ITJ | The International Tax Journal

Digital evidence and its legitimacy in comparative systems

Fatiha Ressa [1]

[1] University of Tlemcen, Algeria. Email: fatiha.omar84@yahoo.com

Abstract---The digital revolution has brought significant changes to criminal law, including the emergence of cybercrimes and the need to prove them using digital evidence. This evidence is characterised by its scientific and technical nature, its ease of replication, and its resistance to destruction. However, the validity of digital evidence depends on how it is collected and how persuasive it is to the judge. The extent of the judge's discretionary authority varies according to the evidentiary system: the Latin system grants the judge considerable freedom, whereas the Anglo-Saxon system imposes strict criteria for the acceptance of digital evidence. The Algerian legislator has sought to adapt legislation to ensure the credibility and effectiveness of digital evidence in criminal proceedings.

Keywords---digital evidence, criminal proof, evidentiary system.

Introduction

In recent decades, the world has witnessed tremendous technical development, producing a new generation of crimes known as cybercrimes or computer crimes, which are perpetrated through digital means. This rapid advancement has created complex challenges for legal systems, which have had to reconsider traditional modes of evidence as they have proven inadequate for dealing with the nature of these newly emerging crimes, which take place in a virtual environment with precise technical and artistic characteristics.

Amid this transformation, digital evidence has emerged as one of the most significant new forms of evidence in criminal law due to its unique technical nature. This raises multiple questions concerning its definition, characteristics and forms, as well as the legality of obtaining and relying on it in court. Legislation and legal systems differ in their stance on the legality of digital evidence. Anglo-Saxon systems strictly apply the exclusionary rule in the event of procedural violations, whereas Latin systems

How to Cite:
Ressa, F. (2025). Digital evidence and its legitimacy in comparative systems. *The International Tax Journal*, *52*(6), 4455–4465. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/425

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025
ITJ is open access and licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
Submitted: 03 August 2025| Revised: 15 October 2025| Accepted: 05 December 2025

grant judges broader discretion to assess the validity of evidence based on the principle of personal conviction. In Algeria, legislators have attempted to introduce specific provisions to regulate digital evidence in line with developments in cybercrime.

Research problem:

This study is based on a central issue:

To what extent can digital evidence be considered legitimate and valid proof in criminal courts, given the differing legal systems and multiple technical and judicial standards associated with it?

Within this framework, the following questions can be raised:

What is meant by digital evidence? What are its most prominent technical and legal characteristics?

What are the most commonly used forms of digital evidence in criminal proceedings?

To what extent is digital evidence considered legitimate in Anglo-Saxon and Latin legal systems?

What is the stance of the Algerian legislator regarding digital evidence in criminal proceedings?

What criteria are used to assess digital evidence and its admissibility in court?

What scientific and legal means are available to evaluate the integrity and validity of digital evidence?

This topic will be addressed by examining the nature of digital evidence in the first section and its legality and validity in criminal cases in the second.

Section One: The Nature of Digital Evidence

Digital evidence is of great importance in the field of proof, as it forms the basis of judicial rulings, whether for proving or disproving crimes. To understand digital evidence, it is necessary to explore its concept through definitions and characteristics that distinguish it from other forms of evidence. This should also consider its novelty and relation to non-material technical means.

Although there are multiple definitional interpretations of digital evidence, most converge on a single point concerning the electronic environment of this newly established form of evidence.

Subsection One: Definition of Digital Evidence

First, we will discuss the general definition of 'evidence', then define 'digital', and finally move on to the technical definitions.

1. Evidence (in language):

Evidence is defined as guidance, direction and inference. Evidence can refer to proof, and its plural form is "proofs" or "indications". Evidence can also indicate guidance, and one person can direct another along a path. In Arabic, the term can be pronounced with both a stressed and unstressed "d" (د), and it can also refer to something that is led to one through indications[1].

In essence, evidence is proof, as in the expression: 'He established the evidence', meaning he clarified and proved it.

2. Digital (in language):

The term 'digital' refers to something related to evidence and derives from the root ' (number), whose plural is " (numbers). It represents the familiar numerical digits (1, 2, 3, etc.)[2].

Second: Digital Evidence in Technical Terms:

The definitions of digital evidence have varied according to the perspectives of scholars and researchers. Some have focused on the technical aspect in their definitions, while others have highlighted the legal nature of this evidence. Meanwhile, another group has emphasized its distinguishing features compared to traditional forms of evidence.

Digital, electronic or informational evidence is defined as evidence derived from electronic systems and devices. It primarily consists of signals or magnetic or electrical waves, which are converted into readable and analysable information using specific digital programmes and techniques. This information can be presented in various forms, such as text, images, audio recordings or graphics, to be used as evidence by law enforcement agencies[3].

It is also defined as 'any digital information or data stored in a computer or its accessories', such as hard disks or memory devices, or stored on any information network or the internet as a result of interaction with it. It also encompasses modern technical means and communication tools that store information in any form that can be converted into comprehensible text indicating a relationship between a crime and its perpetrator[4].

It can therefore be inferred that digital evidence consists of digital data within the digital realm of electronic devices which assist investigators and judges in proving crimes against perpetrators, provided the process of obtaining digital evidence complies with scientific principles and does not violate the law or individuals' rights[5].

The term 'digital evidence' does not imply that the evidence consists solely of numbers; rather, it denotes the manner in which digital data is recorded within the virtual environment, whether it is images, recordings or texts represented as digits (1 or 0). These digits are transformed upon display into forms such as images, documents, or recordings[6].

Subsection Two: Characteristics of Digital Evidence (Electronic Evidence)

Digital evidence is distinguished from other traditional forms of evidence by a set of characteristics that can be outlined as follows:

Branch One: Digital Evidence is Intangible

Digital evidence is considered non-material, meaning it cannot be perceived through the senses or touched like traditional physical evidence. It consists of signals and magnetic or electrical fields stored in electronic media that represent digital data which can be processed by computers or electronic devices. Presenting this data in a tangible form, such as printing or displaying it on a screen, does not make it the evidence itself. Rather, it is merely a process of transferring that information from digital form to a format that can substantiate a specific fact[7].

Branch Two: Digital evidence has a scientific and technical nature.

It belongs to the category of evidence derived from machines[8] and requires the intervention of specialised experts in information technology or digital forensics to examine and assess its admissibility, in a manner similar to that of other scientific evidence, such as genetic fingerprints.

As technology is a product of science, anything arising from technology can be used to demonstrate that electronic forensic evidence is scientific. This is because it is derived from the opinions and scientific conclusions formulated by experts in technical sciences based on their developments in terms of programs and technical devices.

Branch Three: Digital evidence is diverse and evolving.

The term 'digital evidence' or 'electronic evidence' encompasses all data and information of a digital nature that can be exchanged or processed electronically in various forms and types. This evidence can be derived from computers, other digital devices, the internet, or wired and wireless communication networks.

Consequently, the digital traces obtained from these media are rich and varied, containing information related to events that may constitute a crime. In some cases, this information may even be used to secure a conviction or acquittal[9].

This evidence can take many forms, including web pages, emails, text messages and digital videos, as well as files stored on personal computers and information pertaining to internet users, among other modern media.

This diversity illustrates the breadth of the digital forensic evidence base, which includes various types of electronic data and information that can be used to either acquit or convict a defendant[10].

Branch Four: The Difficulty of Removing or Destroying Digital Evidence

The difficulty of removing or destroying digital evidence stems from the nature of digital media itself and its technical characteristics. Even when an order is issued to remove and erase the evidence, traces

of it often remain visible in the device's memory. In fact, the attempt to erase the evidence constitutes independent evidence in itself, since operating systems and storage tools record deletion and modification activities, including the time and the person responsible. These records can be extracted and used as evidence against the person who performed the action.
Digital evidence that has been tampered with or altered can also be subjected to specialised programs and applications[11].

Branch Five: Copying Capability of Digital Evidence
This is one of the most notable technical features that distinguish digital evidence from traditional forms, as copies of digital forensic evidence can be extracted that are identical to the original and have the same scientific value. This feature ensures that the evidence is preserved against damage, distortion or alteration by creating exact duplicates.
Recognising the importance of this matter, the American legislator amended the Criminal Investigation Law on 28 November 2000 by adding Article 39, which explicitly authorises the seizure of digital evidence, including copies of materials stored in automated data processing systems, for presentation to the relevant judicial authorities[12].
Other characteristics include the fact that the perpetrator's attempt to erase evidence creates another piece of evidence, as a copy of this action is saved in the computer and can be recovered later and used as evidence for conviction.
Furthermore, digital or electronic evidence can be used to track and analyse information related to the perpetrator simultaneously. Digital evidence can record an individual's movements and document their habits, behaviours and personal details. Therefore, criminal investigations can more easily achieve their objectives compared to physical evidence[13].

Subsection Three: Forms of Digital or Electronic Evidence
In the field of criminal proof, digital evidence takes several forms that vary according to the technological media used. The most notable forms can be categorised into three main types:
Branch One: Digital Images
Digital images are among the most important forms of modern visual evidence, as they illustrate physical events related to the crime visually. These images can be presented as printed outputs or displayed directly on digital screens. Although digital images appear more advanced than traditional photographs, they are not necessarily better[14].

Branch Two: Audio Recordings
This category encompasses recordings captured and stored by digital devices, including voice conversations via the internet, phones or other modern devices[15].

Branch Three: Written Texts
This category includes all texts written using digital devices, such as emails and text messages, as well as data recorded on computers[16].

Section Two: Legitimacy and Admissibility of Digital Evidence in Criminal Proceedings
Digital evidence is considered a modern form of proof in criminal law, and its acceptance depends on the evidentiary system adopted by a given country. Some systems grant judges considerable freedom when forming their convictions, while others impose strict adherence to legal procedures when collecting and examining evidence. The admissibility of digital evidence depends on the integrity of the procedures followed when it is acquired, as this determines its reliability in court.

Subsection One: The Legitimacy of Digital Evidence in Comparative Legal Systems
The legitimacy of digital evidence is determined by its acceptance in criminal courts. Depending on the nature of the evidentiary system in place, countries vary in their approaches to accepting this type of evidence and incorporating it within the criminal evidentiary system.

Branch One: Legitimacy of Digital Evidence in Anglo-Saxon Systems

This system is referred to as the 'determined evidentiary system' or the 'legal evidence system', in which the legislator pre-defines the admissible evidence. Judges are not permitted to deviate from this and, when evidence meets the legislator's conditions, they are obliged to base their ruling on it, even if they are not personally convinced by it[17].

We will mention some countries that have adopted this system and their stance on digital evidence. The United Kingdom is one of the first countries to pay special attention to regulating matters related to computer usage; it issued the Computer Misuse Act on June 29, 1990, which is considered the first legislation in this area.

However, this law did not address the rules for admitting digital evidence in court, as this issue was already covered by the Police and Criminal Evidence Act 1984, which replaced the General Criminal Evidence Act 1965. Article 69 of this Act addresses the acceptance of digital forensic evidence derived from computers, stipulating that the evidence must be produced by functioning devices and that there should be no reasonable cause to doubt the credibility of the data produced[18].

In the United States, some state legislation has addressed the acceptance of digital evidence in criminal matters. In Alabama, for instance, the Computer Act of 1984 made data resulting from computer programs and data stored in computers admissible as evidential proof.

Similarly, the California Evidence Code of 1983 contains provisions recognising the legitimacy of relying on copies extracted from data stored on a computer and considers them to be the best available evidence with which to prove this data[19].

In systems adopting this approach, digital evidence cannot be acknowledged as having evidential value unless expressly stated in the law as admissible evidence. Conversely, the absence of such a provision in the law undermines its evidential value, even if the necessary conditions of certainty are met, thereby preventing judges from relying on it to support their verdicts.

According to the Anglo-Saxon system, the legitimacy of digital evidence depends on the legislator's assessment, rather than the judge's discretion. The judge's role is merely to verify that the conditions set by law have been met, and they have no role in assessing the evidence's persuasive value[20].

Branch Two: The Legitimacy of Digital Criminal Evidence in Latin Systems

This system is referred to as the 'persuasive evidence system', meaning it is a free evidentiary system where the legislator does not define the means or types of evidence, but rather allows the judge to base their ruling on personal conviction[21], without imposing a specific form of evidence. We will discuss legislation that has adopted this system.

In the French judicial system, digital criminal evidence raises no legal issues regarding its acceptance in court, since the French legislator adopts a free evidentiary system in criminal matters. This system grants judges the freedom to assess evidence and form their own convictions, whether the evidence is traditional or digital.

The French legislator's stance is illustrated by their acceptance of evidence obtained from electronic devices other than computers, such as surveillance cameras and radar devices. This was confirmed by the French Court of Cassation in its ruling dated 28/04/1987, which stated: 'Magnetic recording tapes that have evidential value can be validly presented before the criminal court.'

Consequently, audio and video recordings extracted from modern electronic devices can be used as evidence in a French criminal court, provided the legitimacy conditions are met, in a manner similar to that of traditional evidence[22].

Notably, both the French legislature and judiciary do not differentiate between evidence derived from modern electronic devices and traditional evidence when the conditions of legitimacy are met.

In contrast, the Dutch Computer Crime Act empowers investigative authorities to issue orders to information system operators to provide all necessary technical information for breaching and accessing the system, including disclosing passwords or codes required to run various programs or decode encrypted data.

However, the Dutch legislator has ensured compliance with the principle of legitimacy in evidence collection, similar to other comparative legislation. The principle of excluding illegal evidence has been

emphasised, and it has been stated that digital data recorded in police files cannot be used as criminal evidence if the procedures for obtaining it were illegal[23].

Branch Three: The stance of the Algerian legislator on digital criminal evidence

According to Article 212[24] of the Code of Criminal Procedure: 'Crimes may be proven by any means of proof, except in cases where the law specifies otherwise, and the judge may issue their ruling based on their personal conviction', it is evident that the Algerian legislator has adopted a free evidentiary system. The legislator permits the proof of crimes by all legitimate means of evidence and gives the criminal judge the freedom to assess evidence based on their personal conviction.

Thus, the Algerian legislator has, as a general rule, embraced the free evidentiary system, distancing itself from the notion of imposing any specific type of evidence or process that would restrict the evidentiary procedure. Consequently, criminal evidence is subject to the discretionary authority of the criminal judge when determining its value in proving the criminal fact, in accordance with the principle of personal conviction — one of the most important principles of criminal proof[25].

Therefore, digital evidence poses no legal issues within the Algerian judicial system, which adopts a free evidentiary system where criminal judges are governed by general rules regarding the acceptance of criminal evidence. This applies whether the evidence takes the form of official records or is the result of searches, communications interception or technical expertise related to the examination or analysis of digital forensic evidence extracted from computers and their accessories[26].

In order to address legislative shortcomings in this area, the Algerian legislature has introduced numerous laws and regulations to provide a legal framework for digital evidence, ensuring its legitimacy and admissibility in court and establishing a legal basis for it. One of the most significant pieces of legislation is Law No. 04-09, dated 14 August 2004, which contains specific provisions for preventing crimes relating to information and communication technologies and for counteracting them[27].

The law sets out procedures and technical methods to enable judicial authorities to investigate the digital environment, including monitoring electronic communications. It also establishes the National Authority for the Prevention of Crimes Related to Information and Communication Technologies and their Counteraction.

Subsection Two: The Admissibility of Digital Evidence

Simply obtaining and presenting digital evidence to the court is not enough for it to be accepted as proof of conviction or acquittal. The complex technical nature of this evidence makes it susceptible to tampering and manipulation.

Digital evidence can be altered without non-specialists being able to detect the change. It is also important to note that the margin of error in procedures for collecting and analysing digital evidence remains relatively high given the possibility of compromising data integrity during copying, transmission or technical examination[28]. Therefore, there is a likelihood of human or technical error.

Given the potential for human and technical error, questions arise regarding the credibility of digital evidence as a means of criminal proof. Does this doubt and the potential for error mean that this digital evidence should be excluded from criminal proceedings due to conflict with the presumption of proof? For this reason, we will examine two points: the assessment of digital evidence and methods of evaluating it to ensure its validity.

Branch One: Assessment of Digital Evidence

Legal systems belonging to the Latin family of evidence, including the Algerian legal system, are based on the freedom of criminal proof. These systems grant the judge broad authority in evaluating the evidence presented to them in terms of its persuasive strength. The judge may rely on what satisfies their conscience and reject anything that raises doubt or ambiguity. This principle is enshrined in Article 212 of the Code of Criminal Procedure, which affirms the judge's freedom to reach a decision in criminal matters.

However, the question that arises is whether, under the free evidentiary system, a criminal judge is able to accept or reject evidence based on a lack of conviction and doubts about its credibility[29].

It is challenging to broaden the topic of the criminal judge's authority to assess evidence. While this authority does include scientific evidence, a judge's legal knowledge may not fully grasp the technical or scientific truths concerning the authenticity of digital evidence. Moreover, this evidence has a persuasive value that can reach the level of certainty because it is based on precise scientific and technological principles. As is generally the case with scientific evidence, digital evidence meets the conditions of certainty in terms of its demonstration of reality. This makes it difficult to accept that a judge can exercise his authority to verify the facts established by that evidence.

Nevertheless, this does not contradict our previous statement that digital evidence raises concerns regarding its integrity against tampering and the correctness of the procedures followed to obtain it[30].

Thus, the integrity of digital evidence is questioned from two perspectives:

First: The possibility of tampering with or manipulating digital evidence:

Rapid technological development has enabled digital data to be modified or distorted in ways that are difficult for non-specialists to detect. The result is digital evidence that appears identical to the original at first glance, but is actually forged and altered. This places judges before technical evidence that may present a fabricated fact that is not true.

Secondly, there is a likelihood of technical errors in obtaining digital evidence:[31]

While the likelihood of technical errors in obtaining digital evidence is minimal, it nonetheless exists. Errors typically arise from two causes:

1. Errors in using the correct tool to obtain digital evidence:

This may be due to flaws in the software code or inaccurate technical specifications being relied upon during the retrieval process.

2. Errors in extracting the evidence itself:[32]

This occurs when tools or programs with a reliability level below the required threshold (less than 10%) are used, such as data compression or reduction tools. It can also occur when data is processed differently to the original evaluation method.

It can therefore be concluded that doubts about digital evidence focus not on its content as a means of proof, but on external factors that are independent of it and which may impact its credibility and admissibility in court.

Just as digital evidence is subject to specific rules governing how it is obtained, it is also subject to rules for determining its evidential value.

This is due to the technical nature of this evidence. Consequently, there are specialised technical means relevant to this evidence that allow for its examination and verification of its integrity[33]. These means also ensure the correctness of the procedures followed during its collection and extraction. We will address these means.

Branch Two: Methods for Assessing Digital Evidence

Methods for assessing digital evidence are essential for verifying its integrity and credibility before it is accepted in court. This is particularly important in ensuring that it has not been tampered with and that the procedures followed in obtaining it were correct.

First: Assessing Digital Evidence for Tampering

There are several ways to ensure that digital evidence is not tampered with[34]. Here are some of them:

- The Role of Computer Science:

Computer science plays an important role in providing technical information that helps us to understand the content and structure of digital evidence. This knowledge is used to detect the extent to which the evidence or the data that comprise it have been manipulated. One important method of verifying the credibility of digital evidence is digital analogy analysis, which involves comparing the digital evidence presented in court with the original file stored on the system or device on which it was created. This ensures that both versions match and that the extracted version has not been tampered with[35].

- Algorithms for verification:

Even when the original version of digital evidence is unavailable or has been tampered with, it is possible to verify its integrity through special mathematical operations known as algorithms.

- Neutral evidence:

There is a type of digital evidence known as neutral evidence which is not related to the crime, but which contributes to confirming the integrity of the digital evidence in question by ensuring that the information systems have not been modified or altered[36]. These methods allow one to ascertain the integrity of digital evidence and its alignment with reality.

Second: assessing digital evidence for the technical integrity of the procedures used to obtain it.

A series of technical procedures are usually carried out to obtain digital evidence. As previously mentioned, errors in these procedures could cast doubt on the integrity of the results. Therefore, the Daubert tests can be relied upon to ensure the procedures used to obtain digital evidence are correct, and that the evidence produced is credible enough to be accepted as proof.

We will briefly present the steps taken to verify the technical integrity of these procedures:

From this, one can assess the integrity of digital evidence. If the evidence meets the general conditions that establish trust, it is unreasonable for the judge to reconsider this evidence and subject it to further scrutiny. Like other forms of scientific evidence, digital evidence is conclusive regarding the matter in question.

The possibility of questioning the integrity of digital evidence due to its susceptibility to tampering, or potential errors affecting the procedures for obtaining it, are purely technical matters that a judge cannot decide conclusively without expert support.

Therefore, if the digital evidence meets the aforementioned conditions regarding its integrity and resistance to tampering and error, it cannot be rejected based on the discretionary authority of the judge outlined in Article 212 of the Code of Criminal Procedure. For the judge to exercise their authority to reject evidence based on doubt, factors must be present that call the evidence into question, which the judge cannot definitively ascertain when the scientific and technical integrity of the evidence is established[37].

Therefore, in this case, the judge's role is limited to examining the evidence's connection to the crime and its relevance to the facts of the case.

It should be noted that digital evidence may serve to prove both the crime and the perpetrator. It is clear from the above that digital evidence is suitable for proving crimes committed using digital devices (such as computers or phones), or crimes committed against the moral entity of the device or against the global information network[38].

Conclusion

The digital environment in which electronic evidence exists is inherently advanced, encompassing various types of digital data, collections of fields, and magnetic or electrical pulses. This evidence can be collected and analysed using specialised software and applications to present it in the form of images, audio or video recordings that can be used as evidence for conviction or acquittal. One of the key findings is that scientific and technological advancements have given rise to a new type of crime, for which non-traditional proof is required, referred to as digital evidence.

The digital world has influenced the nature of digital evidence, endowing it with the attributes of scientific and technical evidence and making it difficult to manipulate or dispose of. Indeed, an attempt to destroy it serves as further evidence of tampering. This feature enhances the value of digital evidence in criminal proceedings, meaning that preserving its integrity and ensuring the legitimacy of the procedures for its collection and custody is essential. Comparing different legal systems reveals clear differences in attitudes towards the legitimacy of digital evidence. In Anglo-Saxon systems, which operate under restrictive evidentiary rules, digital evidence cannot be recognised as having evidential

value unless it is explicitly included in the legal list of admissible evidence. Furthermore, acceptance of digital evidence hinges on strict adherence to legal procedures; any violation of these regulations results in the exclusion of such evidence. In contrast, Latin systems adopt a free evidentiary system and digital evidence does not pose any legal challenges regarding its acceptance in court. This system grants judges the freedom to assess evidence and draw conclusions, whether traditional or digital. Thus, judges have broader authority to evaluate the strength of digital evidence based on personal conviction, while considering fundamental guarantees of technical procedure integrity.

Regarding the admissibility of digital evidence, the mere existence of evidence proving a crime occurred and attributing it to a specific individual is insufficient for it to be relied upon in issuing a conviction. This evidence must possess legal value.
This value depends on two main elements: legitimacy, and certainty of correlation to the facts to be proven. This gives it strong admissibility in demonstrating the facts it contains. Any doubts about the credibility of the evidence can be overcome by testing and evaluating it to ensure the accuracy and reliability of the digital data.

There are several recommendations that should be noted, including the following:
1. Encourage the judiciary to accept digital evidence as a reliable and authentic form of evidence that should not be questioned or challenged, except in cases of illegitimacy.
2. Introduce modern methods for collecting digital evidence as legal practices within the framework of the Code of Criminal Procedure.
3. Raise the legal and technical awareness of judges and investigators regarding the characteristics of digital evidence, and how to handle it in order to avoid challenges and legal issues.
4. Engage with international experiences in digital legislation to adopt best practices that balance crime prevention with the protection of fundamental rights.

List of Sources and References:

Ahmed Abdellah Helali, 'The Admissibility of Computer Outputs in Criminal Cases: A Comparative Study', Proceedings of the Conference on Law, Computer and Internet, 3rd edition, Vol. 3, United Arab Emirates University, 2004.

Aida Belabed, 'Digital Evidence Between the Necessity of Criminal Proof and the Right to Information Privacy', Scientific Horizons, Vol. 11, No. 1, 2019.

Ali Hassan Mohamed Al-Tawalia, 'Criminal Search on Computer Systems and the Internet: A Comparative Study', 1st edition, Modern Book World, Jordan, 2004.

Ali Mahmoud Ali Hamuda, 'Evidence Obtained from Electronic Means in the Context of Criminal Proof Theory', Proceedings of the First Scientific Conference on the Legal and Security Aspects of Electronic Operations, organised by Dubai Police Academy, 26–28 April 2003, Dubai.

Baha Al-Mary, 'Social Media Crimes, Mobile Crimes, and the Admissibility of Electronic Evidence', Vol. 2, Cairo: Al-Ahram Publishing and Distribution, 2022.

Belhadi, H. (2019). 'The admissibility of digital evidence in criminal proof'. Journal of Legal and Political Research and Studies, 9(1).

Ben Firdia Mohamed, 'Digital Forensic Evidence and Its Admissibility in Criminal Courts: A Comparative Study', Academic Journal of Legal Research, Vol. 5, No. 1, 2014.

Ben Malik Ahmed and Khal Ibrahim, 'The Role of Digital Evidence in Criminal Proof', Journal of Humanities, University Centre Aï Kafi, Tindouf, Algeria, Vol. 5, No. 1.

Chaima Sayed Abdel Rahman Mohamed Al-Shuqairy, 'The Extent of the Admissibility of Digital Evidence in Proving Traditional Crimes: A Jurisprudential Study', Journal of Sharia and Law, No. 41, Faculty of Sharia and Law, Al-Azhar University, Cairo, April 2023.

Karrar Ghanem Bustan, 'The Scope of Electronic Evidence in Criminal Proof', Journal of Iraqi University, Vol. 73, No. 4, 2025.

Khatoui, M. and Akouch, H., 'The Privacy of Electronic Evidence', Journal of Legal and Political Thought, Vol. 7, No. 1, 2023.

Law No. 09-04 concerning Special Rules for Preventing and Combating Crimes Related to Information and Communication Technologies, Official Gazette No. 47, 6–8 August 2009.

Mamdouh Abdel Hamid Abdel Muttalib, Zubaida Muhammad Qasim and Abdullah Abdul Aziz, 'A Proposed Model for the Rules of Admitting Digital Evidence in Computer Crimes', Conference on Electronic Banking Between Sharia and Law, Vol. 5, Dubai Chamber of Commerce and Industry, 10–12 May 2003.

1- Ousama Hussein Mohi Eldin Abdel Aal, 'The Admissibility of Digital Evidence in Criminal Proof for Cyber Crimes: A Comparative Analytical Study', Journal of Legal and Economic Research, No. 76, June 2021, p. 632.

2- Ben Malik Ahmed and Khal Ibrahim, 'The Role of Digital Evidence in Criminal Proof', Journal of Humanities, University Centre Aï Kafi, Tindouf, Algeria, Vol. 5, No. 1, p. 107.

3- Aida Belabed, 'Digital Evidence Between the Necessity of Criminal Proof and the Right to Information Privacy', Scientific Horizons, Vol. 11, No. 1, 2019, p. 137.

4- Baha Al-Mary, 'Social Media Crimes, Mobile Crimes, and the Admissibility of Electronic Evidence', Vol. 2, Cairo: Al-Ahram Publishing and Distribution, 2022, p. 738.

5- Qusay Ali Abbas, 'The Admissibility of Electronic Evidence in Criminal Proof', Journal of the College of Law and Political Science, No. 26, Iraq, 2024, p. 123.

6- Chaima Sayed Abdel Rahman Mohamed Al-Shuqairy, 'The Extent of the Admissibility of Digital Evidence in Proving Traditional Crimes: A Jurisprudential Study', Journal of Sharia and Law, No. 41, Faculty of Sharia and Law, Al-Azhar University, Cairo, April 2023, p. 879.

7- Ali Mahmoud Ali Hamuda, 'Evidence Obtained from Electronic Means in the Context of Criminal Proof Theory', Proceedings of the First Scientific Conference on the Legal and Security Aspects of Electronic Operations, organised by Dubai Police Academy, 26–28 April 2003, Dubai, p. 22.

8- Chaima Sayed Abdel Rahman Mohamed Al-Shuqairy, 'Ibid', p. 880.

9- Khatoui, M. and Akouch, H., 'The Privacy of Electronic Evidence', Journal of Legal and Political Thought, Vol. 7, No. 1, 2023, p. 1065.

10- Naeem Saidani, 'Investigative Mechanisms for Cyber Crime in Algerian Law', Master's thesis, Faculty of Law, University of Batna, 2013, p. 124.

11- Ben Malik Ahmed and Khal Ibrahim, 'Ibid', p. 109.

12- Belhadi, H. (2019). 'The admissibility of digital evidence in criminal proof'. Journal of Legal and Political Research and Studies, 9(1), pp.20–21.

13- Karrar Ghanem Bustan, 'The Scope of Electronic Evidence in Criminal Proof', Journal of Iraqi University, Vol. 73, No. 4, 2025, p. 294.

14- Chaima Sayed Abdel Rahman Mohamed Al-Shuqairy, 'Ibid', p. 882.

15- Khatoui, M. and Akouch, H., 'Ibid.', p. 1067.

16- Tarek Mohamed Al-Jamli, 'Digital Evidence in the Field of Criminal Proof', Journal of Rights, Vol. 12, No. 1, Libya, n.d., p. 47.

17- Ben Firdia Mohamed, 'Digital Forensic Evidence and Its Admissibility in Criminal Courts: A Comparative Study', Academic Journal of Legal Research, Vol. 5, No. 1, 2014, p. 282.

18- Ahmed Abdellah Helali, 'The Admissibility of Computer Outputs in Criminal Cases: A Comparative Study', Proceedings of the Conference on Law, Computer and Internet, 3rd edition, Vol. 3, United Arab Emirates University, 2004, pp. 727–728.

19- Ali Hassan Mohamed Al-Tawalia, 'Criminal Search on Computer Systems and the Internet: A Comparative Study', 1st edition, Modern Book World, Jordan, 2004, p. 127.

20- Wahiba Lawarim, 'Digital Evidence in the Field of Criminal Proof According to Algerian Legislation', National Criminal Law Journal, Vol. 57, No. 2, Cairo, 2014, p. 85.

21- Ben Firdia Mohamed, Ibid., p. 282.

22- Ben Malik Ahmed and Khalid Ibrahim, Ibid., pp. 110–111.

23- Osama Abdullah Al-Qaid, Ibid, p. 95.

24- Osama Abdullah Al-Qaid, Ibid, p. 95.

25- Qadri, Susan and Abbar, Omar, 'Digital Evidence Between the Conviction of the Criminal Judge and the Oversight of the Supreme Court', Journal of Algerian and Comparative Public Law, Vol. 10, No. 1, Algeria, 2024, p. 233.

26- Ben Malik Ahmed and Khal Ibrahim, Ibid., pp. 111–112.

27- Law No. 09-04 concerning Special Rules for Preventing and Combating Crimes Related to Information and Communication Technologies, Official Gazette No. 47, 6–8 August 2009.

28- Wahiba Lawarim, Ibid., pp. 101–102.

29- Maysoun Khalaf Hamad Al-Hamdani, 'The Legitimacy of Electronic Evidence in Criminal Proof', Journal of Research and Studies in Arabic, Vol. No., No. 65, Egypt, 2016, p. 242.

30- Wahiba Lawarim, Ibid, p. 102.

31- Wahiba Lawarim, Ibid, p. 102.

32- Wahiba Lawarim, Ibid, p. 103.

33- Wahiba Lawarim, Ibid, p. 104.

[34]- Maysoun Khalaf Hamad Al-Hamdani, Ibid, p. 243.
[35]- Mamdouh Abdel Hamid Abdel Muttalib, Zubaida Muhammad Qasim and Abdullah Abdul Aziz, 'A Proposed Model for the Rules of Admitting Digital Evidence in Computer Crimes', Conference on Electronic Banking Between Sharia and Law, Vol. 5, Dubai Chamber of Commerce and Industry, 10–12 May 2003, pp. 2241–2247.
[36]- Mamdouh Abdel Hamid Abdel Muttalib, Zubaida Muhammad Qasim and Abdullah Abdul Aziz, Ibid, pp. 2241–2247.
[37]- Wahiba Lawarim, Ibid, p. 106.
[38]- Previous reference, p. 107.