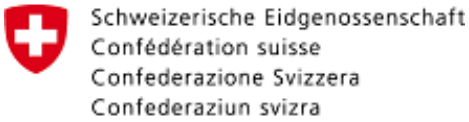


REPORT ON DIGITALLY DERIVED EVIDENCE IN INTERNATIONAL CRIMINAL LAW

as part of

THE DIGITALLY DERIVED EVIDENCE PROJECT

Leiden University

June 2019

Written by:

S. Ali
T. de La Bourdonnaye
E. Grant
C. Lam
A. Ognard
E. Panagakou
A. Piperides
E. Smitshuijzen
I. Greppi
A. Nicolae
A. Nowak
N. Cockerill
N. Primanda
M. Van Gils
S. Zarmsky

Supervised by:

Dr Emma Irving
Nicholas Ortiz, LL.M.
Anamika Misra, LL.M.

Edited by:

S. Ali
E. Grant
N. Primanda
S. Zarmsky

General Coordination by:

Dr Robert Heinsch

REPORT ON DIGITALLY DERIVED EVIDENCE IN INTERNATIONAL CRIMINAL LAW

Universiteit Leiden
The Netherlands

KGF

Report

Acknowledgements

The authors would like to thank the supervisors of the Kalshoven-Gieskes Forum, Dr. Emma Irving, Nicholas Ortiz, Anamika Misra and Dr. Robert Heinsch for their consistent support, encouragement, and guidance throughout the creation of this report. Without their help, this report would not have been possible.

The authors would also like to thank our partner Ilaria Allegrozzi from Human Rights Watch, who set up and strongly supported the case study in Bamenda (contained within another report).

In addition, the authors would like to thank Sam Dubberly and Julian Nichols for sharing their time and knowledge during training seminars.

The authors would like to thank family and friends for supporting us during the creation of this report.

The KGF extends warm thanks to our academic colleagues who are exploring every facet of digitally derived evidence, and without whose work this report would not be possible. This report particularly centres the following works:

- Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' 41 *Fordham International Law Journal* 283 (2018).
- International Bar Association, 'Evidence Matters in ICC Trials: An International Bar Association International Criminal Court & International Criminal Law Programme report providing a comparative perspective on selected evidence matters of current importance in ICC trial practice' (August 2016).
- Aida Ashouri, Caleb Bowers, and Cherrie Warden, 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' 11 *Digital Evidence and Electronic Signature Law Review* 115 (2014).

Finally, the KGF gratefully thanks the Swiss MFA for sponsoring this report.

Table of Contents

List of Abbreviations

CST - Call Sequence Tables

CDR - Call Data records

DDE - Digitally-Derived Evidence

FFM – Fact Finding Mission

IBA - International Bar Association

ICC - International Criminal Court

ICCTs – International Criminal Courts and Tribunals

ICL - International Criminal Law

ICTR - International Criminal Tribunal for Rwanda

ICTY - International Criminal Tribunal for the former Yugoslavia

IIA - Inherent Indicia of Authenticity

IMT – International Military Tribunal

RPE - Rules of Procedure and Evidence

STL - Special Tribunal for Lebanon

UNPROFOR – The United Nations Protection Force

Glossary

Aerial Imagery: Aerial photography is the production of photographic images from balloons, helicopters, or airplanes.[1]

Digital Evidence: This term refers to evidence which is created via digital technology. Such evidence originates from digital technology rather than another type of conventional evidence prior to becoming DDE (see digitalised evidence).

Digitalised/Digitised Evidence: This refers to evidence that would normally fall under another category of evidence, but as it has been copied or preserved virtually it has thus been converted from a physical form to a virtual digital form. When considering DDE which may be digitalised evidence it is important for practitioners to note that the best evidence rule may be applicable. That is, where the original evidence (which has not been digitalised) is not available the party wishing to submit the digitalised version of the evidence (the DDE) may bear the burden of presenting a reasoning as to why the court should accept the secondary evidence (the digitalised form of the evidence). Although it is unlikely for an international criminal court or tribunal to find digitalised DDE inadmissible, there may be adverse effect as to the probative value of the digitalised DDE where the argument for its acceptance is not well founded.

Metadata: This term is used to include information which is embedded in a particular piece of DDE that pertains to the data itself.[2] That is the data concerning the data itself. For example, the date, time, location, elevation, etc. that the primary data was created. Thus, the evidence which the DDE is purporting to can be considered primary data, whereas the data pertaining to primary data may be viewed as secondary data. Therefore, metadata can be understood as "the data of the data." Metadata is an extremely valuable resource to have in ICL and Fact-finding missions, as its presence can be used to aid in the authentication of DDE and therefore increase the probative value of the DDE.

Multi-Value Logical Form: This includes information not only in binary form, but also ternary and all other types of existing or future possible programming languages.[3] This terminology was used as it was determined to be the most inclusive and adaptable to future technological developments, the aim being that any novel programming languages, techniques, and/or styles would be covered by this term.

Photographs: A picture made using a camera, in which an image is focused on to light-sensitive material and then made visible and permanent by chemical treatment or stored digitally.[4]

Radio and Podcast: A podcast is an audio show, usually spread across a series of episodes, which can be downloaded from the Internet and listened to either on a computer, Mp3 player or a

---

[1] Sean Kotz, "What is the difference between Satellite Imagery and Aerial photography?" *Sciencing* (13 March 2018), < https://sciencing.com/up-date-satellite-pictures-look-at-13825.html > accessed 13 December 2020.

[2] 'metadata' (*Merriam-Webster Dictionary* 2019) available at: <https://www.merriam-webster.com/dictionary/metadata> accessed 15 December 2020.

[3] Vranesic Z G and Smith K C 'Engineering aspects of multi-valued logic systems' (1974) 7(9) *Computer* 34, 34-35.

[4] 'photograph' (*English Oxford Living Dictionaries*) <https://en.oxforddictionaries.com/definition/photograph> accessed 15 December 2020.

smartphone. The term, which was coined in 2004, is portmanteau of 'iPod' and 'broadcast'.[5] Digital radio receivers are able to receive and decode a digital program stream into a format that you can hear and see with program details on built in screens. Digital radio is transmitted using digital signals instead of analogue which AM and FM use.[6]

Satellite Imagery: The term "satellite imagery" may refer to a number of types of digitally transmitted images taken by artificial satellites orbiting the Earth.[7]

Social media posts: Websites and applications through which people can share content and data fast, in an efficient manner and even in live-motion.[8]

Unmanned Aerial Vehicle (UAV) footage: Video or photo footage taken from an UAV. The latter, commonly known as a "drone," is an aircraft with no pilot on board, remotely controlled from the ground and / or flying in part autonomously (pre-programmed or navigated by automation systems).[9]

Video: Visual multimedia source through which a series of images forms a moving picture. The video audio components that correspond with the pictures being shown on the screen.[10]

---

[5] Theodora Louloudis, 'What is a podcast and where can I find the best ones to listen to?' *The Telegraph* (13 July 2020) <https://www.telegraph.co.uk/radio/podcasts/what-is-a-podcast-and-where-can-i-find-the-best-ones-to-listen-t/> accessed 13 December 2020.

[6] 'What is digital radio? *ABC Radio* <https://www.abc.net.au/technology/techexplained/articles/2013/02/07/3685432.htm> accessed 10 December 2020.

[7] Sean Kotz, "What is the difference between Satellite Imagery and Aerial photography?"' *Sciencing* (13 March 2018), <https://sciencing.com/up-date-satellite-pictures-look-at-13825.html> accessed 13 December 2020.

[8] Matthew Hudson, 'What is Social Media?' *The Balance Small Business* (8 May 2019) <https://www.thebalancesmb.com/what-is-social-media-2890301> accessed 13 December 2020.

[9] G. Kurt Piehler and M. Houston Johnson, *Encyclopedia of Military Science* (SAGE Publications, Inc., 2013).

[10] Cambridge Dictionary, 'video' <https://dictionary.cambridge.org/dictionary/english/video> accessed 13 December 2020.

I. Introduction

Digitally derived evidence (DDE) has been increasingly used by international criminal courts and tribunals to prosecute perpetrators of international crimes. In conflict situations involving the commission of war crimes, crimes against humanity, and genocide, allegations must be adequately supported by evidence to prove the requisite elements of crimes and modes of liability.[11] Advanced digital tools—including aerial photography, mobile devices, video, radio intercepts, amongst others—capture new and vast quantities of data, which can add supplementary and supporting data to existing evidence. For example, while an eyewitness account may provide relevant information regarding an event, a satellite image may unearth information that would be otherwise inaccessible. Furthermore, phone and computer records may provide data relevant to an individual's activities, or a video may be geo-located and consequently allow investigators to see environmental details that a witness may have forgotten.[12]

Digital evidence is proliferating as quickly as technology is changing and expanding. To date, digital evidence has been used as part of cases in all international tribunals. In the International Criminal Court (ICC), investigations in Kenya, Libya, and Côte D'Ivoire have unfolded partly as a result of the widespread use of mobile phones and social media, which have acted as a new tool for uncovering information. Further, in July 2017 the ICC issued the first-ever arrest warrant based in large part on DDE, in this case videos of killings posted on social media platforms.[13] Given the proliferation of digital evidence and increasing reliance on digital evidence for prosecutions, it is possible that in the future, digital evidence may be the primary evidence upon which some convictions are based.

With this new possibility comes attendant risks. Are tribunals' current Rules of Procedure and Evidence sufficient to handle DDE? Do justice system actors, in particular tribunals, have the necessary technical expertise to realise DDE's potential? While DDE allows new opportunities to seek accountability, international criminal courts and tribunals must be attuned to the challenges posed by the use of DDE. In particular, courts must be aware of issues relating to collection, authenticity, reliability, and admissibility of DDE.[14]

Nevertheless, due to the lack of international legal guidelines, including a definition of DDE at the international level, the current legal framework on DDE is filled with legal issues that must be

[11] Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2018) 41 *Fordham International Law Journal* 283.

[12] International Bar Association, *Evidence Matters in ICC Trials: An International Bar Association International Criminal Court & International Criminal Law Programme report providing a comparative perspective on selected evidence matters of current importance in ICC trial practice* (August 2016), 20.

[13] *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli* (Warrant of Arrest) ICC-01/11-01/17 (15 August 2017).

[14] The ICC Prosecutor has acknowledged the potential of DDE by developing a 2016-2018 Strategic Plan outlining a strategy to recruit experts and acquire specialised equipment to effectively increase the use of technology in Court. ICC Office of the Prosecutor, 'Strategic Plan 2016-2018' (16 November 2015) [59]. In the latest draft of 2019-2021 Strategic Plan, the Prosecutor once again acknowledged the importance of DDE and online investigations, and pledged to continue the ICC's partnership with several organisations, such as the Scientific Advisory Board, the Technology Advisory Board, the University of California Berkeley Human Rights Centre, and the Carnegie Mellon University Centre for Human Rights Science to develop better understandings of the use of digital technology. ICC Office of the Prosecutor, '[draft] Strategic Plan 2019-2021' (14 May 2019) [47].

addressed to close any accountability gaps. As with any novel form of evidence, DDE requires additional expertise in order to effectively handle it in trial proceedings.

This Report aims to provide an overview of the legal standards relating to DDE in international accountability mechanisms. Specifically, the Report discusses the evidentiary rules and jurisprudence of the Nuremberg Tribunal, the ICTY, the ICTR, the STL, and the ICC, with a focus on admissibility, weight, authentication, provenance, and preservation. The Report also provides an overview of current practices in domestic jurisdictions in order to provide information which could potentially be applied to fill the gaps in frameworks for DDE at the international level.

Ultimately, this Report is not intended to develop a comprehensive protocol on how to use DDE for investigators and prosecutors, but to serve as a starting point for educating practitioners on the current state of affairs.

A. Methodology

In order to establish current practices and legal frameworks regarding the use of DDE in ICL, information was gathered from both domestic and international sources of law and supplemented with existing academic literature in the field.

In regard to the framework of ICL, the Report explores the law and practice concerning DDE in various international criminal tribunals throughout history—in particular, the Nuremberg International Military Tribunal, the International Criminal Tribunal for Rwanda ("ICTR"), the International Criminal Tribunal for the former Yugoslavia ("ICTY"), the Special Tribunal for Lebanon ("STL"), and the International Criminal Court ("ICC"). Examining the international legal framework provides the possibility to seek out areas of consensus to uncover pathways for dealing with DDE at the global level.

In regard to domestic jurisdictions, the Report attempts to be as geographically inclusive as possible, covering provisions and/or case law pertaining to DDE in Asia, Africa, Europe, North America, and South America.

The selection of countries for this section was influenced by the familiarity of domestic legal systems amongst the researchers, along with a desire to be representative of many different types of legal systems from different areas around the globe.

B. Limitations

A key limitation to our research is that there is a lack of established rules and practice pertaining to DDE in the field of international criminal law. This stems from the fact that DDE is a quickly evolving form of evidence. In addition, the use of DDE in a criminal law context raises many challenging questions, such as how to safely store DDE and ensure its integrity, or which existing procedural guidelines can be used to allow DDE to be introduced in criminal proceedings.

Another limitation to our research is the lack of access to court records from various domestic jurisdictions. In some cases, only the judgment was publicly accessible, meaning that there was no explanation given by the Court as to how DDE was introduced and evaluated.

Additionally, there is a limited amount of academic literature and research on this topic. As previously mentioned, this can be traced back to the relative newness of DDE and the slowly growing case law on the matter, paired with the low number of actual guidelines and procedures for DDE.

C. Definition of DDE

As digitally derived evidence is quickly developing and there is no universal definition, the following definitions of DDE are adopted by this report as they reflect the current understanding:

Body	Definition
International Bar Association	"Digital and technologically derived evidence, which means evidence taken from and created by digital devices and via technology, such as cameras, satellites and other 'remote sensing technologies' […] We distinguish digital evidence, created by digital technology and itself the record or trace of an action or event used for the purpose of proceedings, from the digitization of documents and records for the purpose of storing, organizing and presenting evidence, as for example, with the ICC's E-Court protocol."[15]
Human Rights Center UC Berkeley	"Digital evidence is data that is created, manipulated, stored, or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding."[16]

As further analysed by Lindsey Freeman, most digital evidence "is considered documentary or forensic evidence, depending on whether any analysis or scientific procedure has been applied in order to validate or verify the evidence".[17] Furthermore, she elaborates that:

> Digital photographs, aerial and satellite images, audio and video recordings, call records, emails, and other electronic records are considered documentary evidence and are therefore evaluated based on the same criteria as paper documents. If forensic processes have been applied to digital information (i.e., audio enhancement or photograph augmentation) or an analytic product or expert report has been compiled using raw digital data (i.e., a geolocated photograph or call sequence table) that evidence may have to be introduced through an expert witness, which would require additional conditions to be met.[18]

[15] International Bar Association (n 12) 19.

[16] Human Rights Center UC Berkeley, School of Law, 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (UC Berkeley, Berkeley February 2014), 1 fn2.

[17] Lindsay Freeman (n 11) 297.

[18] ibid.

D. Definition of Evidentiary Terms

In the following section, evidentiary considerations pertaining to DDE will be discussed, divided into the relevant categories of 'admissibility', 'weight', 'authentication', 'provenance', and 'preservation'. Though these terms will be explored in the following sections, general definitions for each category are outlined below.

'Admissibility' can be understood as the capability of a particular item to be accepted as evidence before the Court.[19] As seen further in this section, in assessing the admissibility of the evidence, the issues of authentication, provenance, and preservation are generally being taken into account by the judges.

Once the evidence has been admitted, the 'weight' of the evidence will be evaluated and determined by the judges. 'Weight of the evidence' refers to "the degree to which evidence convinces triers of fact to either accept or reject a factual assertion".[20] Sometimes, 'weight' is synonymous with the 'strength' of a piece of evidence.[21]

'Authentication' refers to a legal evidentiary process which aims to maintain "the integrity of the trial process by ensuring the evidence tendered establishes what it is offered to prove".[22] Meanwhile, 'provenance' is defined as "[t]he movement and location of real evidence, and the history of those persons who have it in their custody, from the time it is obtained to the time it is presented in court".[23] Another term used for provenance is 'chain of custody'.[24]

Last, 'preservation' refers to how evidence is stored after it is obtained. Preserving evidence to ensure its integrity proves important to the courts' consideration of its originality.[25]

---

[19] The Black's Law Dictionary defined 'admissibility' as 'the quality or state of being allowed to be entered into evidence in a hearing, trial or other proceeding', Bryan A Garner, *Black's Law Dictionary* (9th ed, West 2009), 53.

[20] 'Weight of the evidence" *Legal Information Institute* <https://www.law.cornell.edu/wex/weight_of_the_evidence> accessed 15 December 2020.

[21] ibid.

[22] Aida Ashouri, Caleb Bowers & Cherrie Warden, 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' (2014) *Digital Evidence and Electronic Signature* 115, 117.

[23] ibid 121.

[24] ibid 121.

[25] Loren D Mercer, 'Computer Forensics: Characteristics and Preservation of Digital Evidence' (2004) 73(3) *The FBI Law Enforcement Bulletin* 28, 31.

II. National Laws and Practice

Research on the use of DDE in the area of international criminal law was gathered from both domestic and international jurisdictions and supplemented with existing academic literature in the field. For newly developing and evolving issues in the law, of which DDE is an example, domestic jurisdictions tend to be faster in developing practice.[26]

On this note, though rules regarding the use of DDE in the courtroom are found in a variety of domestic legal frameworks, rules vary considerably amongst countries. This likely stems from a difference in legal tradition, mainly between civil and common law countries. For example, in terms of the scope of regulations, some countries have detailed provisions on specific issues relating to DDE, such as the United States for the authentication of e-mails.[27] According to the Federal Rules of Evidence, the authenticity of an e-mail may be established through a knowledgeable witness.[28] In this instance, the responsibility to authenticate evidence is placed upon the parties, who provide a witness.

Other countries, such as Germany, rely more upon the court's discretion to authenticate material evidence as opposed to the parties. Section 244(2) of the German Code of Criminal Procedure (StPO) holds the court responsible for the inquiries into the truth and authenticity of the evidence.[29] This difference between the regulations of the United States and the German Code highlights a distinction between the more investigative role of civil law courts and a more passive role of courts in common law, which is commonly seen between these two major jurisdictions. Consequently, in this example, the two systems approach the authentication of DDE in different ways.

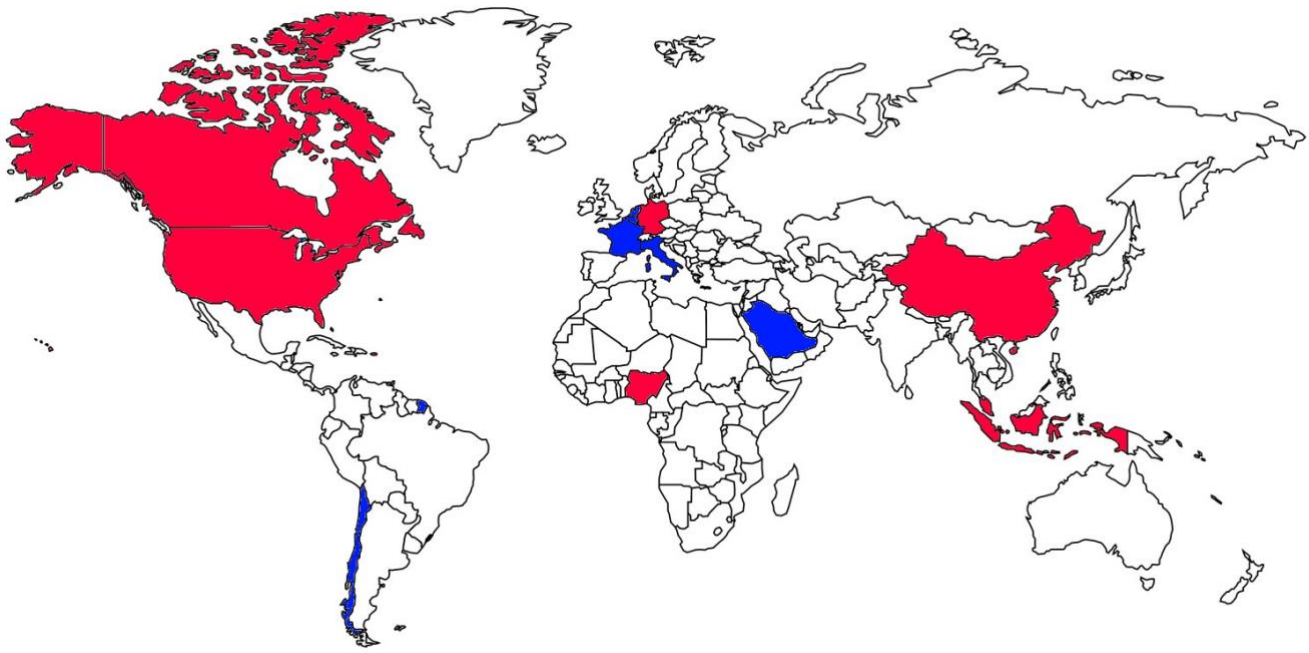
The following section will survey 'admissibility', 'weight', 'authentication', 'provenance', and 'preservation' of DDE in domestic jurisdictions.

[26] OSCE, 'Conference Report: Role of Domestic Jurisdictions in the Implementation of International Humanitarian Law (IHL) – Law and Practice' (OSCE, 19-20 May 2014) <https://www.osce.org/odihr/142256?download=true> accessed 15 December 2020, 6-7.

[27] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, 'Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence' (Rand Corporation 2015) <https://www.rand.org/pubs/research_reports/RR890.html> accessed 24 April 2019, 11.

[28] ibid.

[29] Code of Criminal Procedure of Germany, last amended 23 April 2014, Section 244 (2).



Map Showing Domestic Jurisdictions with Specific and General Provisions Applied to DDE.

Countries in red have specific provisions pertaining to DDE, while countries in blue have general provisions that are applied to DDE.

In this section, the following jurisdictions will be examined: Canada, Chile, China, France, Germany, Indonesia, Italy, Nigeria, Saudi Arabia, The Netherlands and The United States.

A. Admissibility

1. Chile

The Chilean procedure for regulating measures of evidence collection and prosecution of crimes is contained in the 2000 Criminal Procedure Code (CPC). Under the Criminal Procedure Code, the Prosecutor may require copies of electronic correspondences or any relevant digital information related to the object of investigation.[30] Further, under Article 222 of the Criminal Procedure Code, the supervising judge may order the interception and recording if there are reasoned suspicions that a person has committed or participated in the act or organization of a crime.[31]

[30] Criminal Procedure Code of Chile (2000) art 218.

[31] ibid art 222.

Despite the fact that under Article 9 of the CPC, pre-judicial authorisation is required for all proceedings, including evidentiary ones and DDE, the Prosecutor or the police may conduct some type of evidentiary activity that is not explicitly provided for in the CPC, provided that it does not affect the investigation and is not violating the fundamental rights of those under investigation.[32] Moreover, judicial authorities must comply with a proportionality test by establishing that the collection of the evidence is crucial to the process of the investigation and that the case has been adequately analysed in a proportionate manner.[33]

2. China

Article 50 of the Criminal Procedure Law provides for an exhaustive list of eight recognised types of evidence admissible in Court.[34] These include physical evidence, documentary evidence, witness testimonies, victim statements, defendant statements, expert opinions, investigation records, and audio-visual materials and electronic data.[35] Until recently, there were no established rules for how DDE (i.e., the audio-visual materials and electronic data) could be lawfully collected and admitted. However, in 2019, the Ministry of Public Security issued detailed rules of evidence to resolve this issue.[36] These rules include provisions on privacy protection, destruction or return of evidence if it is revealed to be of no use, and how DDE is collected.[37]

3. France

In regard to criminal law, the evidentiary principle of Freedom of the Evidence allows French penal judges to admit any evidence they believe is important, including DDE. For instance, in a 2016 case, a Parisian Court relied upon a tweet to sentence the author of anti-Semitic tweets to jail and a fine,[38] despite there being no specific rules of procedure on how to deal with social media posts as evidence. Yet, the Court provided no information as to the evaluation of the tweet in its opinion.

Concerning civil law, DDE may be admitted establishing the existence of a contract above 1500 euro as long as it is accompanied by an authentic deed ("acte authentique") made by a "huissier", or a public servant.[39]

---

[32] ibid art 9.

[33] Valentina Hernandez and Juan Carlos Lara, 'State Communications Surveillance and the Protection of Fundamental Rights in Chile' (2016) https://www.eff.org/files/2015/12/22/chile-en-dec2015.pdf accessed 15 December 2020, 14.

[34] Criminal Procedure Law of People's Republic of China (1979).

[35] ibid.

[36] Mini vandePol et al., 'China issues new rules to clarify procedures for collection of electronic data in criminal cases' (19 February 2019) Global Compliance News, Baker McKenzie <'https://globalcompliancenews.com/china-issues-new-rules-clarify-procedures-collection-electronic-data-criminal-cases-20190212/> accessed 15 December 2020.

[37] ibid.

[38] Tribunal Correctionnel Paris, 17e ch - ch de la presse, 9/4/2016, LICRA, SOS Racisme / M. X.

[39] Droits-finances, 'Huissier de justice: rôle et missions' (2019) <https://droit-finances.commentcamarche.com/contents/1367-huissier-de-justice-role-et-missions> accessed 15 December 2020.

4. Indonesia

As a result of the Electronic Information and Transactions Law enacted in 2008, DDE in Indonesia can be admitted as a separate category of valid legal evidence.[40] This law further contains several general provisions on the admissibility and the handling of DDE during the investigation and prosecution stages.

With regards to the admissibility criteria, Article 6 of Electronic Information and Transactions Law states that any DDE submitted before the court can be admissible as long as the information contained within it is accessible, can be displayed, its integrity can be warranted, and is accountable.[41]

In 2016, the Indonesian Constitutional Court rendered its judgment No. 20/PUU-XVI/2016, which held that electronic evidence obtained through wiretapping or interception can be admitted as lawful evidence, provided that the interception was lawful as part of law enforcement activities.[42] If the evidence was obtained illegally, then the judges must declare the evidence as inadmissible.[43]

5. Italy

The 2008 law ratifying the Budapest Convention on Cybercrime led to important modifications to the Italian law, upgrading the Code of Criminal Procedure.

The new rule introduced in the amended Code of Criminal Procedure pertains to the collection of digital evidence through the instalment of the so-called "Trojan horse" (known as the "captatore informatico" or "troiano").[44] The evidence is collected by installing the "Trojan horse" in the suspect's device by law enforcement agencies or third parties acting upon request.[45] This "Trojan horse" may bypass the antivirus vulnerability and become the dominus of the device by accessing the webcam, activating the microphone, encrypting the language of certain software, read any data stored in the mobile device, view photographs, record the traceability of the mobile device as a GPS, act as a keylogger, or can even secretly capture everything that is typed into the device.[46]

Recent verdicts issued in the *Musumeci* case by the Italian Supreme Court of Cassation have, however, characterised the acquisition of evidence through the Trojan as "invasive and unlawful".[47] The Court proclaimed the uselessness of the interceptions picked up by Trojan in consideration of the fact that

[40] Law No. 11/2008 on Electronic Information and Transactions, art 5 and art 44.

[41] ibid art 6.

[42] Judgment of Constitutional Court of the Republic of Indonesia, No 20/PUU-XIV/2016 (27 September 2016).

[43] ibid.

[44] Code of Criminal Procedure of Italy (2011) art 189, 226, 266bis.

[45] Pasquale Angelosanto, 'Le intercettazioni telematiche e le criticità del date retention nel contrasto alla criminalità organizzata' (2014) 4 *Sicurezza e Giustizia* 8, 8-13.

[46] ibid.

[47] ibid.

the decree of the judge for the preliminary investigations had derogated from Art 266, which required indicating the place in which the recording of conversations had taken place.[48]

6. Nigeria

The 2011 Nigerian Evidence Act provides detailed evidentiary rules on admissibility in both civil and criminal cases.[49] Section 84 provides the list of conditions which the DDE must fulfil in order to be admissible. Not only must it be relevant to current proceedings, as required by section 1(a), but it is also required:

> (a) [t]hat the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not by anybody, whether corporate or not, or by any individual;
> (b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
> (c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and
> (d) that the information contained in the statement reproduces is derived from information supplied to the computer in the ordinary course of those activities.[50]

These new rules were put into practice right away, as demonstrated by the 2012 *Kubor v. Dickson* case which explicitly recognised the admissibility of electronic evidence.[51] This was quickly followed by other similar cases, such as a case involving a downloaded YouTube video, or a case of ATM theft being decided due to (a lack of) DDE.[52]

7. The Netherlands

Video footage can be admissible as a legal means of evidence through the court's observations during the hearing or through a police report in which a reporter describes what can be seen on the footage (*a testimonium de auditu* – hearsay evidence – is admissible in Dutch criminal courts).[53]

---

[48] ibid.

[49] Evidence Act of Nigeria (2011).

[50] ibid section 84(2).

[51] *Kubor v. Dickson* (2012) LPELR - 9817 (Supreme Court of Nigeria).

[52] Timothy Tion, 'Timothy' (2014) *Digital Evidence and Electronic Signature Law Review* 1178-79.

[53] HR 20 December 1926, ECLI:NL:1926:BG9435, NJ 1927/85 (Supreme Court of the Netherlands).

Furthermore, in one case, a google search was introduced by the public prosecutor to prove that the acronym "ACAB" means "All Cops are Bastards", in order to prosecute someone for insulting a public servant.[54] The Defence pleaded that the meaning of the acronym was not certain.[55] Because facts or circumstances which are common knowledge do not require evidence in Dutch criminal procedure, the public prosecutor used a google search in order to show that the meaning of the acronym "ACAB" was, in fact, common knowledge. The Supreme Court held that the meaning of the abbreviation is common knowledge, but also held that the amount of search results in google did not lead to this conclusion.[56] Information derived from an internet source is generally accepted as facts of common knowledge, if that information does not assume specialist knowledge.[57] The information on Google Maps can also be qualified as a fact of common knowledge.[58]

B. Weight

1. France

For evidence to possess high probative value, it must be authenticated by a "huissier", a public servant, in the form of a "constat", or an authenticating deed.[59]

2. Indonesia

The 2008 Electronic Information and Transactions Law assigns more weight to DDE that is obtained from electronic systems which comply with the following requirements:

> (a) redisplays electronic information and/or electronic documents in their entirety in accordance with the retention period as provided for by rules;
> (b) protects the availability, entirety, authenticity, confidentiality, and accessibility of electronic information in the provision of electronic systems;
> (c) operates in compliance with procedures or guidelines on electronic systems;
> (d) is furnished with procedures or guidelines that are announced with languages, information, or symbols that are understandable to parties attributed to the provision of electronic systems;
> (e) adopts sustainable mechanisms in order to maintain updates, clarity, and accountability for the procedures or guidelines.[60]

3. Italy

---

[54] HR 11 January 2011, ECLI:NL:HR:2011:BP0291, NJ 2011/116 (Supreme Court of the Netherlands).

[55] ibid [3.4].

[56] ibid.

[57] HR 29 March 2016, ECLI:NL:HR:2016:522, NJ 2016/249 (Supreme Court of the Netherlands).

[58] HR 10 July 2018, ECLI:NL:HR:2018:1125, NJ 2018/1531 (Supreme Court of the Netherlands).

[59] Droits-finances (n 39

[60] Law No. 11/2008 on Electronic Information and Transactions, art 5(4), art 16(1).

According to Article 116 of the Code of Criminal Procedure ("Codice di Procedura Penale"), "the court must evaluate the evidence in accordance with its prudent judgment, except as otherwise provided by the law".[61] Accordingly, courts are expected to weigh the evidence freely but must lay down the reasons that led them to accept or reject the evidence provided.[62]

C. Authentication

1. Canada

In Canada, authenticity can be established by a witness who can attest that the DDE was created "in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it".[63]

Additionally, DDE can also be authenticated "by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system".[64]

2. Chile

In one case, a victim provided evidence with facial recognition tools through Facebook profiles in order to find a picture of his aggressor, but the judges decline to admit such DDE based on the consideration that the picture could have easily being photo-shopped, and that the Prosecution did not sufficiently examine the reliability of the facial recognition tool.[65]

3. China

Until 2018, electronic documents could only be authenticated in China by way of a notary, which was a costly procedure and therefore inaccessible to many.[66] Since then, the National People's Congress promulgated the E-commerce Law on 31 August 2018, which was followed by the Supreme Court of China ruling that allowed blockchain to be used for authentication purposes. A government

---

[61] Code of Criminal Procedure of Italy (2008), Article 116

[62] C. Punzi, 'La Prova Digitale nel Processo Penale' (2011) Rivista di Diritto Processuale 2(2)

[63] Evidence Act of Canada (1985) last amended 18 October 2017, s31.8.s.31.1(c).

[64] ibid section 31.3(a).

[65] Fabián Corbalán, 'En libertad queda joven acusado de agredir a carabinero: pruebas sólo eran fotos de Facebook' ['Young Men Accused of Attacking a Policeman is Released: Evidence was solely Based on Facebook Pictures'] (2014) Rabio Bío Bío <*https://eff.org/r.4u9z*> accessed 15 December 2020.

[66] Simon Hui, Zhenyu Ruan and Frank Zhuang, 'China's New Judicial Guidance clarifies scope and improves efficiency of internet disputes' (Lexology, 16 November 2018) <https://www.lexology.com/library/detail.aspx?g=76173563-dae4-4804-9cfe-cbd52413fe0a> accessed 15 December 2020.

blockchain platform was subsequently created to safely store evidence.[67] This system is currently limited to "Internet Courts" (specific courts dealing with e-commerce cases) but could be expanded to other Chinese jurisdictions.[68]

4. France

As stated previously, evidence can be authenticated by a "huissier".[69]

5. Germany

In a case before the Superior Court of Justice of Berlin, judgment delivered on 1 March 2017, images posted on Facebook and saved on the tablet of the defendant were used as evidence.[70] Though the judgment does not provide for further procedural insight as to how the court obtained access to the images uploaded on Facebook, it is evident that the DDE in the case was authenticated by the defendant's own testimony and admission of his guilt, as well as statements from other witnesses.[71]

6. Indonesia

In Indonesia, it is established practice that the judges usually refer to the expert and/or the accused's statements to support the authenticity of the DDE put before the Court.[72]

7. Nigeria

Authentication may be carried out by a "notary public", as provided by Section 150 of the 2011 Evidence Act.[73] Section 84(4) of the 2011 Evidence Act further adds that a particularly detailed certificate should be provided to the Court when computer-generated evidence is turned in.[74]

8. Saudi Arabia

---

[67] Mark Barley, 'Chinese court launches blockchain evidence platform' (2018) *Ledger Insights* <https://www.ledgerinsights.com/chinese-court-blockchain-evidence-platform/> accessed 24 April 2019.

[68] Zhao Wolfie, 'China's Supreme Court Recognizes Blockchain Evidence as Legally Binding' (7 September 2018) *Coindesk* <https://www.coindesk.com/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding> accessed 15 December 2020.

[69] Droits-finances (n 39

[70] Superior Court of Justice Berlin 2a Criminal Division, Judgment of 1 March 2017 - (2A) 172 OJs 26/16 (3/16), 2A 172 OJs 26/16 (3/16).

[71] ibid.

[72] Budy Mulyawan, 'Kekuatan Alat Bukti Informasi Elektronik dalam Penyidikan Tindak Pidana Keimigrasian' (2018) 12 *Jurnal Ilmiah Kebijakan Hukum* 107, 115.

[73] Evidence Act of Nigeria (2011), section 150.

[74] Ibid section 84(4).

In March 2007, the Electronic Transactions Law was enacted in Saudi Arabia.[75] Article 5(2) provides that "information resulting from electronic transactions shall remain in effect and enforceable as long as access to the details thereof is allowed within the electronic data system of the originator thereof and the manner of accessing them is indicated".[76] This provision highlights the emphasis placed upon knowing details of the source and how it was accessed before DDE can be admitted.

Furthermore, Article 9(4) provides that "when assessing the reliability of an electronic transaction the following shall be considered: (a) the method of creating, storing or communicating an electronic record and the possibility of tampering therewith, (b) the method of maintaining the integrity of information, and (c) the method of identifying the originator".[77]

9. The United States of America

The United States provides a means of authenticating DDE in the Federal Rules of Evidence. The Federal Rules of Evidence allow for authentication to be "established via testimony of a knowledgeable witness".[78] Furthermore, email may be authenticated in a variety of ways, including "establishing that the email contains information the defendant would have been familiar with" or "testimony that the defendant had primary access to the device on which the message was produced".[79]

In in 2017, a second amendment was added to the Committee Notes on Rules of Rule 902 of the Federal Rules of Evidence specifically in regard to authentication of DDE in more modern ways, other than through the testimony of a witness. In essence, this amendment makes use of hash values (a number created which represents the original DDE)[80] and certifications (which must contain information akin to that of a witness) to establish authenticity of the submitted DDE.[81]

Rule 902 of the Federal Rules of Evidence specifically in regard to authentication of DDE via witness testimony:

> *Paragraph (13)*: The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. [...] A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that

[75] Electronic Transactions Law of Saudi Arabia, Royal Decree No. M/18, 8 Rabi' I 1428H, 26 March 2007 <https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_003_%20E_E-Transactions%20Act.pdf> accessed 5 June 2019.

[76] ibid art 5(2).

[77] ibid art 9(4).

[78] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson (n 27) 11.

[79] ibid.

[80] "A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical". – Federal Rules of Evidence 902.

[81] ibid.

> information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.[82]

D. Provenance

1. Germany

In Germany, various forms of DDE have been used in practice in (higher) regional courts in order to prosecute war crimes.[83] In a judgment that was delivered on 8 November 2016 by the *Higher Regional Court of Frankfurt am Main*, the defendant was prosecuted for committing war crimes in Syria in November of 2013.[84]

The DDE gathered in the case consisted of digital images, videos, and a Skype conversation that were confiscated from the defendant's smartphone by authorities.[85] The smartphone was obtained by Turkish authorities during a baggage check in Turkey when the defendant left Syria.[86] The smartphone data was then extracted by Turkish authorities, the data stored, and later transferred as evidence to the German authorities.[87]

The judgment of the case does not provide for further protocol references and procedures that were followed in the transfer of the evidence from the Turkish to the German authorities. In addition, the spoken language in the video material was sometimes German, sometimes Arabic, and consequently the video files needed to be interpreted by a professional interpreter for Arabic within the Court.[88] Speech analysis of the videos played a significant role in establishing that the defendant filmed the videos and took part in the committed atrocities.[89]

2. Italy

---

[82] ibid.

[83] Eurojust, 'Prosecuting war crimes of outrage upon personal dignity based on evidence from open sources – Legal framework and recent developments in the Member States of the European Union' (2018) <http://www.eurojust.europa.eu/doclibrary/genocide-network/KnowledgeSharing/Prosecuting%20war%20crimes%20of%20outrage%20upon%20personal%20dignity%20based%20on%20evidence%20from%20open%20sources%20(February%202018)/2018-02_Prosecuting-war-crimes-based-on-evidence-from-open-sources_EN.pdf> accessed 15 December 2020.

[84] Higher Regional Court, Judgement of 8 November 2016 - 5-3 StE 4/16-4-3/16, 8 November 2016.

[85] ibid.

[86] ibid.

[87] ibid.

[88] ibid.

[89] ibid.

As regulated in Article 260(2) of the new Code of Criminal Procedure, the seizures by copying the digital proofs must take place on "adequate data carriers", using techniques that ensure that the copy is in its original form and has not being modified.[90]

E. Preservation

1. Italy

Article 244 (2) of the new Code of Criminal Procedure (*Codice di Procedura Penale*) stipulates that in identifying digital evidence, the legislator must ensure that inspections and searches are carried out using "technical measures capable of ensuring preservation and preventing alteration of the original data".[91]

2. Saudi Arabia

Article 6 of the Electronic Transactions Law provides the following criteria for storing electronic evidence:

> (a) Storing the electronic record in the form it was generated, sent or received or in such form that the contents thereof may be verified as being identical to the contents in which it was generated, sent or received.
> (b) Storing an electronic record in a manner allowing for future use and reference.
> (c) Storing information, together with electronic records, indicating the originator, addressee as well as the date and time of sending and receiving.[92]

F. Conclusion

Domestic legal systems tend to be quicker than international tribunals to respond to new types of evidence. Unlike most international courts and tribunals, domestic jurisdictions do not need to enter into a protracted procedure to amend Rules of Procedure and Evidence requiring approval by multitudinous parties (for example, the amendment process for the Rome Statute as laid out in Articles 121 and 122).[93]

Since domestic legal systems are faster moving and display a wider range of practices regarding DDE in criminal proceedings, it is important to examine how DDE is valued and applied in domestic jurisdictions and cases in order to extrapolate potential new practices to handle DDE in international criminal proceedings.

---

[90] Italian Code of Criminal Procedure (2011), art 260(2)

[91] ibid, art. 244 (2); see also art 247(1 bis), 254(2), 259(2) and 354(2).

[92] Royal Decree of Saudi Arabia "M18" (n 75), art 6.

[93] Rome Statute of the International Criminal Court, (entered into force 1 July 2002, last amended in 2010), 2187 UNTS 90 (hereafter referred to as "Rome Statute") art. 121 and 122.

III. Legal Framework and Practice in International Courts and Tribunals

The following sections provide an overview of legal standards relating to admissibility, weight, authentication, provenance, and preservation of DDE in international courts and tribunals.

A. Admissibility of DDE

There are no explicit evidentiary rules in international criminal law that govern the admissibility and weight of DDE specifically. Therefore, as with any other evidence, all DDE submitted before international courts and tribunals is evaluated according to the general rules of evidence for the specific court or tribunal. In addition, these general rules of evidence can be supplemented by how DDE is admitted or excluded in practice.

1. General Admissibility Rules

According to Rule 89(C) in the ICTY and ICTR Rules of Procedure and Evidence (RPE), the Chamber may admit any relevant evidence which it deems to have probative value.[94] Article 89(D) of the ICTY RPE further provides that a Chamber may exclude evidence if its probative value is substantially outweighed by the need to ensure a fair trial.[95] The Rules of Procedure and Evidence of its sister tribunal, the ICTR, contains no such provision, but the same principle has been applied in practice.[96]

Similar to the general ICTY and ICTR rules, Article 69(4) of the Rome Statute of the ICC provides that "the Court may rule on the relevance or admissibility of any evidence, taking into account, inter alia, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness […]".[97] In 2008, the same general admissibility criteria was adopted by the STL.[98]

From the provisions outlined previously, the general admissibility standard common amongst all the courts and tribunals emerges: (1) relevance and (2) probative value, weighed against (3) potential prejudicial effect.[99] This tripartite test has been applied by the judges for evaluation of the admissibility

[94] International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994), IT/32Rev.50 (hereinafter 'ICTY RPE') rule 89(C); International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995) (hereinafter 'ICTY RPE') rule 89(D).

[95] ICTY RPE rule 89(D).

[96] *Prosecutor v. Édouard Karemera et al.* (Decision on the Prosecutor's Motion for Admission of Certain Exhibits into Evidence) ICTR-98-44-T (25 January 2008) (hereinafter '*Karemara et al.* Admission Decision') [9]; *Prosecutor v. Théoneste Bagosora et al.* (Decision on Prosecutor's Interlocutory Appeal Regarding Exclusion of Evidence) ICTR-98-41-AR73.14 (19 December 2003) (hereinafter '*Bagosora et al.* Exclusion of Evidence Appeal Decision') [16-17].

[97] Rome Statute art 69(4).

[98] Special Tribunal for Lebanon, Rules of Procedure and Evidence (last amended on 10 April 2019, adopted on 20 March 2009) STL-BD-2009-01-Rev.10 (hereinafter 'STL RPE') rule 149(C) and (D).

[99] Christopher Gosnell, 'Admissibility of Evidence' in Karim A.A. Khan, Caroline Buisman and Christopher Gosnell (eds), *Principles of Evidence in International Criminal Justice* (Oxford University Press 2018), 375.

of evidence. For instance, in its Decision on the Admissibility of Four Documents in *Lubanga*, the ICC Chamber held that when considering the admissibility of a piece of evidence, the Chamber must: (1) ensure that the evidence is *prima facie* relevant to the trial: (2) assess whether the evidence has, on a *prima facie* basis, probative value; and (3) when relevant, weigh the probative value of the evidence against any potential prejudicial effect.[100] Likewise, similar rulings can be found in case law of both the ICTY[101] and the ICTR.[102]

When it comes to DDE, practice demonstrates that the issue of probative value is the most challenged and discussed criterion in regard to admissibility. As a general principle, according to the jurisprudence of the ICTY, the ICTR, and the ICC, one of the main factors in the assessment of probative value is the "reliability" of the evidence.[103] "Reliability" depends upon many circumstances, such as the origin, content, corroboration, truthfulness, voluntariness, and trustworthiness of the evidence.[104] Furthermore, the assessment of reliability is closely related to that of credibility,[105] as well as the issue of authentication.[106] The interplay between admissibility, authentication, and reliability is further discussed below.

a) International Criminal Tribunal for the Former Yugoslavia (ICTY)

The threshold for admissibility at the ICTY is low. Admission does not presume that the document provides an accurate portrayal of facts[107] but requires "sufficient indicia of reliability to make out a prima facie case for the admission of that document."[108]

---

[100] *Prosecutor v. Thomas Lubanga Dyilo* (Decision on the Admissibility of four documents) ICC-01/04-01/06 (13 June 2008) (hereinafter '*Lubanga* Four Documents Decision') [27-31].

[101] *Prosecutor v. Zejnil Delalić et al.* (Decision on the Motion of the Prosecution for the Admissibility of Evidence) IT-96-21-T (19 January 1998) (hereinafter '*Delalić* Admissibility Decision') [16].

[102] *Prosecutor v. Théoneste Bagosora et al.* (Decision on the Admissibility of Proposed Testimony of Witness DBY) ICTR-98-41-T (18 September 2003) [4], [6].

[103] *Lubanga* Four Documents Decision (n 100) [28-30]; *Delalić* Admissibility Decision (n 101) [18]; *Prosecutor v. Dusko Tadić* (Decision on Defence Motion on Hearsay) IT-94-1-T (5 August 1996) (hereinafter '*Tadić* Hearsay Decision') [9, 15]; *Prosecutor v. Pauline Nyiramasuhuko et al.* (Decision on Pauline Nyiramasuhuko's Appeal on the Admissibility of Evidence ICTR-98-42-AR73.2 (4 October 2004) (hereinafter *Nyiramasuhuko* Admissibility Appeal Decision) [7].

[104] Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* (Cambridge University Press 2016), 468; *Tadić* Hearsay Decision (n 103) [16]; *Prosecutor v. Alfred Musema* (Judgment and Sentence) ICTR-96-13-A (27 January 2000) (hereinafter '*Musema* Trial Judgment') [42]

[105] 'Only evidence that is reliable and credible may be considered to have probative value' see *Prosecutor v. Édouard Karemera et al.* (Decision on Joseph Nzirorera's Appeal of Decision on Admission of Evidence Rebutting Adjudicated Facts) ICTR-98-44-AR73.17 (29 May 2009) [14].

[106] According to Aida Ashouri, Caleb Bowers and Cherrie Warden, 'Authentication and reliability are related, but distinct concepts. The purpose of authentication is to ensure that the admitted evidence has not been manipulated or tampered with, while the purpose of reliability is to establish whether a piece of evidence is what it purports to be'. (n 22) 117.

[107] *Prosecutor v. Radoslav Brdanin and Momir Talic* (Order on the standard governing the admission of evidence) IT-99-36-T (15 February 2002) [18].

[108] ibid citing *Prosecutor v. Zlatko Aleksovski* (Decision on Prosecutor's Appeal on Admissibility of Evidence) IT-95-14/1-T (16 January 1999) [15].

In *Mladic*, several 360-degree photographs taken by investigators were introduced by the Prosecution as evidence in relation to a sniping incident in the Širokača area of Sarajevo.[109] After submitting this evidence, the Prosecutor called upon the investigator who took the photos to testify about the process and methodology of creating the 360-degree photographs. Furthermore, the witness served to help the Prosecutor in guiding the judges through the 360-degree photographs and reconstruct the events by relating it to previously introduced evidence.[110] The Chamber admitted the 360-degree photographs as evidence, which later played a significant role in convicting the accused.[111]

The ICTY has also addressed the admissibility of aerial images in its *Tolimir* trial judgment. During this trial, the US Government provided the aerial images to the Prosecutor,[112] but did not allow the Prosecutor to share any information relating to the "technical or analytical sources, methods, or capabilities of the systems, organizations, or personnel used to collect, analyze, or produce these imagery-derived products".[113] The Defence challenged the admissibility of the aerial images on the grounds that "no evidence was presented on their origin, the method of their creation, the manner of their editing, how to interpret them or whether they were delivered to the Prosecution in their original form or previously modified".[114] The Trial Chamber nevertheless admitted the DDE with corroborating "complementary forensic and anthropological reports", and testimony from two OTP prosecutors and witnesses linking the aerial images with the burial sites.[115]

b) Special Tribunal for Lebanon (STL)

DDE has been used extensively by the STL in the *Ayyash* case. In this case, the Prosecution relied mainly on telecommunications data in the form of Call Sequence Tables as evidence.[116] The Call Sequence Tables were introduced by the Prosecutor's analysts and explained by telecommunications experts. These Prosecution experts explained 'how cellular signals and cell tower sites are used to geolocate the cell phone user.'[117]

Considering another type of DDE, the STL Chamber in *Ayyash* declined to admit information from the WikiLeaks website as evidence, noting that the "Trial Chamber is not satisfied that the documents have the necessary prima facie indicia of reliability—namely, authenticity and accuracy—for admission

[109] *Prosecutor v. Ratko Mladić* (Transcript) IT-09-92-T (26 September 2013).

[110] ibid.

[111] *Prosecutor v. Ratko Mladić* (Judgment, Volume II of V), IT-09-92-T (22 November 2017) 984-991.

[112] Aerial images were submitted to establish the presence of particular locations of gravesites and reburial activities, buildings and vehicles, large groups of prisoners, and bodies.

[113] *Prosecutor v. Zdravko Tolimir* (Judgment) IT-05-88/2-T (12 December 2012) (hereinafter '*Tolimir* Trial Judgment') [67-68].

[114] *Prosecutor v. Zdravko Tolimir* (Defence Final Trial Brief) IT-05-88/2-T (1 October 2012) [158].

[115] International Bar Association (n 12) 25 fn.70.

[116] Lindsay Freeman (n 11) 308.

[117] ibid 313.

into evidence".[118] This decision shows that the source of the information is one of the key elements that the Chamber considers when determining admissibility.

c) International Criminal Court (ICC)

The ICC has also developed standards for the admissibility and evaluation of DDE in practice. In its first case, *Lubanga*, the ICC Chamber relied on videos as corroborating evidence for determining the ages of the alleged child soldiers.[119] On appeal, Defence counsel for Lubanga challenged the Trial Chamber decision to assess the age of individuals on the basis of video, as the video lacked any corroborating evidence.[120] However, the Appeal Chamber rejected that argument and instead held that "there is no strict legal requirement that the video excerpts had to be corroborated by other evidence in order for the Trial Chamber to be able to rely on them. Depending on the circumstances, a single piece of evidence, such as a video image of a person, may suffice to establish a specific fact".[121]

Later, in the case of *Katanga and Ngudjolo*, the Court determined that before video or audio material can be admitted as evidence, the Chamber must be presented with evidence of its originality and integrity.[122] Since "the relevance of audio or video material depends on the date and/or location of recording, evidence must be provided in this regard".[123]

In the *Al Mahdi* case, the Prosecution's evidence against the defendant included satellite images, archive photographs, audio and video recordings, as well as 360-degree panoramic photographs related to the destruction of several mausoleums and mosques in Timbuktu.[124] Furthermore, the Prosecution introduced a complex digital platform to present this DDE in collaboration with SITU Research. This platform displayed videos collected from the internet alongside satellite images and photographs taken of sites in Mali before and after the destruction. However, since the defendant pled guilty, the platform was never challenged as evidence before the Court,[125] and the platform's creators were not asked to testify about their methodology.[126] The Prosecution "did take extra steps to ascertain the date, time, and location, but did not show concern that the images and videos may be doctored or

---

[118] *Prosecutor v. Salim Jamil Ayyash et al.* (Decision on the Admissibility of Documents Published on the Wikileaks Website) STL-11-01/T/TC (21 May 2015) [42].

[119] *Prosecutor v. Thomas Lubanga Dyilo* (Judgment pursuant to Article 74 of the Statute) ICC-01/04-01/06 (14 March 2012) (hereinafter '*Lubanga* Trial Judgment').

[120] *Prosecutor v. Thomas Lubanga Dyilo* (Judgment on the Appeal of Mr Thomas Lubanga Dyilo against his conviction) ICC-01/04-01/06 (1 December 2014) [216-218].

[121] ibid [218].

[122] *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecutor's Bar Table Motions) ICC-01/04-01/07 (17 December 2010) (hereinafter '*Katanga and Ngudjolo* Bar Table Decision') [24].

[123] Göran Sluiter et al., *International Criminal Procedure Principles and Rules* (Oxford University Press 2013) 1066.

[124] *Prosecutor v. Ahmad Al Faqi Al Mahdi*, (Opening Transcript) ICC-01/12-01/15-T-4-Red-ENG (22 August 2016) (hereinafter '*Al Mahdi* Opening Transcript').

[125] Lindsay Freeman (n 11) 319.

[126] ibid.

staged".[127] Nevertheless, the evidence was agreed upon by the Defence as part of the admission of guilt.

As articulated by Lindsay Freeman, when the Court was faced with new types of DDE in *Bemba et al.*, it unusually chose to rule on admissibility upon admission as opposed to final judgment; in this case the new types of evidence were "call data records, telephone intercepts by Dutch authorities, and financial records emanating from Western Union".[128] The Prosecution presented a series of Call Sequence Tables,[129] call data records, as well as call logs and audio recordings from communications made by Bemba at the ICC Detention Centre (hereinafter 'Detention Centre materials').[130]

In evaluating the admissibility of this telecommunication evidence, the Trial Chamber conducted its own assessment by: (1) matching the identification number of the audio recordings/transcripts in their original languages to a given working-language transcript; (2) matching the communication to its corresponding log using the call duration and the e-court metadata; and (3) matching the telephone numbers with the speakers by taking into account voice samples, call content, and other relevant information.[131]

The Defence challenged the admissibility of the evidence based on the lack of Prosecution evidence establishing its authenticity and chain of custody.[132] The Chamber disagreed, stating that there was an "array of mutually reinforcing information confirming the accuracy of the intercepted communications and their corresponding logs".[133] The Chamber "further noted that some communications and logs had inherent indicia of authenticity, such as corporate watermarks of the telecommunications provider".[134]

The Defence also challenged the reliability of all the Detention Centre materials due to the fact that the spoken content between the two interlocutors was out of sync, meaning that the speech from one side of the call was temporarily misaligned with that of the other.[135] Regarding this issue, the Trial Chamber held that such technical irregularities with the recorded conversations, though notable, were not significant enough to exclude the evidence from the proceedings.[136] This determination by the

---

[127] Lindsay Freeman (n 11) 327. SITU Research, 'ICC Digital Platform: Timbuktu, Mali' <https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali> accessed 15 December 2020.

[128] ibid. *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Judgment Pursuant to Article 74 Rome Statute) ICC-01/05-01/13 (19 October 2016) (hereinafter '*Bemba et al.* Trial Judgment') [208].

[129] Indicating the data, phone numbers involved and the source of information.

[130] *Bemba et al.* Trial Judgment (n 128) [213-214].

[131] ibid, [216].

[132] ibid, [217].

[133] ibid, [218-223].

[134] Lindsay Freeman (n 11) 327.

[135] *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Public Redacted Version of "Corrigendum of ICC-01/05-01/13-1902-Conf-Corr") ICC-01-05-01/13 (29 July 2016) [204-209].

[136] ibid [226-227].

Trial Chamber concerning the reliability and authenticity of the Detention Centre materials were upheld by the Appeal Chamber.[137]

Also of note, screenshots from Facebook used by the Prosecutor to link two individuals were challenged by the Defence "on the basis that the ownership of the Facebook account could not be forensically verified and that there was no metadata attached to the screenshots".[138] Despite the objections of the Defence, in its final judgment, the Trial Chamber did not address the issue of the admissibility of screenshots from Facebook.

Most recently, on 15 August 2017, the ICC issued a public arrest warrant for Mahmoud Mustafa Busayf Al-Werfalli, based in large part on videos of executions in Libya found on social media platforms.[139] As of November 2020, the Chamber has not yet issued any decision on the admissibility of this evidence at trial, raising important issues regarding the standard of proof for DDE pre-trial.

2. Rules on Exclusion of Evidence

In addition to the general rules on admissibility, international tribunals have also stipulated conditions for the exclusion of evidence.

The ICC's exclusionary rule is outlined in Article 69(7) of the Rome Statute, which provides that:

> evidence obtained by means of a violation of the Rome Statute or internationally recognized human rights shall not be admissible if: (a) the violation casts substantial doubt on the reliability of the evidence; or (b) the admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings.[140]

Similar exclusionary provisions are also found in Rule 95 of the ICTR[141] and ICTY[142] RPE, as well as in Rule 162(A) of the STL RPE.[143]

---

[137] *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Appeal Judgment) ICC-01/05-01/13 (8 March 2018) (hereinafter '*Bemba et al.* Appeal Judgment') [621].

[138] International Bar Association (n 12) 27; ibid. [83-84]; metadata of a photo or video will be stripped if it is uploaded to social media platforms such as Facebook, Jeff James, 'How Facebook Handles Image EXIF Data' ITPro Today (7 December 2011) <https://www.itprotoday.com/strategy/how-facebook-handles-image-exif-data> accessed 15 December 2020.

[139] *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli* (Warrant of Arrest) ICC-01/11-01/17 (15 August 2017).

[140] Rome Statute art 69(7).

[141] ICTR RPE rule 95.

[142] ICTY RPE rule 95.

[143] STL RPE rule 162(A).

As clarified by the Chamber in *Lubanga*, a violation of Article 69(7) of the Rome Statute does not lead to automatic exclusion of evidence.[144] Instead, the judges have the discretion "to seek an appropriate balance between the Rome Statute's fundamental values in each concrete case".[145]

In *Lubanga*, the ICC enumerated two considerations for evaluating a violation of the right to privacy under Article 69(7) of the Rome Statute: the *lawfulness* and *proportionality* of the collection of evidence.[146] In this case Defence challenged the admissibility of certain evidence seized by Congolese police authorities, arguing that it should be excluded because the Defendant's right to privacy was violated and the evidence was seized in violation of Congolese procedural law.[147] Ultimately, the Chamber ruled that while the search and seizure of the evidence was carried out in conjunction with lawful criminal proceedings,[148] it violated the principle of proportionality due to the magnitude of items which were confiscated, including hundreds of items of "correspondence, photographs, invitations, legislation, reports, diaries", and "personal information" which was not relevant to the case.[149]

Nevertheless, the Chamber considered that the violation of the principle of proportionality did not affect the reliability of the evidence, and thus deemed the seized items to be admissible as evidence.[150] In evaluating the appropriate balance between the Rome Statute's fundamental values and the violation of the right to privacy, the Chamber referenced the ICTY *Delalic* case, which ruled that evidence can still be admitted if the violation is considered only a minor breach of procedural rules.[151]

On another note, in *Bemba et al.*, the Defence did not object to the reliability and accuracy of Western Union Records, but did challenge the admissibility of the records on the basis of the exclusionary rules outlined in Article 69(7) of the Rome Statute.[152] The Defence argued that the records had been obtained in violation of the applicable national procedures because the financial data of the accused and other individuals was obtained without prior authorization or court order from the competent Austrian authorities.[153] Ultimately, the Defence claimed that the collection of the records was in violation of the accused's right of privacy and submitted that the admission of the Western Union Records into evidence "would be antithetical to and would seriously damage the integrity of the proceedings" in violation of Article 69(7) of the Statute.[154]

---

144 *Prosecutor v. Thomas Lubanga Dyilo* (Decision on Confirmation of Charges) ICC-01/04-01/06 (29 January 2007) (hereinafter '*Lubanga* Confirmation Decision') [84].

145 ibid.

146 ibid.

147 ibid.

148 ibid [73-76].

149 ibid [79-82].

150 ibid [85-90].

151 ibid [88].

152 *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7) ICC-01/05-01/13 (29 April 2016).

153 ibid [11].

154 ibid [14].

In the interlocutory ruling rendered on 29 April 2019, the Trial Chamber held that based on, "the facts and submissions presented it is not proven that the Prosecution's contacts with Western Union and the reception of financial data prior to the first order of the Austrian Authorities vitiate judicially approved orders and, in consequence, led to a manifest violation of Article 38 of the Austrian Banking Act".[155] Accordingly, the Chamber found that the "manner in which the Western Union Documents were provided is not so manifestly unlawful that it fails to be "in accordance with the law for purposes of the right to privacy as reviewed under Article 69(7) of the Statute".[156]

In the Appeal Judgment, the Appeal Chamber concluded that the Trial Chamber erred in referring to national law in determining the violation of Article 69(7) Rome Statute and in failing to make a determination on the collection of the Western Union Records against the principle of proportionality.[157] Even so, the Appeals Chamber stated that "none of these errors, whether on their own or in combination, affects the validity of the Trial Chamber's conclusion in the First Western Union Decision that no violation of the Statute or of internationally recognised human rights within the meaning of article 69 (7) of the Statute had occurred in the collection of the Western Union Records".[158]

In addition to the Western Union Records, in *Bemba et al.*, Defence also objected to the admission of the Detention Centre materials on the basis of Article 69(7) of the Rome Statute.[159] The Defence submitted that the decision of the Pre-Trial Chamber to authorise the Prosecution's access to the Detention Centre materials violated the Defendant's statutory and human rights because it was: (1) unlawful, as the Detention Centre materials were part of Mr. Bemba's detention record protected by under Regulation 92 of the Court; (2) unsupported by evidence of a grounded suspicion of criminal activity; (3) unnecessary to fulfil the objective of the Prosecution's request; and (4) disproportionate.[160]

In response to this objection, the Trial Chamber held that the intercepted communications record was not within the scope of Regulation 92 of the Regulation of the Court.[161] In addition, the Trial Chamber found that the access to the Detention Centre materials was necessary because it "may be of essence for the Prosecution to be able to shed further light on the relevant facts for purposes of its investigation".[162] Finally, admission of the Detention Centre materials were found to be proportionate because the Prosecution would only receive recordings identified as relevant to its investigations.[163]

---

[155] ibid [48-60].

[156] ibid [60].

[157] *Bemba et al.* Appeal Judgment (n 137).

[158] ibid.

[159] *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Public redacted version of "Prosecution's Second Request for the Admission of Evidence from the Bar Table") ICC-Ol/05-01/13-1113 (31 July 2015).

[160] ibid.

[161] *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Decision on Bemba and Arido Defence Requests to Declare Certain Materials Inadmissible) ICC-01/05-01/13 (30 October 2015), [14].

[162] ibid [16].

[163] ibid [17].

This decision was upheld by the Appeals Chamber, and furthermore, the Appeals Chamber emphasised that Regulation 174(1) of the Regulations of the Registry specifically provides that all telephone conversations of detained persons shall be passively monitored, and that passive monitoring entails the recording of telephone calls.[164] Additionally, the Appeal Chamber also stated that the Pre-Trial Chamber only authorised the recordings to the Prosecution for the purposes of the investigation into possible offences under Article 70 of the Rome Statute,[165] which was both necessary to fulfil the objective of the Prosecution's request and proportionate.

On a similar note, in the *Ayyash* case at the STL, the Trial Chamber found, that the transfer of the collected Call Data Records to the Prosecutor was "legally authorised by UN Security Council Resolutions, access to the records was strictly limited, and the transfer was proportionate to the legitimate aim of investigating the attack of 14 February 2005"; thus, it "did not violate the right to privacy according to international human rights law".[166] The Trial Court's decision was upheld on appeal.[167]

B. Evidentiary Weight of DDE

As explored in the preceding Section, the approach of most international criminal courts and tribunals toward admissibility is lenient. Generally, DDE can be admitted as long as it is relevant and has probative value. Determining probative value involves an assessment of the extent to which a particular item of evidence tends to prove the facts it purports to prove, while 'weight' is used to decide the relative importance of a piece of evidence in deciding whether a fact is proven.[168] Probative value can be assessed at a preliminary stage, while weight is assigned to evidence in the final analysis. Weight is not determined in a vacuum. Authentication, provenance, and preservation all influence the weight that judges accord to the DDE. These factors are discussed in detail after considering general rules related to evidentiary weight in ICCTs.

1. General Rules on Evidentiary Weight

The ICC Chamber emphasised that "its determination on the admissibility of evidence" has "no bearing on the final weight to be afforded to it, which will only be determined by the Chamber at the end of the case when assessing the evidence as a whole".[169]

---

[164] *Bemba* Appeal Judgment (n 157) [374].

[165] ibid [376].

[166] International Bar Association Evidence (n 12) 27. *Prosecutor v. Salim Jamil Ayyash et al.* (Decision on Five Prosecution Motions on Call Sequence Tables and Eight Witness Statements and on The Legality of the Transfer of Call Data Records to UNIIIC And STL's Prosecution) STL-11-01/T/TC (6 May 2015) [108–110].

[167] *Prosecutor v. Salim Jamil Ayyash et al.* (Decision on appeal by counsel for Mr Oneissi Against the Trial Chamber's decision on the legality of the transfer of call data records) STL-11-01/T/ACAR126.9 (28 July 2015).

[168] *Musema* Trial Judgment (n 104) [41]; *Prosecutor v. Dragoljub Kunarac et al.* (Decision on Motion for Acquittal) IT-96-23 (3 July 2000) [4]; see also Richard May and Marieke Wierda, *International Criminal Evidence* (Transnational Publishers 2002) 19.

[169] *Prosecutor v. Jean-Pierre Bemba Gombo* (Decision on the admission into evidence of items deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute") ICC-01/05-01/08 (27 June 2013) [9]. A similar position was also has been held by the judges in ICTR, see *Nyiramasuhuko* Admissibility Appeal Decision (n 103) [7].

Furthermore, as held by the Chamber in *Katanga and Ngudjolo*, 'weight' is a highly subjective issue which depends on the intrinsic quality and characteristics of the evidence, as well as the amount and the quality of other available evidence on the same issue.[170]

The Rome Statute and RPE of the ICC do not provide any precise rules for determination of the weight of evidence, therefore leaving this task to the discretion of judges.[171] In the *Bemba* Confirmation of Charges, the Chamber re-iterated that it "takes a case-by-case approach in assessing the relevance and probative value of each piece" of evidence and the Chamber "will give the evidence the weight that it considers appropriate" based on its own assessment.[172]

In the *Brdanin and Talic* case, the ICTY emphasised that the admissibility of documentary evidence must be distinguished from the weight assigned to it by the tribunal, and that several different factors may be taken into account to assess this weight, such as authenticity or proof of authorship.[173]

In the *Gbagbo* Adjournment Decision, the Pre-Trial Chamber noted that evidence (especially documentary evidence) should be authenticated and have clear and unbroken chains of custody.[174] In line with this ruling, in *Bemba et al.*, the Chamber stated that it would also evaluate the source or author, the role of the evidence in relevant events, and the chain of custody in order to determine the weight of evidence.[175]

2. Weight of Demonstrative Evidence

Evidence can also be presented and admitted as demonstrative evidence, which has previously been assigned little weight by ICC judges. For instance, in the *Al-Mahdi* case, an interactive digital platform prepared in collaboration with SITU Research was introduced as demonstrative evidence to present multiple images in a clear manner.[176] Likewise, in *Katanga and Ngudjolo*, multiple satellite images and photographs were arranged into a 360-degree "virtual reality" presentation of the village of Bogoro and its surroundings, which was also admitted as demonstrative evidence.[177] In this case, the Trial Chamber noted that such demonstrative evidence had "very limited evidentiary value" and was "simply a tool for orientation, just like a diagram or drawing".[178]

---

[170] *Katanga and Ngudjolo* Bar Table Decision (n 122) [13].

[171] Robert Cryer et al., (n 104) 468; Donald Piragoff, 'Evidence', in Roy S Lee (ed) *The international Criminal Court—Elements of Crimes and rules of procedure and Evidence* (Transnational Publishers 2001) 349-401.

[172] *Prosecutor v. Jean-Pierre Bemba Gombo* (Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo) ICC-01/05-01/08 (15 June 2009) [58-59]

[173] *Prosecutor v. Radoslav Brdanin and Momir Talić* (Order on the standard governing the admission of evidence) IT-99-36-T (15 February 2002) (hereinafter '*Brdanin and Talić* Admission Standard Order') [16, 18].

[174] *Prosecutor v. Laurent Gbagbo* (Decision Adjourning the Hearing on the Confirmation of Charges Pursuant to the Article 61(7)(c)(i) of the Rome Statute) ICC-02/11-01/11 (3 June 2013) [27].

[175] *Bemba et al.* Trial Judgment (n 128) [247].

[176] Lindsay Freeman (n 11) 319; *Al Mahdi* Opening Transcript (n 124) 44-48.

[177] *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the disclosure of evidentiary material relating to the Prosecutor's site visit to Bogoro on 28, 29 and 31 March 2009) ICC-01/04-01/07-1515 (7 October 2009) [39].

[178] ibid.

In the STL case of *Ayyash et al.*, the Prosecution presented two 3D models of before and after the explosion on 14 February 2005 in Beirut, Lebanon. The models were admitted by the Chamber into evidence as "demonstrative exhibits", which have been used by the Chamber merely for evaluating the evidence.[179] Demonstrative evidence is therefore not necessarily attributed with evidentiary value as it is intended to be an aid for comprehension of the evidence.[180]

C. Authentication of DDE

Authentication is important when submitting and/or relying on DDE, as electronic evidence can be easily manipulated. Currently, there is no established procedure for authenticating DDE in international criminal law (ICL), but the RPE of international criminal courts and tribunals do contain provisions which allow the court or tribunal to request authentication of evidence. For instance, Rule 89(e) of the ICTY RPE reads: "[a] Chamber may request verification of the authenticity of evidence obtained out of court",[181] which is identical to Rule 89 of the ICTR RPE.[182] In addition, it has been established that the party submitting evidence bears the burden of establishing its authenticity.[183]

As mentioned previously, authentication has been considered a fundamental factor when weighing evidence. This was evidenced in *Martić* when the ICTY held that "[f]actors such as authenticity and proof of authorship will naturally assume the greatest importance in the Trial Chamber's assessment of the weight to be attached to individual pieces of evidence".[184]

It is important to note that although 'authenticity' is often equated with 'reliability', the two are in fact distinct concepts. Authenticity "ensure[s] the evidence has not been manipulated or tampered with",[185] whereas reliability "establishes whether a piece of evidence is what it purports to be".[186] That is, a video can be authentic, or free from manipulation, and yet be staged. For example, a government could stage a video using actors, costumes, and constructed sets to depict a particular organised armed group carrying out torture and summary executions. In this example, the staged video would be authentic so long as it has not been digitally manipulated and/or altered from its original form. However, the video would not be reliable, since the claimed conduct did not actually occur.

---

[179] International Bar Association (n 12) 28. *Prosecutor v. Salim Jamil Ayyash et al.* (Decision on Prosecution's Motion to Admit into Evidence Photographs, Videos, Maps, and 3-D Models) STL-11-01/T/TC (12 January 2014) [9]

[180] Lindsay Freeman (n 11) 320.

[181] ICTY RPE rule 89(e).

[182] ICTR RPE rule 89(e).

[183] Prosecutor v. *Milan Martić* (Decision Adopting Guidelines on the Standards Governing the Admission of Evidence) IT-95-11-T (19 January 2006) Annex A [6]: "When objections are raised on grounds of authenticity or reliability, this Trial Chamber will follow the practice of this Tribunal, namely, to admit documents and video recordings and then decide on the weight to be given to them within the context of the trial record as a whole. As provided for in Rule 89(E) of the Rules, the tendering party may be requested to provide the Trial Chamber with verification of the authenticity of evidence obtained out of court. Additionally, when an objection is made on the ground of reliability, the tendering party may be required to produce sufficient indicia of reliability to make a *prima facie* case for the admission of the document, audio tape or video in question. On the request of a party or *proprio motu*, the Trial Chamber may order the party tendering copies of evidence to present the original or the best legible, audible or visible copy available."

[184] ibid Annex A [3] (emphasis added).

[185] Aida Ashouri, Caleb Bowers and Cherrie Warden (n **Error! Bookmark not defined.**) 117.

[186] ibid, 117.

The distinction between 'authenticity' and 'reliability' has also been demonstrated in ICL jurisprudence. In *Lubanga*, the ICC Chamber held: "The *indicia* of reliability have been assessed on a broad basis and the Chamber has borne in mind that a document, although authentic, may be unreliable".[187] Furthermore, in *Popović et al.*, the ICTY Chamber held that "in determining if a document is *prima facie* [reliable], the Trial Chamber will consider whether a reasonable trier of fact could find the document to be what the tendering party purports it to be.[188] If no reasonable trier of fact could find that the document is what is purports to be, then the document is patently unreliable and does not possess the probative value required under Rule 89(C)".[189]

The ICTR Chamber, in *Bagosora et al.,* has also touched upon the overlap and distinction between authenticity and reliability, holding that "[A]uthenticity and reliability are overlapping concepts: the fact that the document is what it purports to be enhances the likely truth of the contents thereof," and has concluded that the required 'indicia of reliability' are also relevant in the assessment of a document's authenticity.[190]

Further, the ICTR Chamber in *Musema* Trial Judgment also ruled that when the weight of documentary evidence is assessed, the authenticity of a document and of its contents is vital for establishing the credibility and reliability of such evidence.[191]

In any event, after documentary evidence has been admitted, the other party "may challenge as to when, by whom and under what circumstances the material came into existence", as held by the ICTY Chamber in *Kordić*.[192]

Finally, it is important to note that in the *ad hoc* Tribunals, "while a Chamber always retains the competence under Rule 89(d) to request verification of the authenticity of evidence obtained out of court, to require absolute proof of a document's authenticity before it could be admitted would be to require a far more stringent test than the standard envisioned by Sub-rule 89(c)".[193]

In the following sections, different approaches to authenticating DDE will be discussed. These approaches include authentication *via* witness corroboration, evidence with inherent *indicia* of

---

[187] *Lubanga* Trial Judgment (n 119) [109].

[188] *Prosecutor v. Vujadin Popović et al.* (Decision on Admissibility of Intercepted Communications) IT-05-88-T (2007) (hereinafter '*Popović et al.* Intercepted Communications Decision') [35].

[189] ibid.

[190] *Prosecutor v. Bagosora et al.* (Decision on Admission of TAB 19 of Binder Produced in Connection with Appearance of Witness Maxwell Nkole (TC)) ICTR-98-41-T (13 September 2004) (hereinafter '*Bagosora et al.* Tab 19 Decision') [8].

[191] *Musema* Trial Judgment (n 104) [64].

[192] *Prosecutor v. Kordić and Čerkez* (Decision on the Prosecution Application to Admit the Tulica Report and Doessier into Evidence) IT-95-14/2-T (29 July 1999) [34, 36].

[193] Marc Nerenberg and Wibke Timmerman, 'Documentary Evidence' in Karim A. A. Khan, Caroline Buisman and Christopher Gosnell (eds) *Principles of Evidence in International Criminal Justice* (Oxford University Press 2010) 454; *Nyiramasuhuko* Admissibility Appeal Decision (n 103) [7]; *Prosecutor v. Delalić and Delić* (Decision on Application of Defendant Zejnil Delalić Leave to Appeal Against the Decision of the Trial Chamber of 19 January 1998 for the Admissibility of Evidence) IT-96-21 (4 March 1998).

authenticity, authentication *via* the origin of the evidence, and authentication *via* mutual agreement or lack of challenge.

1. Authentication via Witness Corroboration

As mentioned in Section III.B.1, in the *Tolimir* Trial Judgment, the ICTY Trial Chamber admitted the DDE on the basis of other corroborating evidence. This included "complementary forensic and anthropological reports", and testimony from two OTP prosecutors and witnesses linking the aerial images with the burial sites.[194]

In *Milutinovic et al.*, video evidence depicting the shelling of villages was submitted but the ICTY did not grant the evidence any weight as the corroborating witness testimony lacked sufficient certainty to establish when the videos were taken.[195] This demonstrates that when corroborating witness testimony is of low quality, this may adversely affect the authenticity of the DDE in question in the eyes of the Court. However, in the same case, the Court did rely on videos submitted by the Defence which were authenticated by two witnesses when determining whether a village had sustained substantial damage or was completely destroyed.[196]

In *Bemba et al.* expert witness testimony, *inter alia*, was used to establish the authenticity of DDE (in this instance, CDRs).[197] However, the Trial Chamber emphasised that:

> It was not necessary for the Prosecution to provide further testimonial evidence on [various means of establishing authenticity]. To conclude otherwise would overstate the burden of proof required and would have disproportionately lengthened the trial – it is easy to imagine that accepting the Defence's objections at face value would have led to more 'authenticity witnesses' in these proceedings than all the witnesses who actually testified on the facts and circumstances described in the charges. In the light of all the information on authenticity before the Chamber, calling witnesses solely on such matters would have been a formal and useless exercise.[198]

The decision was upheld by the Appeals Chamber by re-affirming that DDE does not necessarily need to be supported by live witness corroborating testimony.[199]

Authentication *via* witness corroboration is not limited to authentication *via* live testimony. This category may also include evidence that is authenticated through affidavits or other forms of certified information.

In the Nuremberg IMT,[200] the Prosecution based its case (in part) upon three videos documenting Nazi crimes during the Second World War (*Nazi Concentration Camps*, *The Nazi Plan*, *Cruelties of the*

---

[194] International Bar Association Evidence Matters (n 12) 25 fn.70. *Tolimir* Trial Judgment (n 113) [70].

[195] *Prosecutor v. Milan Milutinovic et al.* (Judgment) IT-05-87-T (26 February 2009) (hereinafter '*Milutinović et al.* Trial Judgment') [896-897].

[196] ibid, [884].

[197] *Bemba et al.* Appeal Judgment (n 157) [221].

[198] *Bemba et al.* Trial Judgment (n 128) [225].

[199] *Bemba et al.* Appeal Judgment (n 157) [621].

[200] Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947).

German-Fascist Intruders). These films contained within themselves certificates of authenticity, which were presented on-screen prior to the start of the film. The first certificate, given by Lieutenant Colonel George C. Stevens, stated, "these motion pictures constitute a true representation of the individuals and scenes photographed".[201] The second, from Lieutenant E.R. Kellogg, stated that "the images of these excerpts from the original negative have not been retouched, distorted or otherwise altered in any respect".[202] Furthermore, James Donovan, a member of Jackson's legal team, stated before the videos were played that "[w]hile these motion pictures speak for themselves in evidencing life and death in Nazi concentration camps, *proper authentication of the films is contained in the affidavits* of the United States Army and Navy officers to which I have referred".[203]

The Prosecution's submission of DDE authenticated *via* affidavits in the Nuremberg IMT did not go unchallenged. The Defence raised the issue that it was impossible to cross-examine the video footage, and that this was contrary to Article 16(e) of the London Charter.[204] The Prosecution refuted this by arguing that Article 19 of the London Charter allowed the Tribunal to "adopt and apply to the great possible extent expeditious and non-technical procedure and shall admit any evidence which it deems to have probative value", and should not be undermined by Article 16.[205] Furthermore, the Prosecution argued that the trial did not need to be unnecessarily elongated by having those who created the certificates of authenticity come to testify in person.[206] Ultimately, the video evidence was admitted as evidence.
On a similar note, in *Lubanga*, the Trial Chamber assessed the value of a hearsay statement contained in video evidence submitted by the Prosecution and held that "the probative value of a hearsay statement will depend upon the context and character of the evidence in question" and that "[t]he absence of the opportunity to cross-examine the person who made the statements, and whether the hearsay is 'first-hand' or more removed, are also relevant".[207]

2. Inherent Indicia of Authenticity

DDE with inherent indicia of authenticity[208] includes but may not be limited to DDE with internal markers (e.g., metadata) and external factors (e.g., DDE collected and prepared by the Registry). Thus, DDE with inherent indicia of authenticity has intrinsic secondary information such as metadata (e.g., geolocation, time, and date) which corroborates the primary evidence (e.g., the metadata corroborates that a video was taken is a particular location as the metadata corresponds to the geolocation of images depicted within the video).

---

[201] 2 Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947) 433.

[202] ibid 433-434.

[203] 2 Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947) 433 (emphasis added)

[204] Agreement by the Government of the United Kingdom of Great Britain and North Ireland, the Government of the United States of America, the Provisional Government of the French Republic and the Government of the Union of Soviet Socialist Republics for the Prosecution and Punishment of the Major War Criminals of the European Axis (concluded 8 August 1945 London) 82 UNTS 279 (hereinafter 'London Charter') art.16(e).

[205] 3 Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947) 545.

[206] ibid.

[207] *Lubanga* Four Documents Decision (n 100) [28].

[208] The terminology "Inherent Indicia of Authenticity" was taken from *Bemba et al.* Trial Judgment (n 128) [219].

An instance of DDE with indicia of authenticity is discussed in the ICC's *Bemba et al.* case, which focused on recordings of ICC Detention Centre communications. In this case, the Trial Chamber conducted its own independent assessment of the evidence,[209] finding that "some communications and logs do have inherent indicia of authenticity".[210] For example, some call logs had corporate watermarks of the telecommunications providers, or began with "persons identifying themselves as the ICC when connecting Mr. Bemba's calls".[211]

From the tribunals' jurisprudence, several key factors of inherent indicia of authenticity emerge. These include DDE containing watermarks, metadata, or other forms of identification inherently present in the evidence (such as communications beginning with an individual stating they are from the ICC).

3. Authentication via Origin of the Evidence

In *Bemba et al.*, the Trial Chamber held that it was unreasonable and unnecessary to call witnesses to authenticate materials for which the Registry had kept a log of chain of custody, exhaustively chronicled when seized, and were unsealed by the Registry in the physical presence of one or more members of the Defence counsel.[212]

4. Authentication by Mutual Agreement or Lack of Challenge

DDE has also been found to be authentic by the ICC when its authenticity is not challenged by any party or has been agreed upon as authentic. For instance, in *Lubanga*, the Prosecution submitted video evidence which was not challenged by the Defence (although the corroborating witness testimony was criticised), and the Trial Chamber found the video to be authentic.[213] This principle was confirmed in *Bemba* when the ICC held that authenticity can be established when the parties are in agreement as to the authenticity of the evidence.[214] In *Al Mahdi*, the Prosecutor used a novel digital platform to virtually reconstruct locations and demonstrate the damage to them. As the accused entered a guilty plea, which the Court accepted, the authenticity of this evidence was never challenged, and this instance may be viewed at as authentication by mutual agreement.[215]

Authentication by mutual agreement is not unique to DDE. The ICC RPE maintains that evidence which is mutually agreed upon, including DDE, may be considered "as being proven, unless [a] Chamber is of the opinion that a more complete presentation of the alleged facts is required in the interests of justice, in particular the interests of the victims."[216] Therefore, it is possible to have DDE authenticated by mutual agreement of the parties.

---

[209] ibid [216].

[210] ibid.

[211] ibid [219].

[212] ibid [222-225].

[213] *Lubanga* Trial Judgment (n 119) [710].

[214] *Prosecutor v. Jean-Pierre Bemba Gombo et al (*Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute) ICC-01/05-01/08-2299-Red (8 October 2012) [9]

[215] *Prosecutor v. Ahmad Al Faqi Al Mahdi* (Judgment and Sentence) ICC-01/12-01/15 (27 September 2016).

[216] ICC RPE Rule 69.

D. Provenance

International criminal courts and tribunals have often considered the provenance to determine authenticity.[217] In order to establish provenance—also known as chain of custody—a tribunal may require testimony about the authorship, conservation, and movement of the evidence.[218]

a) International Criminal Tribunal for the Former Yugoslavia (ICTY)

In *Popović et al.*, the Trial Chamber admitted intercepted radio communications as evidence.[219] The Prosecution submitted testimony by several witnesses, including intercept operators, an expert in radio relay communications, and a Prosecution analyst.[220] The Defence challenged the chain of custody of the DDE, since "not even the [intercept] operators themselves were certain where the intercepts were sent and some pages turned up missing."[221] Further, the Prosecution expert witness could not explain the whereabouts of the intercept materials from July 1995 to Prosecution acquisition in 1998, which Defendant Beara characterised as "a complete lack of any legally sufficient chain of custody."[222] Nevertheless, the Trial Chamber was satisfied from witness testimony about the chain of custody,[223] and in its final judgment found that there was no deficiency in the chain of custody of the intercept materials.[224] In evaluating the evidentiary weight of the DDE, the Court gave the evidence significant weight because of author testimony that the handwritten transcriptions were contemporaneous with the events.[225]

In *Milutinovic et al.*, a witness testified that he made a video showing excessive use of force in Kosovo.[226] The witness testified that he had handed over the video to the Foreign Liaison Service and one other person.[227] The individuals he supposedly handed the evidence over to, however, contradicted his testimony upon cross-examination.[228] This led to the Court not giving any weight to the testimony relating to the chain of custody of the video.[229]

---

[217] *Prosecutor v. Vidoje Blagojević and Dragan Jokić* (Trial Judgment) IT-02-60-T (17 January 2005) [29].

[218] ibid.

[219] *Prosecutor v. Vujadin Popović et al.* (Judgment Volume I) IT-05-88-T (10 June 2010) (hereinafter '*Popović et al.* Trial Judgment') [64-66].

[220] ibid [65].

[221] *Prosecutor v. Popović et al.* (Defendant, Ljubisa Beara's notice of filing a public redacted version of the Beara Final Trial Brief) IT-05-88 (28 July 2010) [271].

[222] *Prosecutor v. Popović et al.* (Decision on Admissibility of Intercepted Communications) IT-05-88-T (7 December 2007) [66].

[223] ibid [67].

[224] *Prosecutor v. Popović et al.* (Trial Judgment) (n 219) [64-66].

[225] ibid [65].

[226] *Milutinovic et al.* Trial Judgment (n 195) [546].

[227] ibid.

[228] ibid.

[229] ibid.

In *Brdanin*, intercepted telephone communications were admitted even though the chain of custody was not clearly established and the original, missing evidence was different than that which the Court relied upon.[230] The intercepted communications were originally recorded on cassettes and an incomplete version of the audio was transferred to storage tapes.[231] The storage tapes were in "unsupervised possession" without logs or methods of preservation for years before coming into the possession of the OTP.[232] The original recording cassettes were erased.[233] However, despite lack of authorship testimony and the fact that the DDE had been edited, the Trial Chamber was "satisfied beyond reasonable doubt of the reliability even though the chain of custody was not perfect".[234]

b) International Criminal Tribunal for Rwanda (ICTR)

As opposed to the ICC and ICTY, the ICTR has refused to admit evidence without the corroboration of the author's testimony. For example, in *Renzaho*, the Court refused to admit audio evidence of a telephone recording due to lack of information regarding the provenance of the audiotape, despite four witnesses claiming to identify the accused's voice on the recording.[235] Only after the journalist who recorded the audiotape testified in court was the tape was admitted.[236]

c) International Criminal Court (ICC)

At the ICC, judges find much evidence admissible and evaluate the weight of the evidence subsequently after the admission of the evidence.[237] In addition, the Court noted pre-trial in *Lubanga* that nothing in the Rome Statute framework "expressly states that the absence of information about the chain of custody or transmission affects the admissibility or probative value of Prosecution evidence".[238] Therefore, the absence of authorship testimony will not usually lead to the inadmissibility of the DDE. This is especially the case if the Defence does not specifically object to the provenance but only raises a 'general objection' to the admissibility of the evidence.

Although a lack of clear provenance and an absence of author testimony does not automatically result in the inadmissibility of evidence, ICC judges appear to accord more weight to DDE if its provenance has been well investigated and established. In the case of *Bemba et al.*, the Defence quoted from digital source materials without strictly following the established procedure by failing to disclose the evidence

---

[230] *Prosecutor v. Radoslav Brdanin* (Judgment) IT-99-36-T (1 September 2004) [34].

[231] ibid.

[232] *Prosecutor v. Radoslav Brdanin* (Decision on the Defence "Objection To Intercept Evidence"') (3 October 2003) [13.2].

[233] ibid.

[234] ibid.

[235] *Prosecutor v. Tharcisse Renzaho* (Decision on Exclusion of Testimony and Admission of Exhibit) ICTR-97-31-T (2007) (hereinafter '*Renzaho* Exclusion and Admission Decision') [1, 2].

[236] ibid.

[237] ibid, 116.

[238] *Lubanga* Confirmation Decision (n 144) [96].

to the Court and the Prosecution for inspection before trial.[239] The Court determined that since neither the provenance nor the reliability of the evidence had been clearly established, or even tested, the materials carried "little, if any, evidentiary weight".[240]

E. Preservation of DDE

In order for a Court to rely on DDE, it is necessary that the evidence has been properly preserved. Preservation is defined as "long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span the information is required for".[241]

a) International Criminal Tribunal for the Former Yugoslavia (ICTY)

In *Popović et al.*, the Prosecution sought submission of intercepted communications that were initially recorded on audiotapes that had not been preserved.[242] The audiotapes had been transcribed by intercept operators into handwritten notebooks,[243] which were then typed into computers so electronic versions of the communications could be sent to Command.[244] Due to the fact that the Prosecution did not have all original audiotapes, the ICTY allowed the handwritten notes.[245]

The Defence challenged the admissibility of the handwritten notes on the basis of a lack of preservation of the audiotapes.[246] The Trial Chamber stated that in light of 28 testimonies by intercept operators who verified the authenticity of the evidence by identifying their own handwriting and confirming they indeed transcribed the conversation into the notebooks, the evidence was admissible, despite the Trial Chamber acknowledging that it was "conscious that discrepancies exist in the testimony of the intercept operators".[247]

In the same case, altered evidence was submitted by the Prosecution and challenged by the Defence. The altered evidence consisted of aerial images that were provided by the US government, purporting to show burial sites,[248] though the Defence challenged the lack of comparative aerial imagery and the lack of site codes and coordinates.[249] In addition, the witness through whom the evidence was tendered

---

[239] *Prosecutor v. Jean-Pierre Bemba Gombo et al.* (Decision on the Admissibility and Abuse of Process Challenges) ICC-01/05-01/08 (24 June 2010) [254].

[240] ibid [255].

[241] US Legal, 'Digital Preservation Law and Legal Definition' <https://definitions.uslegal.com/d/digital-preservation> accessed 15 December 2020.

[242] *Prosecutor v. Popović et al.* (Decision on Admissibility of Intercepted Communications) IT-05-88-T (7 December 2007) [3].

[243] ibid [39].

[244] ibid.

[245] ibid.

[246] ibid [41].

[247] ibid [42].

[248] *Prosecutor v. Popović et al.* Trial Judgment (n 219) IT-05-88-T [72].

[249] ibid [74].

stated that he had added and removed dates on certain images.[250] Despite this, the ICTY admitted the evidence on the "extensive evidence" given by three witnesses.[251] Furthermore, the Trial Chamber stated that it did not find that the weight of the aerial images adversely affected by the witness's "explanation that for the purposes of this case, he had erased certain dates, marked by the United States Government in white, and replaced them by dates marked with a colour pen".[252]

In *Tolimir*, the Prosecution also submitted aerial images to prove the existence of burial sites and reburials, buildings and vehicles, large groups of prisoners, and bodies. [253] As in *Popović et al.*, these images had also been provided by the US government, pursuant to Rule 70, prohibiting the Prosecution discussing any information relating to the origin of this evidence during the case.[254] The Trial Chamber acknowledged the Defence's argument that the reliability of the evidence was impaired without information on the method of creation and editing of the aerial images.[255] However, the Court still found the aerial images to be reliable and of probative value, and admitted them into evidence because two witnesses testified extensively on the use of the images.[256]

As previously stated, the bar for admissions of evidence at the ICTY is low. The Court finds evidence that has not been properly preserved often admissible. However, the challenged evidence was in those cases always complemented by extensive witness testimonies, often by the authors of the evidence.

b) International Criminal Court (ICC)

The topic of preservation has not yet been adjudicated in the case law of the ICC.[257] However, the Court is currently developing it's "e-Court protocol," which includes developing and standardising the preservation of DDE submitted to the Court.[258]

[250] ibid.

[251] ibid [73].

[252] ibid [75].

[253] *Prosecutor v. Tolimir* Trial Judgment (n 113) [67].

[254] ibid [68].

[255] ibid [69].

[256] ibid [70].

[257] Aida Ashouri, Caleb Bowers and Cherrie Warden (n 22) 123-125.

[258] ibid, 124.

F. Conclusion

Concerning admissibility, unlike some domestic systems, the approach of most international criminal courts and tribunals is lenient. Generally, DDE can be admitted as long as it is relevant and has probative value. After DDE is admitted, judges accord weight to the evidence using their discretion. Authentication, provenance, and preservation all influence the admissibility and weight the judges accord to the DDE.

Furthermore, international criminal courts and tribunals must ensure that the evidence being presented has not been manipulated or tampered with in order to determine whether the evidence is authentic. As digital evidence can be easily manipulated, authentication is particularly important in the field of DDE. This topic has been discussed in some ICL case law along with provisions in the RPE of international courts and tribunals, which contain procedures allowing the court or tribunal to request authentication. At the ICC, in *Bemba et al.*, the Court held that DDE does not necessarily need to be supported by corroborating testimony, but it is common practice to have a witness establish the authenticity of the DDE.[259] Moreover, in cases where corroborating testimony is of a low quality, it can affect the authenticity of the DDE in question, so much that the Court may not find the evidence to be admissible.[260] Practice shows that authentication of the evidence is very relevant for admissibility of DDE. However, since there is no standard procedure for authenticating evidence, there is an absence of clarity surrounding the topic. Therefore, there is a need for a means of authenticating evidence consistently.

In order to determine the authentication of DDE, international courts and tribunals have often examined the chain of custody, or provenance, of the DDE. At the ICC and ICTY, the threshold for admissibility for evidence regarding the chain of custody seems low.[261] The judges do accord more weight to DDE if its provenance has been well established, preferably with author testimony.[262] The ICTR refuses to admit evidence without a clearly established chain of custody.[263] Therefore, it is important that data that may help verify the chain of custody of DDE is well maintained.

Preservation of DDE, on the other hand, has not yet been discussed in the case law of many courts and tribunals. Only the ICTY has made statements regarding the importance of the preservation of DDE in its case law.[264] Similar to that of provenance, the bar for admissibility of poorly preserved evidence at the ICTY seems low. The Court finds evidence that has been poorly preserved often admissible.[265] However, in these cases, DDE is always complemented by corroborating evidence. This is likely to become an area of growing importance for DDE. Courts and tribunals should consider

[259] *Bemba et al.* Abuse of Process Decision (n 239) [621, 221].

[260] *Milutinovic et al.* Judgment (n 195) [896-897].

[261] *Lubanga* Confirmation Decision (n 144) [96]; *Brdanin and Talic* Admission Standard Order (n 173) [18].

[262] *Popović et al.* Trial Judgment (n 219) [66].

[263] *Renzaho* Exclusion and Admission Decision (n 235) [1-2].

[264] *Popović et al.* Trial Judgment (n 219); *Tolimir* Trial Judgment (n 113) [67].

[265] *Popović et al.* Trial Judgment (n 219) [39-44].

working closely with NGOs that have developed additional tools such as the 'EyeWitness App',[266] which allows civilians to film videos and effectively store them in a database, and 'MediCapt', which allows health care workers to capture, preserve, and transmit forensic evidence of cases of sexual violence.[267]

.

[266] Owen Bowcott, 'EyeWitness to Atrocities: the app aimed at bringing war criminals to justice' (2015) The Guardian < https://www.theguardian.com/technology/2015/jun/08/eyewitness-to-atrocities-the-app-aimed-at-bringing-war-criminals-to-justice>. See also <https://www.eyewitnessproject.org>.

[267] Physicians for Human Rights 'PHR's mobile app MediCapt puts cutting edge technology in the service of preventing sexual violence' (19 May 2019) < https://phr.org/issues/sexual-violence/program-on-sexual-violence-in-conflict-zones/tools/> accessed 15 December 2020.

IV. Overall Conclusion

The primary mission of international courts and tribunals is to put an end to impunity for perpetrators committing the most serious crimes of concern to the international community. Evidence is the key element in proving the crime and linking the accused to the crime committed. Yet, since Nuremberg, international courts and tribunals have adopted a rather flexible approach towards the rules of procedure and evidence, which has provided challenges for practitioners in evaluating DDE.

This report has highlighted the major role that DDE plays in international criminal investigations and trials. Due to the fact that currently there is no standardised procedure for the use of DDE in ICL, the report has highlighted several challenges mostly pertaining to admissibility and weight, authentication, provenance, and preservation, and practices in domestic jurisdictions.

Since DDE is becoming more and more prevalent in ICL courtrooms, further development of clear rules and standardised formats for the use of DDE is necessary. This would result in more credibility of DDE in international legal proceedings and would aid the efficiency of trials in front of courts and tribunals. Because of ongoing resource inequalities between the Office of the Prosecutor and the Defence, sufficient and adequate resources must be available for the Defence to investigate DDE.[268] In this regard, the ICC should provide funding to hire experts, and open opportunities for training when investigating sources of digital evidence.

In light of the rapid development of digital technologies, admitting and evaluating DDE has been particularly challenging for international courts, partly due to a lack of technological literacy amongst those inside the courtroom. The lack of expertise and knowledge on DDE in the courtroom could hamper the work of international courts and tribunals when evaluating the evidence. International criminal courts and tribunals must adapt by incorporating the necessary technical facilities and expertise to collect and work with DDE and new types of evidence. Further trainings and workshops on emerging electronic technologies should be available for judges and lawyers, which could significantly help to fill the potential gap of technological knowledge relating to DDE amongst courtroom officials. We hope this Report is one step in this process of advancing knowledge of DDE.

[268] International Bar Association (n 12) 32.

List of Cases

A. International Cases

1. International Criminal Tribunal for Former Yugoslavia

- Prosecutor v. Dragoljub Kunarac et al.(Decision on Motion for Acquittal) IT-96-23 (3 July 2000)
- Prosecutor v. Dusko Tadić (Decision on Defence Motion on Hearsay) IT-94-1-T (5 August 1996)
- Prosecutor v. Milan Martić (Decision Adopting Guidelines on the Standards Governing the Admission of Evidence) IT-95-11-T (19 January 2006)
- Prosecutor v. Milan Milutinovic et al. (Judgment) IT-05-87-T (26 February 2009)
- Prosecutor v. Radislav Krstić (Trial Judgment) IT-98-33-T (2 August 2001)
- Prosecutor v. Radoslav Brdanin and Momir Talic, (Order on the standard governing the admission of evidence) IT-99-36-T (15 February 2002)
- Prosecutor v. Radoslav Brdanin (Judgment) IT-99-36-T (1 September 2004)
- Prosecutor v. Ratko Mladić (Transcript) IT-09-92-T (26 September 2013)
- Prosecutor v. Ratko Mladić (Judgment, Volume II of V), IT-09-92-T (22 November 2017)
- Prosecutor v. Vidoje Blagojević and Dragan Jokić (Trial Judgment) IT-02-60-T (17 January 2005)
- Prosecutor v. Vujadin Popović et al. (Decision on Admissibility of Intercepted Communications) IT-05-88-T (7 December 2007)
- Prosecutor v. Vujadin Popović et al. (Judgment Volume I) IT-05-88-T (10 June 2010)
- Prosecutor v. Zdravko Tolimir (Defence Final Trial Brief) IT-05-88/2-T (1 October 2012)
- Prosecutor v. Zdravko Tolimir (Judgment) IT-05-88/2-T (12 December 2012)
- Prosecutor v. *Zejnil Delalić* Delalić et al. (Decision on the Motion of the Prosecution for the Admissibility of Evidence) IT-96-21-T (19 January 1998)

2. International Criminal Tribunal for Rwanda

- Prosecutor v. Alfred Musema (Judgment and Sentence) ICTR-96-13-A (27 January 2000)
- Prosecutor v. *Théoneste* Bagosora et al. (Decision on the Admissibility of Proposed Testimony of Witness DBY) ICTR-98-41-T (18 September 2003)
- Prosecutor v. *Théoneste* Bagosora et al. (Decision on Prosecutor's Interlocutory Appeal Regarding Exclusion of Evidence) ICTR-98-41-AR73.14 (19 December 2003)
- Prosecutor v. *Théoneste* Bagosora et al. (Decision on Admission of TAB 19 of Binder Produced in Connection with Appearance of Witness Maxwell Nkole (TC)) ICTR-98-41-T (13 September 2004)
- Prosecutor v. *Édouard* Karemera et al. (Decision on the Prosecutor's Motion for Admission of Certain Exhibits into Evidence) ICTR-98-44-T (25 January 2008)

- Prosecutor v. *Édouard* Karemera et al. (Decision on Joseph Nzirorera's Appeal of Decision on Admission of Evidence Rebutting Adjudicated Facts) ICTR-98-44-AR73.17 (29 May 2009)
- Prosecutor v. Karemera et al. (Judgment) ICTR-98-44-T (2 February 2012)
- Prosecutor v. Pauline Nyiramasuhuko et al. (Decision on Pauline Nyiramasuhuko's Appeal on the Admissibility of Evidence) ICTR-98-42-AR73.2 (4 October 2004)
- Prosecutor v. Tharcisse Renzaho (Decision on Exclusion of Testimony and Admission of Exhibit) ICTR-97-31-T (2007)

3. International Criminal Court

- Prosecutor v. Ahmad Al Faqi Al Mahdi, (Opening Transcript) ICC-01/12-01/15-T-4-Red-ENG (22 August 2016)
- Prosecutor v. Ahmad Al Faqi Al Mahdi (Judgment and Sentence) ICC-01/12-01/15, (27 September 2016)
- Prosecutor v. Francis Kirimi Muthaura et al. (Decision on the Confirmation of Charges Pursuant to Article 61(7)(a) and (b) of the Rome Statute) ICC-01/09-02/11 (23 January 2012)
- Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui, (Decision on the disclosure of evidentiary material relating to the Prosecutor's site visit to Bogoro on 28, 29 and 31 March 2009) ICC-01/04-01/07-1515 (7 October 2009)
- Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui (Decision on the Prosecutor's Bar Table Motions) ICC-01/04-01/07 (17 December 2010)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Decision on the Admissibility and Abuse of Process Challenges) ICC-01/05-01/08 (24 June 2010)
- Prosecutor v. Jean-Pierre Bemba Gombo (Decision on the admission into evidence of items deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute") ICC-01/05-01/08 (27 June 2013
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute) ICC-01/05-01/08-2299-Red (8 October 2012)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Public Redacted Version of Defence Response to Prosecution's Third Request for the Admission of Evidence from the Bar Table) ICC-01/05-01/13 (9 October 2015)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Decision on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7)) ICC-01/05-01/13 (29 April 2016)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Public Redacted Version of "Corrigendum of ICC-01/05-01/13-1902-Conf-Corr") ICC-01-05-01/13 (29 July 2016)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Judgment Pursuant to Article 74 Rome Statute) ICC-01/05-01/13 (19 October 2016)
- Prosecutor v. Jean-Pierre Bemba Gombo et al. (Appeal Judgment) ICC-01/05-01/13 (8 March 2018)

- Prosecutor v. Laurent Gbagbo (Decision Adjourning the Hearing on the Confirmation of Charges Pursuant to the Article 61(7)(c)(i) of the Rome Statute) ICC-02/11-01/11 (3 June 2013)
- Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli (Warrant of Arrest) ICC-01/11-01/17 (15 August 2017)
- Prosecutor v. Thomas Lubanga Dyilo (Decision on the Admissibility of four documents) ICC-01/04-01/06 (13 June 2008)
- Prosecutor v. Thomas Lubanga Dyilo (Decision on the Admission of Material from the Bar Table) ICC-01/04-01/06 (24 June 2009)
- Prosecutor v. Thomas Lubanga Dyilo (Decision on Confirmation of Charges) ICC-01/04-01/06 (29 January 2007)
- Prosecutor v. Thomas Lubanga Dyilo (Judgment pursuant to Article 74 of the Statute) ICC-01/04-01/06 (14 March 2012)
- Prosecutor v. Thomas Lubanga Dyilo (Judgment on the Appeal of Mr Thomas Lubanga Dyilo against his conviction) ICC-01/04-01/06 (1 December 2014)
- Prosecutor v. William Samoei Ruto and Joshua Arap Sang (Transcript) ICC-01/09-01/11-T-66-Red-ENG (5 November 2013)

4. Special Tribunal for Lebanon

- Prosecutor v. Salim Jamil Ayyash et al. (Decision on Prosecution's Motion to Admit into Evidence Photographs, Videos, Maps, and 3-D Models) STL-11-01/T/TC (12 January 2014)
- Prosecutor v. Salim Jamil Ayyash et al. (Decision on Five Prosecution Motions on Call Sequence Tables and Eight Witness Statements and on The Legality of the Transfer of Call Data Records to UNIIIC And STL's Prosecution) STL-11-01/T/TC (6 May 2015)
- Prosecutor v. Salim Jamil Ayyash et al. (Decision on the Admissibility of Documents Published on the Wikileaks Website) STL-11-01/T/TC (21 May 2015)
- Prosecutor v. Salim Jamil Ayyash et al. (Decision on appeal by counsel for Mr Oneissi Against the Trial Chamber's decision on the legality of the transfer of call data records) STL-11-01/T/ACAR126.9 (28 July 2015)

5. Nuremberg Tribunal

- Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947)
- 2 Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947)
- 3 Trial of The Major War Criminals Before the International Military Tribunal 98-99 (1947)

B. Domestic Cases

1. France

- Tribunal Correctionnel Paris, 17e ch - ch de la presse, 9/4/2016, LICRA, SOS Racisme / M. X

2. Germany

- Higher Regional Court, Judgment of 8 November 2016 - 5-3 StE 4/16-4-3/16, 8 November 2016
- Superior Court of Justice Berlin 2a Criminal Division, *Judgment of 1 March 2017* - (2A) 172 OJs 26/16 (3/16), 2A 172 OJs 26/16 (3/16)

3. Indonesia

- Judgment of Constitutional Court of the Republic of Indonesia, No 20/PUU-XIV/2016 (27 September 2016)

4. Nigeria

- Kubor v. Dickson [2012] Supreme Court of Nigeria

5. The Netherlands

- HR 20 December 1926, ECLI:NL:1926:BG9435, *NJ* 1927/85 (Supreme Court of the Netherlands).
- HR 11 January 2011, ECLI:NL:HR:2011:BP0291, *NJ* 2011/116 (Supreme Court of the Netherlands).
- HR 29 March 2016, ECLI:NL:HR:2016:522, *NJ* 2016/249 (Supreme Court of the Netherlands).
- HR 10 July 2018, ECLI:NL:HR:2018:1125, *NJ* 2018/1531 (Supreme Court of the Netherlands).

6. The United States of America

- Kortz v. Guardian Life Ins. Co., 144 F.2d 676 (10th Cir. COA 1944)
- Riley v. California, 134 S. Ct. 2473 (2014)

V. Bibliography

A. Books

Cryer R et al., *An Introduction to International Criminal Law and Procedure* (Cambridge University Press 2016)

Garner B A, *Black's Law Dictionary* (9th ed, West 2009)

May R and Wierda M, *International Criminal Evidence* (Transnational Publishers 2002

Piehler G K and Johnson M H, *Encyclopedia of Military Science* (SAGE Publications Inc, 2013)

Slutier G et al., *International Criminal Procedure Principles and Rules* (Oxford University Press 2013)

B. Book Chapters

Gosnell C, 'Admissibility of Evidence' in in Karim A.A. Khan, Caroline Buisman and Christopher Gosnell (eds), *Principles of Evidence in International Criminal Justice* (Oxford University Press 2018)

Nerenberg M and Timmerman W, 'Documentary Evidence' in Karim A. A. Khan, Caroline Buisman, Christopher Gosnell (eds), *Principles of Evidence in International Criminal Justice* (Oxford University Press 2018)

Piragoff D, 'Evidence', in Roy S Lee (ed) *The international Criminal Court—Elements of Crimes and rules of procedure and Evidence* (Transnational Publishers 2001)

C. Journal Articles

Angelosanto P, 'Le intercettazioni telematiche e le criticità del date retention nel contrasto alla criminalità organizzata' (2014) 4 *Sicurezza e Giustizia* 8

Ashouri A, Bowers C and Warden C, 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115

Freeman L, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2017) 41 *Fordham International Law Journal* 283

Mercer L D, 'Computer Forensics: Characteristics and Preservation of Digital Evidence' (2004) 73(3) *The FBI Law Enforcement Bulletin* 28

Mulyawan B, 'Kekuatan Alat Bukti Informasi Elektronik dalam Penyidikan Tindak Pidana Keimigrasian' (2018) 12 *Jurnal Ilmiah Kebijakan Hukum* 107

Tion T, 'Electronic evidence in Nigeria' (2014) *Digital Evidence and Electronic Signature Law Review* 11

Vranesic Z G and Smith K C 'Engineering aspects of multi-valued logic systems' (1974) 7(9) *Computer* 34

D. Online Articles

Barley M, "Chinese court launches blockchain evidence platform" *Ledger Insights* (2018) <https://www.ledgerinsights.com/chinese-court-blockchain-evidence-platform/> accessed 15 December 2020

Droits-finances staff, 'Huissier de justice: rôle et missions' (2019) <https://droit-finances.commentcamarche.com/contents/1367-huissier-de-justice-role-et-missions> accessed 15 December 2020

Hudson M, 'What is Social Media?' *The Balance Small Business* (8 May 2019) <https://www.thebalancesmb.com/what-is-social-media-2890301> accessed 13 December 2020

Hui S, Ruan Z and Zhuang F, 'China's New Judicial Guidance clarifies scope and improves efficiency of internet disputes' *Lexology* (7 September 2018) <https://www.lexology.com/library/detail.aspx?g=76173563-dae4-4804-9cfe-cbd52413fe0a> accessed 15 December 2020

James J, 'How Facebook Handles Image EXIF Data' ITPro Today (7 December 2011) < https://www.itprotoday.com/strategy/how-facebook-handles-image-exif-data> accessed 15 December 2020

Kotz S, 'What is the difference between Satellite Imagery and Aerial photography?' *Sciencing* (13 March 2018), <https://sciencing.com/up-date-satellite-pictures-look-at-13825.html> accessed 13 December 2020

Louloudis T, 'What is a podcast and where can I find the best ones to listen to?' *The Telegraph* (13 July 2020) <https://www.telegraph.co.uk/radio/podcasts/what-is-a-podcast-and-where-can-i-find-the-best-ones-to-listen-t/> accessed 13 December 2020

Corbalán F, 'En libertad queda joven acusado de agredir a carabinero: pruebas sólo eran fotos de Facebook" ["Young Men Accused of Attacking a Policeman is Released: Evidence was solely Based on Facebook Pictures'] (2014) Rabio Bío Bío <*https://eff.org/r.4u9z*> accessed 15 December 2020.

Wolfie Z, "China's Supreme Court Recognizes Blockchain Evidence as Legally Binding" (7 September 2018) *Coindesk* <https://www.coindesk.com/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding> accessed 15 December 2020

vandePol M et al., 'China issues new rules to clarify procedures for collection of electronic data in criminal cases' (19 February 2019) Global Compliance News, Baker McKenzie <'https://globalcompliancenews.com/china-issues-new-rules-clarify-procedures-collection-electronic-data-criminal-cases-20190212/> accessed 15 December 2020.

E. Reports

Eurojust, 'Prosecuting war crimes of outrage upon personal dignity based on evidence from open sources – Legal framework and recent developments in the Member States of the European Union' (2018) <http://www.eurojust.europa.eu/doclibrary/genocide-network/KnowledgeSharing/Prosecuting%20war%20crimes%20of%20outrage%20upon%20personal%20dignity%20based%20on%20evidence%20from%20open%20sources%20(February%202018)/2018-02_Prosecuting-war-crimes-based-on-evidence-from-open-sources_EN.pdf> accessed 15 December 2020.

Goodison S E, Davis R C, and Jackson B A, 'Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence' (Rand Corporation, 2015) <https://www.rand.org/pubs/research_reports/RR890.html> accessed 24 April 2019

Human Rights Center UC Berkeley, School of Law, 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court '(UC Berkeley, Berkeley February 2014)

ICC Office of the Prosecutor, 'Strategic Plan 2016-2018' (16 November 2015)

ICC Office of the Prosecutor, '[draft] Strategic Plan 2019-2012' (14 May 2019)

International Bar Association, 'Evidence Matters in ICC Trials: An International Bar Association International Criminal Court & International Criminal Law Programme report providing a comparative perspective on selected evidence matters of current importance in ICC trial practice' (August 2016)

OSCE, 'Conference Report: Role of Domestic Jurisdictions in the Implementation of International Humanitarian Law (IHL) – Law and Practice' (OSCE, 19-20 May 2014) <https://www.osce.org/odihr/142256?download=true> accessed 15 December 2020

F. Miscellaneous

'metadata' (*Merriam-Webster Dictionary,* 2019) <https://www.merriam-webster.com/dictionary/metadata> accessed 15 December 2020

'photograph' (*English Oxford Living Dictionaries)* <https://en.oxforddictionaries.com/definition/photograph> accessed 15 December 2020

'video' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/video> accessed 13 December 2020

'Digital Preservation Law and Legal Definition' <https://definitions.uslegal.com/d/digital-preservation> accessed 15 December 2020

'Weight of the evidence" *Legal Information Institute* < https://www.law.cornell.edu/wex/weight_of_the_evidence> accessed 15 December 2020

G. International Agreements/Treaties/Conventions

Agreement by the Government of the United Kingdom of Great Britain and North Ireland, the Government of the United States of America, the Provisional Government of the French Republic and the Government of the Union of Soviet Socialist Republics for the Prosecution and Punishment of the Major War Criminals of the European Axis (concluded 8 August 1945 London) 82 UNTS 279

Rome Statute of the International Criminal Court, (entered into force 1 July 2002, last amended in 2010), 2187 UNTS 90

H. Rules of Procedure and Evidence of International Courts and Tribunals

International Criminal Court Rules of Procedure and Evidence (2013) ICC-PIDS-LT-02-002/13_Eng

International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994), IT/32Rev.50x

International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995)

Special Tribunal for Lebanon, Rules of Procedure and Evidence (last amended on 10 April 2019, adopted on 20 March 2009) STL-BD-2009-01-Rev.10

I. National Legislation

1. Canada

Canada Evidence Act R.S.C 1985, c. C-5 (last amended 18 October 2017)

2. Chile

Chilean Criminal Procedure Code (2000)

3. China

Criminal Procedure Law of People's Republic of China

4. Germany

German Code of Criminal Procedure (last amended 23 April 2014)

5. Indonesia

Law No. 11/2008 on Electronic Information and Transactions

6. Italy

Italian Code of Criminal Procedure (2011)

7. Nigeria

Evidence Act (2011)

8. Saudi Arabia

Electronic Transactions Law, Royal Decree No. M/18, 8 Rabi' I 1428H

9. The United States of America

Federal Rules of Evidence 902

.