be exploited for intelligence gathering, targeting of opposition members, or propaganda purposes. Organizations collecting evidence must implement strict policies preventing inappropriate secondary use, yet maintaining absolute control over materials proves difficult once evidence enters legal proceedings or becomes publicly known (Dubberley et al., 2020).

Consent and participation of affected communities represents an emerging ethical consideration. Communities affected by crimes documented through digital evidence may have interests in how materials are collected, preserved, and utilized. Participatory approaches that engage communities in decision-making regarding evidence handling respect community agency and incorporate local knowledge, yet resource constraints and security considerations may limit participatory possibilities (Clarke, 2019).

The commodification concern emerges when digital evidence collection becomes professionalized and commercialized. Organizations collecting evidence may develop financial interests in continued collection and institutional growth that could potentially influence evidence-related decisions. While professionalization enhances technical capacity and sustainability, it also creates risks that institutional interests might outweigh victim-centered considerations.

Researcher safety constitutes an ethical responsibility often overlooked in OSINT discussions. Individuals conducting open-source investigations of international crimes may face threats from conflict parties, criminal organizations, or government agencies.

Organizations employing investigators must implement security protocols, provide training in digital security, and offer support for investigators experiencing threats. The assassination of journalists and human rights defenders documenting atrocities demonstrates that these risks are concrete rather than theoretical (RSF, 2020).

Platform ethics involves consideration of social media companies' roles and responsibilities. Platforms hosting evidence of international crimes face competing pressures to remove graphic content for community safety while preserving material for accountability purposes. Some platforms have developed evidence preservation programs cooperating with investigators, while others prioritize removal without consideration of evidentiary value. Developing ethical frameworks for platform responses to conflict documentation remains an ongoing challenge (Dubberley et al., 2020).

The question of who should collect and control digital evidence raises further ethical considerations. Options include official investigative bodies such as the ICC, national prosecutors, international commissions of inquiry, human rights organizations, specialized documentation centers, and affected communities themselves. Each approach carries distinct ethical implications regarding legitimacy, technical capacity, resource availability, and community connection. Coordination among multiple actors complicates evidence stewardship and raises concerns about duplicated efforts and inconsistent standards.

10. Future Developments and Recommendations

The trajectory of digital evidence and OSINT in international criminal justice points toward increasing centrality and sophistication, yet realizing this potential while addressing current limitations requires intentional development of legal frameworks, technical capacities, and institutional practices.

Artificial intelligence applications in evidence analysis will expand substantially, offering powerful tools for managing massive evidence collections while introducing new challenges requiring careful governance. Machine learning algorithms can classify millions of images and videos, identifying content depicting weapons, military equipment, destruction, or specific individuals with accuracy approaching or exceeding human capabilities. Natural language processing enables analysis of textual content in multiple languages, detecting patterns and relevant information within vast databases (Skelton, 2020).

These technologies offer efficiency gains essential for handling modern evidence volumes, yet they also create risks. Algorithms may embed biases present in training data, leading to systematic over-identification or under-identification of particular content categories. Black box decision-making processes in complex neural networks impede transparency and explainability necessary for legal proceedings. Over-reliance on automated systems may cause investigators to miss materials that algorithms incorrectly filter as irrelevant.

Recommendations for AI governance in international criminal evidence analysis include maintaining human oversight of algorithmically generated results, requiring transparency regarding algorithm training and decision-making processes, validating system accuracy through testing on diverse datasets, and establishing clear accountability for errors.

Courts should require prosecution to explain AI methodologies when algorithms were used to identify or analyze evidence, ensuring defense can challenge reliability (Greenberg, 2020).

Blockchain technologies offer promising approaches to evidence authentication and chain of custody documentation. Blockchain's distributed ledger architecture creates tamper-evident records of evidence handling, with cryptographic hashing ensuring that any alteration of recorded information would be immediately detectable. Several organizations have begun implementing blockchain-based evidence preservation systems, recording hash values of collected materials in distributed ledgers that provide permanent verification of evidence existence and integrity at specific times (Hala Systems, 2019).

Broader adoption of blockchain evidence authentication could address persistent chain of custody challenges, yet implementation requires careful design to balance security with accessibility. Purely decentralized systems may create coordination difficulties, while systems incorporating central authority elements risk recreating vulnerabilities that blockchain aims to address. Recommendations include development of standardized protocols for blockchain evidence preservation, creation of governance frameworks for operating blockchain evidence systems, and judicial education regarding blockchain authentication methodologies.

Standardization of digital evidence handling protocols across international criminal justice institutions would enhance consistency and quality. Currently, different tribunals, courts, and investigative mechanisms employ varying approaches to evidence collection, preservation, and authentication. The Berkeley Protocol on Digital Open Source Investigations provides comprehensive guidance, yet it lacks binding authority and requires supplementation with institution-specific implementation measures (Human Rights Center, 2020).

Recommendations include adoption of common evidence handling standards by international criminal justice institutions, development of accreditation programs for digital evidence collection organizations, creation of standardized metadata schemas ensuring interoperability across evidence management systems, and establishment of mutual recognition frameworks enabling evidence collected by one institution to be utilized by others without duplicative authentication.

Enhanced technical assistance to domestic jurisdictions exercising universal jurisdiction over international crimes would strengthen decentralized accountability efforts. Many states possess legal authority to prosecute international crimes but lack specialized expertise in digital evidence and OSINT. Capacity building initiatives providing training, technical tools, and expert support could enable more effective domestic prosecutions complementing international tribunal work (Kaleck & Kroker, 2021).

Recommendations include establishing international technical assistance mechanisms providing digital evidence expertise to national prosecutors, developing training programs for domestic investigators and judges regarding digital evidence authentication and admissibility, creating shared databases enabling prosecutors across jurisdictions to access preserved digital evidence collections, and facilitating expert witness networks connecting technical specialists with prosecutors requiring assistance.

Platform cooperation with accountability initiatives requires formalization through agreements establishing preservation procedures, evidence disclosure protocols, and content moderation policies that account for evidentiary value. Currently, platform responses to documentation of international crimes are inconsistent and unpredictable. Development of structured cooperation frameworks could enhance evidence preservation while respecting platform concerns regarding user privacy and community safety (Dubberley et al., 2020).

Recommendations include negotiating formal agreements between major platforms and international criminal justice institutions regarding evidence preservation, establishing clear procedures for platforms to receive and respond to evidence preservation requests, creating technical systems enabling secure transfer of evidence from platforms to investigators, and developing content moderation policies that distinguish between graphic violence requiring removal for community protection and documentation of international crimes warranting preservation.

Victim and witness protection in the digital evidence context demands enhanced measures addressing distinctive risks created by digital materials. Unlike traditional evidence, digital materials may reveal identities of sources and witnesses through metadata, visible features, contextual information, or technical analysis. Once evidence enters legal proceedings or becomes public, controlling access proves difficult.

Recommendations include developing advanced anonymization techniques for digital evidence including face blurring, voice distortion, and metadata stripping that preserve evidentiary value while protecting identities, implementing strict protocols for redaction of identifying information before evidence disclosure, creating secure evidence presentation systems enabling use of sensitive materials in proceedings without public release, and providing protective relocation and security measures for individuals whose identities might be compromised through digital evidence.

Ethical frameworks specific to digital evidence and OSINT should be developed and adopted by organizations engaged in evidence collection for international criminal accountability. General human rights principles provide foundational guidance but require adaptation to digital evidence contexts addressing issues such as consent, privacy, dignity, and re-traumatization.

Recommendations include developing codes of conduct for digital evidence collection incorporating privacy protection, informed consent where feasible, source security, victim dignity, and cultural sensitivity, establishing ethics review processes for evidence collection activities similar to research ethics review boards, creating remedial mechanisms enabling individuals to request removal of their identifying information from evidence databases when consistent with accountability objectives, and conducting impact assessments before evidence collection regarding potential harms to individuals and communities.

International legal instruments addressing digital evidence admissibility could provide authoritative guidance reducing current uncertainties. While flexible evidentiary rules enable adaptation to emerging evidence forms, they also create unpredictability regarding admissibility standards. Development of specific provisions addressing digital evidence

authentication, metadata verification, and technical expertise requirements would enhance legal certainty.

Recommendations include amendments to Rules of Procedure and Evidence of international criminal courts specifically addressing digital evidence authentication requirements, development of practice directions by Trial Chambers providing detailed guidance on digital evidence handling, creation of model legislation for domestic courts addressing international criminal proceedings with digital evidence provisions, and negotiation of international agreements establishing minimum standards for digital evidence admissibility in transnational investigations.

Investment in research and development of verification technologies would enhance authentication capabilities keeping pace with manipulation techniques. As deep fake technologies and sophisticated editing tools become increasingly accessible, detection methodologies must advance correspondingly. This requires sustained research funding, collaboration between technical experts and legal practitioners, and rapid translation of research findings into practical investigative tools.

Recommendations include establishing research partnerships between technical institutions and international criminal justice organizations focused on authentication technology development, creating innovation prizes incentivizing development of effective verification tools, requiring evidence technology companies to contribute to authentication research as condition of selling manipulation tools, and developing rapid response mechanisms for assessing authenticity of specific pieces of contested evidence.

Training and education initiatives should integrate digital evidence and OSINT methodologies into legal education, judicial training, and professional development for investigators and prosecutors. Current legal education typically provides minimal coverage of digital evidence issues, leaving practitioners inadequately prepared for contemporary practice realities.

Recommendations include incorporating digital evidence modules into law school curricula, developing continuing legal education programs for judges and lawyers focused on digital evidence authentication and admissibility, creating training programs for investigators in OSINT collection and verification methodologies, and establishing fellowship programs enabling traditional investigators to develop digital evidence expertise through placement with specialized organizations.

Interdisciplinary collaboration between legal practitioners, technical experts, human rights advocates, and affected communities should be formalized through institutional mechanisms ensuring diverse perspectives inform evidence handling practices. Currently, these communities often work in parallel with insufficient coordination and mutual understanding.

Recommendations include establishing interdisciplinary advisory bodies within international criminal institutions providing guidance on digital evidence issues, creating secondment programs enabling technologists to work within legal institutions and legal practitioners to work with technical organizations, developing joint training initiatives

bringing together different professional communities, and facilitating regular conferences and workshops focused on digital evidence in international criminal justice.

Resource allocation must prioritize digital evidence infrastructure development, recognizing that contemporary international criminal investigations require substantial investment in technical systems, specialized personnel, and training. Many institutions operate with budgets developed for traditional investigations and lack resources for necessary digital capabilities.

Recommendations include increased budgetary allocations for digital evidence infrastructure within international criminal institutions, creation of dedicated funding mechanisms supporting digital evidence preservation organizations, development of cost-sharing arrangements enabling multiple institutions to support common infrastructure, and advocacy with donor governments and organizations regarding funding priorities for digital accountability initiatives.

The integration of emerging technologies including virtual reality, augmented reality, and three-dimensional modeling offers opportunities for enhanced evidence presentation and analysis. These technologies can reconstruct crime scenes, enable virtual site visits when territorial access is impossible, and help judges and fact-finders understand spatial relationships and event sequences.

Recommendations include pilot programs testing virtual reality applications in international criminal proceedings, development of standards for three-dimensional modeling ensuring accuracy and preventing manipulation, research regarding cognitive impacts of immersive evidence presentation on fact-finding, and guidelines for appropriate use of emerging technologies balancing enhanced comprehension against potential prejudicial effects.

Conclusion

The integration of digital evidence and open-source intelligence into international criminal investigations and prosecutions represents a paradigm shift with profound implications for accountability, evidence law, and the pursuit of justice for mass atrocities. This research has examined the multifaceted dimensions of this transformation, analyzing technical methodologies, legal frameworks, practical applications, challenges, and ethical considerations that characterize the contemporary landscape of technology-mediated international criminal justice.

Digital evidence and OSINT have demonstrably enhanced investigative capabilities, enabling documentation and prosecution of international crimes in circumstances where traditional methodologies prove impossible. Conflicts occurring in territories inaccessible to investigators can now be monitored remotely through satellite imagery, social media documentation, and other digital sources. Patterns of violence invisible through individual incident examination emerge through analysis of aggregated digital data. Individual criminal responsibility can be established through digital communications, geolocation records, and command structure documentation previously unavailable.

The case studies examined illustrate successful application of these methodologies across diverse contexts, from European universal jurisdiction prosecutions relying on Syrian

conflict documentation to ICC investigations utilizing satellite imagery in Darfur. These precedents establish that rigorous authentication, multi-source corroboration, and expert analysis can render digital materials sufficiently reliable for admission in the most serious criminal proceedings. Judicial willingness to admit digital evidence when properly authenticated signals institutional adaptation to technological realities.

Yet substantial challenges persist, demanding ongoing attention from practitioners, scholars, and institutions. Authentication of digital materials in an era of sophisticated manipulation technologies requires constant methodological refinement and technical advancement. Chain of custody documentation must be adapted to digital evidence characteristics while maintaining evidentiary integrity. Massive evidence volumes strain organizational capacities, necessitating development of analytical tools and prioritization frameworks. Legal ambiguities regarding admissibility standards, privacy implications, and platform cooperation require clarification through jurisprudential development and legislative action.

Ethical considerations surrounding privacy, dignity, consent, and source protection demand principled frameworks balancing accountability imperatives against fundamental rights. The pursuit of justice cannot justify unlimited intrusion into privacy or disregard for victim dignity. Frameworks must be developed ensuring that evidence collection and utilization respect the rights and interests of those whose suffering is documented, while maintaining the effectiveness necessary for successful prosecution of mass atrocities.

The future trajectory of digital evidence in international criminal justice appears clear: technological capabilities will continue advancing, evidence volumes will grow exponentially, and investigations will rely increasingly on digital materials. Realizing the potential of these developments while addressing inherent risks requires intentional action across multiple dimensions including legal framework development, technical capacity building, standardization of practices, ethical governance, and resource allocation.

International criminal justice institutions must invest in digital infrastructure, recruit technical expertise, and adapt procedural frameworks to technological realities. Domestic jurisdictions exercising universal jurisdiction require technical assistance enabling effective use of digital evidence. Platform companies should formalize cooperation with accountability initiatives through structured agreements. The international community must recognize that accountability for contemporary conflicts demands support for digital evidence collection, preservation, and analysis.

The research presented here contributes to ongoing discussions regarding evidence standards, investigative methodologies, and institutional adaptation in international criminal law. By comprehensively examining technical, legal, practical, and ethical dimensions of digital evidence and OSINT, this work provides foundation for informed policy development, judicial decision-making, and scholarly analysis. The recommendations offered aim to enhance quality, consistency, and rights-compatibility of digital evidence utilization while strengthening accountability for international crimes.

As technology continues evolving at accelerating pace, the legal and institutional frameworks governing its application in international criminal justice must evolve

correspondingly. This requires sustained engagement from all stakeholders including legal practitioners, technical experts, human rights advocates, affected communities, and policymakers. The stakes could not be higher, as effective accountability for genocide, crimes against humanity, war crimes, and other mass atrocities increasingly depends upon our collective capacity to harness digital evidence and open-source intelligence while preserving fundamental principles of justice, fairness, and human rights protection.

References

1. AAAS (American Association for the Advancement of Science). (2012). *Satellite imagery analysis of villages in Darfur*. AAAS Geospatial Technologies Project.

2. Alexa Koenig, A., Tigas, M., & Rahhal, S. (2014). Framing human rights violations at a distance: An analysis of epistemological and evidentiary challenges using Syrian video content. *International Journal of Communication*, 8, 3552-3575.

3. Ambos, K. (2015). Evidence in international criminal procedure. In W. A. Schabas & N. Bernaz (Eds.), *Routledge handbook of international criminal law* (pp. 253-268). Routledge.

4. Aronson, J. D. (2011). The strengths and weaknesses of social media evidence in human rights advocacy. *Journal of Human Rights Practice*, 3(1), 23-36. https://doi.org/10.1093/jhuman/huq022

5. Aronson, J. D. (2018). Satellite surveillance of mass graves. In J. D. Aronson (Ed.), *Who's watching? Privacy, surveillance, and accountability in international criminal justice* (pp. 145-168). Cambridge University Press.

6. Ball, P. (2020). *Statistics and human rights: Methods for documenting atrocities*. Human Rights Data Analysis Group.

7. Bellingcat. (2016). *MH17: The open source investigation, two years later*. https://www.bellingcat.com/news/uk-and-europe/2016/07/16/mh17-the-open-source-investigation-two-years-later/

8. Bellingcat Investigation Team. (2021). *Digital verification in conflict zones: Syria case study*. Bellingcat.

9. Bromley, P., & Andersen, M. E. (2012). Satellite imagery analysis as evidence for international criminal prosecutions: Perspectives from international criminal law. *Yearbook of International Humanitarian Law*, 15, 47-74.

10. Brown, M. A. (2020). Geolocation techniques in digital investigations. *Digital Investigation*, 33, 200926. https://doi.org/10.1016/j.diin.2020.200926

11. Caligiuri, A., & Torres Soriano, M. R. (2018). OSINT in the context of hybrid threats. *European Journal of Security Research*, 3(1), 31-50.

12. Carrier, B. (2005). *File system forensic analysis*. Addison-Wesley.

13. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

14. Chaffee, E. C. (2018). The heavy burden of thin air: Evolving evidentiary challenges with digital and electronically stored information in international criminal trials. *Michigan State Law Review*, 2018(2), 289-344.

15. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753-1820.

16. Clarke, K. M. (2019). *Affective justice: The international criminal court and the pan-Africanist pushback*. Duke University Press.

17. Convention on the Rights of the Child, November 20, 1989, 1577 U.N.T.S. 3.

18. Cryer, R., Friman, H., Robinson, D., & Wilmshurst, E. (2019). *An introduction to international criminal law and procedure* (4th ed.). Cambridge University Press.

19. Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal*, 125, 326-398.

20. Dubberley, S., Griffin, E., & Bal, H. M. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press.

21. European Convention on Human Rights, November 4, 1950, E.T.S. No. 5, 213 U.N.T.S. 221.

22. Farid, H. (2016). Photo forensics. MIT Press.

23. Farid, H. (2018). Digital forensics. *Annual Review of Statistics and Its Application*, 5, 79-97.

24. Freeman, L. (2020). *Digital evidence and war crimes prosecutions: The impact of digital technologies on international criminal investigations and trials*. Fortess Press.

25. Godbole, S. (2019). Chronolocation: Applying temporal analysis to open source investigations. *International Journal of Digital Evidence*, 18(2), 44-59.

26. Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 U.S. presidential election. *Political Communication*, 37(3), 357-378.

27. Greenberg, D. P. (2020). Artificial intelligence in international criminal investigations. *Harvard Journal of Law & Technology*, 33(2), 557-612.

28. Hala Systems. (2019). *Blockchain technology for evidence preservation in conflict zones*. https://www.halasystems.com

29. Hamdani, A., & Maldonado, D. (2020). Digital evidence in international criminal law. *American University International Law Review*, 35(3), 567-624.

30. Human Rights Center, University of California, Berkeley. (2020). *Berkeley Protocol on digital open source investigations*. United Nations.

31. ICC (International Criminal Court). (2016). *Policy on children*. https://www.icc-cpi.int/Publications/Policy-on-Children.pdf

32. ICC (International Criminal Court). (2017). Warrant of arrest for Mahmoud Mustafa Busayf Al-Werfalli. ICC-01/11-01/17.

33. ICC Regulations of the Court. (2004). ICC-BD/01-05-16.

34. ICC Rules of Procedure and Evidence. (2002). ICC-ASP/1/3.

35. ICRC (International Committee of the Red Cross). (2015). *International humanitarian law and the challenges of contemporary armed conflicts*. ICRC.

36. ICTY (International Criminal Tribunal for the former Yugoslavia) Rules of Procedure and Evidence. (2015). IT/32/Rev. 50.

37. IIIM (International, Impartial and Independent Mechanism). (2020). *Fourth report of the International, Impartial and Independent Mechanism*. A/75/743.

38. International Covenant on Civil and Political Rights, December 16, 1966, 999 U.N.T.S. 171.

39. ISO/IEC 27037:2012. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*.

40. JIT (Joint Investigation Team). (2016). *MH17 criminal investigation: Preliminary results*. Public Prosecution Service of the Netherlands.

41. Kaleck, W., & Kroker, P. (2021). Syrian torture investigations in Germany and beyond: Breathing new life into universal jurisdiction in Europe? *Journal of International Criminal Justice*, 19(1), 165-191.

42. Kerr, O. S. (2018). Encryption workarounds. *Georgetown Law Journal*, 106, 989-1030.

43. Kersten, M. (2017). A war crimes tribunal in your pocket: The ICC comes to social media. *Justice in Conflict*. https://justiceinconflict.org/2017/08/17/a-war-crimes-tribunal-in-your-pocket-the-icc-comes-to-social-media/

44. Koblenz Higher Regional Court. (2021). Judgment in the Eyad A. trial. Case No. 1 StE 9/21.

45. Koettl, C. (2018). From crowd-sourcing to open-source: A new era of investigations. In S. Dubberley et al. (Eds.), *Digital witness: Using open source information for human rights investigation* (pp. 23-44). Oxford University Press.

46. Marx, A., & Goward, S. (2013). Remote sensing in human rights and international humanitarian law monitoring. *International Review of the Red Cross*, 95(890), 717-740.

47. May, R., & Wierda, M. (2002). *International criminal evidence*. Transnational Publishers.

48. Molina, O. (2020). The evidentiary value of digital information in international criminal trials. *Leiden Journal of International Law*, 33(4), 917-939.

49. NATO (North Atlantic Treaty Organization). (2001). *NATO Open Source Intelligence handbook*. NATO.

50. Ní Aoláin, F. (2012). Advancing feminist positioning in the field of transitional justice. *International Journal of Transitional Justice*, 6(2), 205-228.

51. Planet Labs. (2020). *Satellite imagery for human rights monitoring*. https://www.planet.com

52. Prosecutor v. Aleksovski, Case No. IT-95-14/1-A, Appeals Chamber Judgment (March 24, 2000).

53. Prosecutor v. Bemba, Case No. ICC-01/05-01/08, Appeals Chamber Judgment (June 8, 2018).

54. Prosecutor v. Bemba et al., Case No. ICC-01/05-01/13, Trial Chamber Judgment (March 19, 2016).

55. Prosecutor v. Katanga, Case No. ICC-01/04-01/07, Trial Chamber II Judgment (March 7, 2014).

56. Prosecutor v. Katanga, Case No. ICC-01/04-01/07, Decision on the prosecution request for admission of digital evidence (February 28, 2013).

57. Prosecutor v. Kordić and Čerkez, Case No. IT-95-14/2-A, Appeals Chamber Judgment (December 17, 2004).

58. Prosecutor v. Popović et al., Case No. IT-05-88-T, Trial Chamber Judgment (June 10, 2010).

59. Public Prosecution Service. (2019). *MH17 trial to begin on 9 March 2020*. Public Prosecution Service of the Netherlands.

60. Roberts, S. T. (2017). Content moderation. In L. Schintler & C. McNeely (Eds.), *Encyclopedia of big data*. Springer.

61. Roberts, S. T. (2020). Social media's silent filter: Content moderation and platform accountability. In S. Dubberley et al. (Eds.), *Digital witness* (pp. 213-229). Oxford University Press.

62. Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 3.

63. RSF (Reporters Without Borders). (2020). *Journalists killed in 2020*. https://rsf.org/en

64. Silverman, C. (2014). *Verification handbook: A definitive guide to verifying digital content for emergency coverage*. European Journalism Centre.

65. Silverman, C., Tsubaki, R., Crawford, K., Kalnes, Ø., & Stahn, C. (2020). Verification and digital investigations. In S. Dubberley et al. (Eds.), *Digital witness* (pp. 120-145). Oxford University Press.

66. Skelton, A. (2020). Artificial intelligence and international criminal justice. *Criminal Law Forum*, 31(2), 193-226.

67. Sommer, P. (2008). Directors' and corporate advisors' guide to digital investigations and evidence. *Information Security Technical Report*, 13(3), 145-156.

68. Syrian Archive. (2021). *Methodology*. https://syrianarchive.org/en/about/methodology

69. Turner, P. (2019). Metadata in digital evidence: Technical and legal dimensions. *International Journal of Law and Information Technology*, 27(2), 134-158.

70. Wald, P. M. (2002). Running the trial of the century: The nuremberg legacy. *Cardozo Law Review*, 27, 1559-1598.

71. Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe.

72. Wiebke, J. (2021). The Koblenz trial: The first criminal trial on torture in Syrian government detention centers. *Völkerrechtsblog*. https://voelkerrechtsblog.org/the-koblenz-trial/

73. Zawati, H. M. (2014). *Fair labelling and the dilemma of prosecuting gender-based crimes at the International Criminal Tribunals*. Oxford University Press.