Dragi Rashkovski, PhD*
Veronika Rashkovska, PhD**

THE DIFFERENCE BETWEEN DIGITAL EVIDENCE AND EVIDENCE IN DIGITAL FORM

Abstract

At first glance, the two concepts—*digital evidence* and *evidence in digital form*—may seem synonymous. However, while all digital evidence can indeed be classified as evidence in digital form, not all evidence in digital form qualifies as digital evidence. This distinction leads to the conclusion that digital evidence constitutes a subset of evidence in digital form. Yet, even this conclusion is not entirely absolute, as for digital evidence to be admissible in judicial proceedings, it must satisfy specific prerequisites. These are not merely technical prerequisites—which fall outside the scope of this paper—but primarily legal prerequisites that determine whether "ordinary" digital records may be transformed into "admissible" digital evidence capable of serving as the basis for a court ruling.

Digital evidence, as a specific category of evidence in digital form, is distinguished from other types of digital-form evidence by the presence of metadata, which serves to substantiate many of its inherent properties. In the absence of such metadata, digital evidence is reduced to mere evidence in digital form, lacking the distinctive qualities that render it probative and admissible.

Metadata is often described as "data about data." These are digital records which, although sometimes invisible or, if visible, incomprehensible to the ordinary user of information technology, provide the unique "fingerprint" of a digital record. Much like a fingerprint left on a physical piece of evidence, metadata authenticates and preserves the integrity of the digital record. Without such a "fingerprint," one might say that "the glass is shattered on the floor, but it cannot be determined which of those present threw it." Metadata thus constitutes the DNA of a digital record. Although technical in its essence, metadata is not merely a technical concept. It also functions as a legal category, explicitly addressed in numerous legal instruments regulating the collection of digital evidence, which underscores its fundamental importance.

One of the objectives of this scholarly paper is to make this legal-technical concept more accessible to legal practitioners—judges, prosecutors, defense attorneys, and others—through illustrative examples and an interpretation of existing international legal norms, thereby enabling them to reason in accordance with relevant international standards. At the same time, by examining domestic (Macedonian) legislation, which addresses this subject within what appears to be a somewhat "forgotten" statute, the paper seeks to highlight the gaps that must be addressed in order to ensure the effective application of these norms.

Digital evidence has, by its very nature, always existed in digital form, whereas evidence presented in digital form may have originally existed in written or oral form.

* Dragi Rashkovski, PhD., Associate Professor, Ss. Cyril and Methodius University in Skopje, Iustinianus Primus Faculty of Law, e-mail: rashkovskid@gmail.com, https://orcid.org/0009-0001-0042-7763

** Veronika Rashkovska, Assistant Professor, Faculty of Legal Sciences, International Relations and Diplomacy – MIT University – Skopje, bul. Treta Makedonska brigade 66b, 1000 Skopje, Republic of North Macedonia, https://orcid.org/0009-0000-1343-9846

Keywords: digital evidence; evidence in digital form; metadata; digital forensics

I. Introduction

Legal proceedings—whether civil, criminal, administrative, or conducted within the internal procedures of legal entities—increasingly rely on digital records as the basis of their evidentiary process. Yet digital records, particularly in the era of artificial intelligence, may create distorted perceptions among participants in legal transactions or within decision-making bodies. In such cases, objective truth may be transformed into falsehood, and a participant lacking technical expertise may be unable to recognize or explain this distortion.

The general notion of a *digital record* refers to any entry created on one of the many available data storage media, and the prevailing perception is that such a record may serve as digital evidence "if necessary."

In the digital era, the saying *"paper endures everything"* may be reformulated as *"the memory device records everything."* This parallel is not coincidental, for just as not every sheet of paper qualifies as written evidence, not every digital record qualifies as digital evidence. In what follows, we will first draw a distinction between digital records and evidence in digital form and subsequently turn to the difference between evidence in digital form and digital evidence.

At first glance, this may appear to be a matter of "searching for different shades of the same color." However, the legal basis for distinguishing these concepts demonstrates that, at times, they are not merely different shades within a spectrum, but rather as distinct as black and white.

II. Digital Evidence – Evidence in Digital Form and the "Best Evidence Rule"

Evidence in digital form may originate in three different ways. First, it may have existed in written form and subsequently been digitized through scanning. Second, it may have existed in oral form—such as a directly heard voice or transmitted testimony—later preserved on a digital medium. Third, it may be created natively in digital form, which leads to the conclusion that, in the perceptual world, such evidence does not and has never existed in any form other than digital.

The mere transposition of a paper document into a digital record—whether in Word, PDF, or any other readable digital format—does not in itself transform that record into digital evidence. From a legal standpoint, such records will always retain the character of written evidence. The reasons for their digitization may vary—such as cost-effectiveness, procedural efficiency, or protection from damage—but whenever requested by any party in the proceedings, the submitting party is obliged to present the original document, which in this case is the written record.

Without exception, although jurisdictions may designate the rule under different names, its essence remains the same worldwide: upon request, the submitting party must provide the original evidence—whether written, oral, or digital. The consistent presence of this requirement across various legal instruments justifies treating the obligation to present the original as a universal principle, irrespective of where it is defined or the terminology employed. Common formulations of this rule include the "best evidence rule," the "requirement of the original," or similar expressions, yet its substantive meaning is always identical. For example:

In the OSCE manual Evidence and Objections: Domestic and International Standards (2016)[1], the rationale for requiring the original form and content of a digital document intended to serve as evidence in court is emphasized. The manual states:

[1] https://www.osce.org/files/f/documents/b/4/315111.pdf

"The Best Evidence Rule applies during trial when one party seeks to prove the contents of a document (written document, recording, or photograph). This rule requires the original to be presented, as it constitutes the best evidence. In cases where the original does not exist, the party submitting the document must provide an acceptable explanation for its absence. If the court accepts the explanation, the party may then use a copy to prove the contents of the document. This does not apply in cases involving questions of authenticity of the original or where it would be unfair to permit the use of a copy."

Similarly, with near-universal precision, the requirement to present the original document is codified in Rule 1002 of the United States Federal Rules of Evidence, titled *"Requirement of the Original."*[2] The rule provides:

"An original writing, recording, or photograph is required in order to prove its content, unless these rules or a federal statute provide otherwise."

The essence of this paper lies precisely in distinguishing ordinary records from those that constitute digital evidence.

A particular challenge in the application of the Best Evidence Rule arises in relation to text messages exchanged through various applications. Such records are increasingly presented as central evidence in both civil and criminal proceedings, and their content often constitutes one of the key elements in the evidentiary process. In these cases, the requirement to submit the original evidence assumes a different dimension, since the original itself is digital. This circumstance necessitates the fulfillment of additional prerequisites, which will be examined in the sections that follow.

In legal literature, an illustrative example is the U.S. case *Edwards v. The Younger American State Foundation*[3]. In its judgment, the court underscored the importance of presenting the original record for verifying authenticity. The ruling stated:

"With respect to electronic data, the Best Evidence Rule applies to computer printouts or other 'output' if it accurately reflects the information. To ensure accuracy, the court held that the electronic file in its native format, or a properly processed image including all metadata, must be presented."

The *Edwards* case demonstrates that, in the context of electronic messages, presenting the content alone is insufficient. Establishing who sent the message, when it was sent, and that no information has been altered is essential for proving authenticity under the Best Evidence Rule. The court held that screenshots of messages do not constitute sufficient evidence. Moreover, as already noted, each digital record format carries its own particularities, which must be preserved during both collection and presentation. For this reason, the most common formats are individually addressed in legal practice, specifying how they should be documented and presented, all while ensuring compliance with the Best Evidence Rule.

The discussion of the Best Evidence Rule, or its synonymous formulations, in relation to digital evidence is not coincidental. It represents the first threshold that a digital record must meet in order to be regarded as digital evidence. If the original itself exists as a digital record, then it may qualify as digital evidence and can subsequently be evaluated against the additional parameters and characteristics required for its admissibility in court.

If, under the Best Evidence Rule, a digital record originates in written or oral form, it does not qualify as digital evidence. Rather, it constitutes written evidence which, through the use

[2] https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_dec_1_2019_0.pdf
[3] https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00140/188037/129/

of information technology, has been transformed into a digital record. Its most accurate classification, therefore, is written evidence in digital form.

This distinction between categories is drawn not merely for semantic purposes, but in order to establish the credibility, authenticity, and integrity of evidence in judicial or administrative proceedings, a matter that will be further examined below.

III. The Difference Between Preserving Digital Evidence and Preserving Other Evidence in Digital Form

Digital evidence is highly sensitive to external influences. Although it may sound self-evident, even a single action—such as a mouse click—can fundamentally alter its content or render it unusable in judicial proceedings. By contrast, evidence in digital form that does not qualify as digital evidence is less susceptible to modification and can be more readily reproduced, thereby serving as a simpler means of preservation.

The preservation of digital evidence, once collected, requires adherence to a wide range of internationally recognized technical procedures and normative frameworks. These standards—largely harmonized across international organizations—are designed to safeguard the integrity, reliability, and admissibility of such evidence before judicial and quasi-judicial bodies.

The distinctiveness of digital evidence arises not only from its susceptibility to manipulation but also from its inherent form. As noted, digital evidence exists exclusively as a digital record, and preserving the original requires ensuring that it cannot be altered. Unlike other types of evidence that have been converted into digital form, the original of digital evidence cannot be reproduced once it is lost or compromised.

In contrast, evidence in digital form that originates from paper-based records can often be reproduced even if the physical original has been destroyed, provided it was issued by a competent public authority or a similar institution. Digital evidence, however—such as communications exchanged through electronic applications—exists solely in a single original instance and cannot be recreated once destroyed, particularly if the device containing it has already been seized.

For this reason, all digital forensics guidelines prescribe detailed procedures for the preservation, documentation, and chain of custody of digital evidence—standards that are not applied with the same rigor to other types of evidence in digital form. This particularity also stems from the fact that the proper preservation of digital evidence is essential for safeguarding its metadata. Without metadata, digital evidence becomes decontextualized, thereby losing both its authenticity and its probative value.

Accordingly, the preservation of digital evidence, as regulated by international guidelines and normative acts, will be examined through direct reference to several of these sources. Such instruments, developed at both European and global levels, do not operate in isolation but rather overlap and converge. This general harmonization fosters legal certainty for those responsible for preserving digital evidence and ensures predictability for those who encounter it in the evidentiary process.

The European Commission Anti-Fraud Office created the Guidelines on Digital Forensic Procedures on forensic investigation for OLAF staff[4] by taking into account both the internationally approved standards ISO/IEC Standard 27037 on "Guidelines for identification, collection, acquisition and preservation of digital evidence," adopted in October 2012 and the

[4] https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf

"Good practice guide for digital evidence" published by the UK Association of Chief Police Officers (ACPO) in March 2012

"In Guideline 27 of the same, it is stated that:"

"Guideline 27, concerning the preservation of electronic evidence, is applicable both to the storage and the archiving of electronic evidence that take place after completion of the proceedings. The electronic evidence should be stored and archived in the original form in which it was created, transmitted and received and in a manner which does not materially change the data. The electronic evidence should be available in a readable format during the entire duration of the proceedings. The integrity of electronic evidence should be maintained at all stages."

Consequently, the preservation of electronic evidence, once seized, must remain in its electronic form, exactly as it was collected. This requirement implies that the reverse process—printing electronic evidence into hard copy and storing it in that manner as a means of protection against alteration—is impermissible. By contrast, other forms of evidence in digital form, which do not qualify as digital evidence, follow an inverse logic. Such records originate in another medium and are subsequently converted into digital form primarily for ease of preservation and storage. Thus, these two categories of records differ fundamentally in the rationale underlying their digital preservation.

The preservation of digital evidence is inextricably linked to the chain of custody. Without strict adherence to the chain of custody, the mere physical safeguarding of evidence lacks legal effect. The chain of custody requires that every procedural step and every instance of contact with digital evidence be documented and carried out in a forensically sound manner. Although this principle applies universally to all categories of evidence, a breach in the case of digital evidence will, in most instances, result in its exclusion from judicial proceedings. By contrast, with other types of evidence in digital form, the chain of custody can more easily be reconstructed, thereby allowing procedural deficiencies to be remedied.

Inadequate preservation—whether resulting from external physical factors or from software-based interference—may appear insignificant to an untrained observer, but to a qualified forensic examiner it is tantamount to the destruction of the evidence itself. By way of analogy, mishandling digital evidence is comparable to storing chemical samples outdoors, exposed to drafts and smoke, thereby irreparably compromising their probative value.

In the aforementioned OLAF Guidelines, the imperative of proper preservation of digital evidence explicitly includes the requirement that original seized media be stored in a digital forensic laboratory. This requirement pertains specifically to the safeguarding of original media obtained by competent authorities. By contrast, other categories of evidence in digital form—unlike digital evidence—are typically preserved in ordinary document files or on conventional storage media once converted into digital format. From an economic perspective, the preservation of such evidence is considerably less costly and less complex. However, the distinctive characteristics of digital evidence—some of which have already been noted—necessitate its storage under far stricter conditions in order to guarantee its authenticity and evidentiary reliability. In this regard, the OLAF Guidelines describe the digital forensic laboratory as:

The OLAF forensic laboratory consists of physically isolated and secured offices within OLAF where forensic services are provided. These include dedicated server rooms, in which digital forensic evidence and working files are stored, as well as consultation spaces for investigators and operational analysts.

Among the various provisions concerning the preservation of digital evidence, OLAF places particular emphasis on the process of creating a digital forensic copy, which represents one

of the primary methods of safeguarding such evidence. Article 8.1 of the aforementioned OLAF legal instrument explicitly stipulates that:

Immediately after the return from the digital forensic operation, the DES shall create two back-up copies of the digital forensic image on tape, and place them in sealed envelopes with unique identification numbers. One of these is the in-house backup copy, which shall be stored in the OLAF Forensic Archives. The other is the off-site backup copy, which shall be stored in a protected area outside the OLAF premises. Both premises are protected by access control and CCTV cameras.

The aforementioned ISO/IEC 27037:2012, which addresses digital forensic processes and the application of relevant standards, explicitly identifies the preservation of digital evidence as a distinct phase within the digital forensic framework. Under this standard, preservation is a mandatory component, regulated by strict procedural requirements.

Preservation is the process of securely maintaining custody of property without altering or changing the content of data that resides on devices and removable media. The preservation process is critical for potential digital evidence to be useful in the investigation, and should be initiated and maintained throughout the digital evidence handling processes. Potential digital evidence must be preserved to maintain its integrity for its admissibility in a court of law.

IV. Differences in Presenting Digital Evidence and Evidence in Digital Form

Evidence in digital form that does not qualify as digital evidence can generally be presented by almost any participant in legal proceedings, regardless of the nature of the case. Such presentation does not require specialized IT skills; it usually involves nothing more than opening the digitized document—most often in PDF format or as an image—a routine task for the average user of information technology. The process then continues with reading the content of the digitized document, a task that the parties themselves may undertake if they consider themselves sufficiently capable and qualified.

In the case of digital evidence, the process of presentation is considerably more complex. Before reaching the presentation stage, digital evidence must undergo several preceding phases: the creation of a digital forensic copy, the extraction phase, the selection or examination phase, and the analysis phase, after which the evidence may finally be presented.

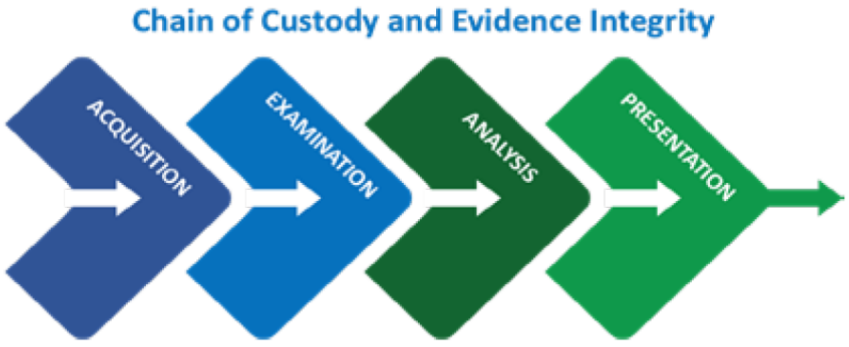

Figure 1. Digital Forensics Laboratory Analysis Model[5]

As highlighted in the Interpol *Global Guidelines for Digital Forensics Laboratory*, presentation is not merely the disclosure of analytical findings, but rather a constituent phase of

[5] https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics

the digital forensics process, which should be conducted within a digital forensic laboratory. This framing of presentation also determines the role of the "presenter." Each stage of the digital forensics process must be performed by a qualified digital forensic examiner. Such an examiner is a professional who possesses appropriate academic training and has been formally authorized by the state in which they operate. Accordingly, only a digital forensic examiner may serve as the presenter of digital evidence that has undergone the full forensic process up to the stage of presentation.

This does not imply that the analysis of evidence cannot be undertaken by laypersons or by the parties to the proceedings; however, the presentation of such evidence must be carried out by a digital forensic examiner. By way of analogy, medical findings are presented by a medical expert, not by a prosecutor or a defendant, although the latter are free to interpret them. Nevertheless, in the interest of professionalism and expertise—and above all, because of the technical challenges that may arise during presentation, as well as the need to address questions concerning the preceding forensic phases—this stage must be performed by a digital forensic examiner.

The presentation phase forms an integral part of the chain of custody of evidence, and if it is interrupted, all subsequent findings and procedures are rendered void. The aforementioned Interpol Global Guidelines emphasize the importance of the presentation of digital evidence and explain why this process must be carried out by digital forensic examiners. Section 5.4 specifically states that:

The Presentation phase requires putting together findings in a presentable and understandable way for stakeholders. When the analysis phase is completed, the Examiner needs to put the findings and results in a forensic report. The Examiner should illustrate and translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand. They may also be expected to interpret those facts, and to express an opinion on their meaning. In some cases when a large number of exhibits are analysed, it will be difficult for the examiner to present the outcome to the investigation team. It is recommended to adopt an analytic software, to facilitate matching digital evidence with other data from the investigations. This kind of tools can also be used to index and search all the exhibits, providing the investigation team with a global overview of the case

In Section 6 of the same Global Guidelines, the presentation of evidence by a digital forensic examiner is placed within the quality assurance framework, underscoring the examiner's role in the overall process. The examiner is not merely a general presenter in the proceedings; rather, their responsibility is to explain both the results obtained and the methodology by which those results were reached, as well as the procedures that were followed.

When presenting a forensic report in court, examiners may be required not only to explain the process of analysis. They may also be asked to clarify their professional competence, the equipment employed, the methodology selected, the procedures used in handling evidence, and other relevant aspects. It is essential that procedures for addressing these issues are properly established and implemented within the Digital Forensic Laboratory (DFL).

V. Legislation in the Republic of North Macedonia

The Republic of North Macedonia has enacted the *Law on Electronic Documents, Electronic Identification, and Trust Services*, which distinguishes between documents that are digital, documents that have been digitized, and documents that originally existed in digital form.

This law is further elaborated in the *Regulation on the Detailed Conditions for the Preparation of Documents for Electronic Storage and Qualified Electronic Storage and the Formats of Documents Suitable for Storage*, published in the *Official Gazette of the Republic of North Macedonia* No. 72 of 20 March 2020.

Based on the Regulation, Article 4 defines the process of digitizing documents that were not originally created in digital form as follows:

The person responsible for preparing documents for secure electronic storage shall digitize a document that was not originally created in electronic form, in a format suitable for electronic storage, whereby:

1) it must be ensured that the external form of the document prepared for secure electronic storage is identical to that of the original document;

2) if the document contains metadata, the metadata of the digitized document must be displayed, namely:

a) additional information relevant for establishing the authenticity of the document;

b) the date of digitization of the document;

c) information regarding the person who carried out the digitization procedure;

d) data on the format in which the document is stored;

e) technical data concerning the means used to digitize the document;

f) information regarding any damage to the content, form, or format of the document;

3) the stored document, together with the records and actions undertaken, must be kept separately from the original document.

Unlike Article 4, Article 5 of the Regulation defines the method of storing documents that were originally created in digital form, in a manner distinct from the previous category. What was emphasized earlier is now codified into a legal norm, which practically confirms the theoretical premise: that documents (evidence) originally created in electronic form require much more careful and professionally qualified handling in every respect. This necessity arises primarily from the specific nature of documents created natively in digital form—above all, from the need to preserve their metadata in order to demonstrate their immutability throughout the chain of custody. Accordingly, Article 5 of the Regulation provides:

When preparing an electronic document that was originally created in electronic form and is suitable for secure electronic storage, the person responsible for preparing such documents must:

1) verify the document and take measures to ensure its integrity during the secure electronic storage process, without conversion;

2) if the document contains metadata, ensure that the metadata of the electronic document is displayed, namely:

a) information on the format of the electronic document or its components;

b) additional information relevant for authentication;

c) the date of creation of the document; and

d) information demonstrating the validity of the certificate for the applied electronic signature, electronic seal, and time stamp at the time of their application to the electronic document;

3) store the digitized document, the records, and the actions undertaken separately from the original document.

Conclusion

Digital documents play an increasingly significant role in contemporary legal proceedings. In an era where much of human activity is mediated through bits and data, it is inevitable that these digital elements become integral to legal processes. The handling of digital documents therefore requires considerable caution, and even greater care must be exercised when dealing with documents originally created in digital form. Such caution applies not only to their preservation and storage, but equally to their presentation in judicial and administrative contexts.

What is important for the trial is the presentation of the relevant digital records found. The presentation thereof should be done by a person who was the bearer of the process of downloading, examination and analysis of digital evidence, or a person who has received relevant authorization from the competent institution. The presentation is made in order for the court, the prosecution and the defendants to be made available the material they have come across during the previous 3 phases. The presentation should show the whole chain of custody/evidence and prove that the procedure was done in a formally correct way, scientifically justified and scientifically proven. The presentation of the different types of found files should be done in such a way that the record should always lead to its origin, i.e. to the forensic record in the copy. If necessary, the presentation should prove that the record exists in the original device. Different types of files require a different procedure to prove their authenticity, whereas the content extraction must be done by referencing and suggesting to the native document.

Not every digital document constitutes evidence in digital form, and still less should it be regarded automatically as digital evidence.

E-sources:

1. https://www.osce.org/files/f/documents/b/4/315111.pdf
2. https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_dec_1_2019_0.pdf
3. https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00140/188037/129/
4. https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08 234355dbe544_en?filename=guidelines_en_bb84583638.pdf
5. https://www.iso.org/standard/44381.html
6. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigital Forensics