ASJP Algerian Scientific Journal Platform

Afak For Sciences Journal
Issn: 2507-7228 – Eissn: 2602-5345
https://www.asjp.cerist.dz/en/PresentationRevue/351

Volume: 09/ N°: 04 (2024), P 97-113

Digital Evidence and Proving Cybercrime "Between High Technology and Law Constraints"

*Rihab Yousfi**

Mohamed El Bachir El Ibrahimi University,Bordj Bou Arreridj, Algeria
Cyber justice Laboratory,

rihab.yousfi@univ-bba.dz

Wahiba Louarem

Mohamed El Bachir El Ibrahimi University,Bordj Bou Arreridj, Algeria
Cyber justice Laboratory,

wahiba.laouarem@univ-bba.dz

Abstract ;

The advent of the Internet and the development of information technology have led to new forms of criminality. Technology is now used both as a means of committing crimes and as an object of crimes. Consequently, law enforcement agencies must adapt to these new forms of criminal evidence. It is essential to develop evidence-gathering methods that align with advancements in cybercrime. This evolution has given rise to a new form of evidence derived from the digital environment. Such evidence presents unique challenges due to its privacy concerns and continuous development. The distinct nature of the digital environment necessitates criminal legal provisions that are compatible with it. Therefore, a reconsideration of the procedural aspects of the adopted criminal policy is required.

Article info

Received
August 19 ;2024
Accepted
September 21 ;2024

Keyword:

- ✓ *Digital Evidence*
- ✓ *Digital Binary*
- ✓ *Data*
- ✓ *Digital Environment*
- ✓ *cyber crime*

* *Corresponding author*

1. *Introduction*

The information and communication revolution has introduced new means that have significantly improved life. The development and fusion of information and communication technology were central to this revolution. This fusion has empowered individuals and countries, eliminated barriers and distances, and provided greater freedom for individuals to pursue their interests. It has also facilitated and accelerated the transfer and storage of information. However, it has also opened the door to new forms of crime, known as information crimes, cybercrimes, or high-tech crimes.

These new crimes pose clear challenges to established laws. The nature of crime has shifted from its traditional physical form to a moral one. The perpetrators have also changed, with the emergence of professionals and specialists in informatics. These individuals target automated data processing systems or use technology and information systems to commit or facilitate traditional crimes. Consequently, we are now dealing with a different type of crime pattern. These crimes rely on intelligence and high technology, which are unfamiliar in traditional crime patterns. They are based on the use of advanced technologies and electronic media.

Proving this type of crime has become a complex issue requiring in-depth study. Traditional procedural means are no longer sufficient to prove these new crimes. It is necessary to search for strong evidence appropriate to the nature of these crimes. This evidence must be sufficient to decode codes and translate pulses and vibrations into words and tangible data. Such data can serve as evidence for these offenses. Digital evidence, or technical evidence extracted from the digital environment, is the most important means of proving these crimes. Digital evidence is essential for proving cybercrime.

However, digital evidence faces many obstacles. The most significant challenge is that perpetrators are experienced professionals who rely on advanced technology and strive to conceal their identities. Additionally, law enforcement agencies sometimes lack the necessary expertise, which can lead to difficulties in extracting, destroying, or erasing evidence. The situation becomes more complicated when dealing with information and data stored abroad. It is difficult to search for and seize evidence located in a foreign country, making the search for digital evidence extremely challenging.

Due to the specific nature of digital evidence, traditional procedures for collecting and extracting evidence are no longer sufficient without technological support. This prompted the Algerian legislator to regulate the procedural aspects of investigating cybercrime. Under Law 09-04 of August 5, 2009, special rules were established for the prevention and control of crimes related to information and communication technologies. This law regulates inspection in the digital environment, electronic surveillance, and the preservation of information data.

This leads us to question the adequacy of the rules established in the law to regulate

digital evidence. Due to its specificity and the obstacles facing its extraction, we must consider the extent of its authenticity in proving cybercrime. Additionally, we need to examine how this type of scientific and technical evidence is subject to the discretionary authority of the judge. To address these questions and explore the topic further, we have divided this study into two sections.

- **First Section:** The role of digital evidence in proving cybercrime.
- **Second Section:** Obstacles facing the extraction of digital evidence.

In addressing the topic of this study, we followed a three-dimensional approach: descriptive, analytical and deductive, and comparative.

First Section: The Role of Digital Evidence in Proving Cybercrime

The rules of evidence are based on establishing proof of the fact on which they are founded. Criminal evidence is the driving force behind the rules of criminal evidence. With the emergence of cybercrime, digital evidence has become the most important form of proof. It includes all digital data that can confirm the commission of the crime or establish a relationship between the crime and the accused[1].

Digital evidence is one of the most significant developments in modern legal systems. It aligns with the scientific, technological, and technical revolution of the current era. This evolution in criminal thought has emerged alongside a new type of crime: cybercrime or digital crime[2].

In this section, we address the concept of digital evidence by clarifying its definition and identifying its types. We also examine the characteristics of digital evidence and its areas of use in the first requirement. Subsequently, we explain how to extract digital evidence by presenting the procedures and conditions for its extraction in the second requirement.

First Requirement: The Definition of Digital Evidence

Evidence is the means of proof in general. It encompasses the rules related to the search for evidence, its establishment before the judiciary, and its evaluation by the judiciary to reach a verdict on the fact being proven[3]. Traditional evidence is limited in proving electronic crimes, whether it is a tool in the commission of the crime or helps to hide its effects. This limitation hinders the acquisition of evidence. Consequently, traditional evidence procedures cannot be applied to information characterized by a moral nature. The evidence obtained is private and dominated by scientific and technical aspects, increasing the difficulty of access and proof[4]. This necessitates shedding light on digital evidence by addressing its definition in the first part and explaining its nature in the second part.

Firstly: Definition of Digital Evidence

Evidence is defined as the tool that the judge uses to reach the truth. It is the fact from which the judge draws evidence to form his conviction in the judgment he reaches. However, digital evidence has received several definitions. The definitions given to digital evidence are

numerous and varied. Below, we will present the most important definitions of digital evidence in jurisprudence and law, as well as its definition by some international organizations.

Some jurisprudence defines digital evidence as "information stored, received, or transmitted in digital form by an electronic device that can be used in court to help prove the attribution of a crime to the perpetrator.[5]"

Computer evidence is also defined as "a statement or expression produced or transmitted accurately from a computer, whether it is a sound recording, a layout, or various printouts.[6]"

Some define digital evidence as information accepted by reason and logic and approved by science. This information is obtained through

legal and scientific procedures by translating computational data stored in information systems, devices, accessories, and communication networks. It can be used at any stage of investigation or trial to prove the truth of an act, object, or person related to a crime, perpetrator, or victim[7].

The Scientific Working Group on Digital Evidence defines digital evidence as "information of evidentiary value stored or transmitted in binary form." The US report to the INTERPOL Scientific Symposium on Digital Evidence defines it as "data that can be created, communicated, and stored digitally and enables a computer to perform a task.[8]"

Some definitions have added the description of virtual evidence to computer-assisted evidence. This suggests that the information exists in multiple domains and appears in different forms, whether homogeneous or electromagnetic. It can be collected and analyzed using advanced technologies and applications. The evidence appears as digital outputs or displays from automated processing systems. These can be used to prove or disprove the crime or provide a case report.

According to the U.S. Department of Justice, technical evidence can be divided into three main groups:

1. Records stored in a computer, including automated word processing programs and archived documents such as emails.

2. Records created by computer programs, not by humans, such as log files.

3. Records created by computers, including hardware transactions such as ATMs, records stored in electronic processing systems, and spreadsheets such as Excel[9].

The Egyptian legislator defined digital evidence in Law No. 175 of 2018 on combating information technology crimes as "any electronic information that has the power or evidential value stored, transferred, extracted, or taken from computers, information networks, and the like, and can be collected and analyzed using special electronic devices, programs, or applications[10].

Therefore, according to this definition, digital evidence can be extracted from personal computers, smartphones, and

cloud storage sites. This data may include audio and video files, electronic messages, and Internet browsing records. This evidence is essential in investigations, especially those related to cybercrime.

The International Organization for Digital Evidence (IOCE), in cooperation with the Scientific Working Group on Digital Evidence (SWGDE), issued a document on standards for the recovery, preservation, and examination of digital evidence. It defines digital evidence as "information of potential value stored or transmitted in digital form.

The same document defines digital evidence as "the physical elements and data components associated with these elements at the time of acquisition or seizure of the evidence[11]."

With reference to Algerian law, particularly Law 04/09, which includes special rules for preventing and combating crimes related to information and communication technologies, Article 02 introduces concepts such as information system, information data, service providers, electronic communications, and other related concepts. However, it does not address the concept of digital evidence or provide its definition.

Secondly: Types of Digital Evidence

The types of digital evidence in terms of proof can be divided into two categories. The first category is evidence prepared to be a means of proof. The second category is evidence not prepared as a means of proof. Digital evidence takes several forms, including electronic documents and digital images. Therefore, digital evidence is not limited to one form. Below, we review the types of digital evidence:

a. Electronic Documents

Electronic documents are texts written by computer, including email messages containing information. The UNCITRAL law defines them as "any electronic means used in transactions that can be invoked or resorted to for evidentiary purposes.[12]"

In many countries, electronic certificates are now introduced into computers. An electronic certificate is a document where the witness is not physically present but provides testimony through electronic means. This method is valued for its speed of completion, preservation, and retrieval. The certificate can be printed on paper, saved inside a computer, or stored on disks or other media. It can also be sent by email.

This method is often used in international trials where witnesses are not in the country where the trial is taking place. Witnesses testify via chat using special programs supported by writing and images. The testimony is sent to the court for review using a webcam, allowing the witness to be heard in audio and video. Questions from the court or other parties are written and sent via computer. This method was used in the International Criminal Court during the trial of former President Slobodan Milosevic and his associate for war crimes committed in Kosovo.

The Statute of the International Criminal Court recognizes the possibility of providing testimony by electronic means under Rule 87. The video conference

method is one of the methods used in remote criminal investigation and trial. It is a modern means of multi-party audio-visual communication. This method requires preparing the various locations where the parties participate from a technical standpoint and providing a good communications network to ensure clear and continuous image and sound. Video conferencing may include two or several locations within the same state or between different countries. It is sometimes used to hear witnesses to protect them from mafia retaliation if they attend in person. It is also used to try defendants who are inside a penal institution before a court located hundreds of miles away, without compromising the rights of the defense.

This method was used in the United States, where nearly sixty people were heard at their residence in Italy regarding the incident of cutting the cable car wires at a winter sports center in Italy caused by a US military aircraft. It has also been used in many countries, including Italy, Canada, Australia, and New Zealand. In Algeria, this technique has been adopted for trials since 2015 under Law 03/15 dated February 1, 2015, on the modernization of justice. Initially, this procedure was applied conservatively until 2020, when Law 04/20 was issued to amend the Code of Criminal Procedure. With this amendment, video conferencing was generalized remotely under Book II bis, entitled "Use of Audio and Visual Means of Communication During the Trial," in Articles 441 bis to 441 bis 11[13]. Among the technical conditions for applying the remote video trial technique is maintaining the confidentiality and integrity of the communication. It cannot be conducted through unprotected networks or social media sites. Additionally, there is an obligation to record all statements on electronic support and attach them to the proceedings file.

b. Digital Images

The digital image represents an alternative technology to traditional photographs. Many countries use electronic means to seize this type of evidence by installing digital video cameras in selected locations for surveillance. This serves as both a tool for crime prevention and for seizing legitimate evidence. The use of such surveillance must respect the individual's right to privacy and be conducted by competent authorities within the limits permitted by law.

In this regard, the American judiciary has ruled that it is illegal to take pictures of a person in a private place if they have a right to privacy. The French legislator regulated electronic surveillance through video cameras in public places under the law of January 21, 1995, specifically Article 10. However, the French judiciary differentiates between images taken in public and private places[14].

Thirdly: The Legal Nature of Digital Evidence

Digital evidence is one of the most important types of evidence used in modern criminal investigations. It provides strong proof to either confirm or deny the commission of a crime. However, the nature of this evidence, whether physical or moral, needs to be clarified.

Digital evidence can take the form of paper outputs that can be physically touched. It may also exist as supports, such as magnetic tapes, magnetic disks, or paperless electronic evidence displayed on computer screens[15].

To determine the legal nature of digital evidence, it is necessary to first identify its characteristics and then determine its status among other types of evidence.

a. Characteristics of Digital Evidence

The environment in which electronic evidence exists is diverse and sophisticated. It contains multiple types of electronic data that can be used as evidence of guilt or innocence. This environment, known as virtual space, is a moral medium. This characteristic distinguishes digital evidence from traditional evidence.

1. **Digital Evidence is Scientific and Technical in Nature**

Digital evidence requires a technical environment for its formation and can only be detected using scientific methods. Scientific evidence must adhere to the rule that it responds to the whole truth, following the principle in comparative justice that "the law seeks justice, but science seeks truth[16]." This principle applies equally to digital evidence.

Digital evidence can only be detected using scientific methods. It must be preserved based on scientific principles. Therefore, it is necessary to modernize the methods of writing records to ensure they are compatible with the phenomenon of scientific evidence[17].

If we conclude that digital evidence is scientific evidence, it proves that technology is its most important feature. This is due to its scientific advantage. Digital evidence results from digital pulses and does not exist outside its digital environment. It is reproducible, allowing for the extraction of copies of digital forensic evidence that are identical to the original and have the same value. This characteristic is not found in traditional evidence. Technology is an effective tool for preserving evidence against loss, damage, change, and distortion.

Digital evidence is not visual evidence that can be understood only by reading. It is intangible electronic data with characteristics that distinguish it from physical evidence taken from the crime scene[18].

Dealing with digital evidence differs from handling physical evidence. Digital evidence is managed by specialized technicians because it is not tangible. It consists of digital pulses and magnetic fields, whose value lies in the ability to interact with solid pieces. Translating digital evidence into a tangible physical form does not convert it into physical evidence. Instead, it involves transferring information from its digital nature to a physical form that can be inferred.

2. **The High Storage Capacity of Digital Evidence**

A small disk can store a small library, and a digital video camera can store hundreds of pictures. This high storage capacity undoubtedly distinguishes digital evidence from other types of evidence[19].

3. **Difficulty in Disposing of Digital Evidence**

Traditional evidence, such as papers and tapes, can be easily disposed of by burning or shredding. Similarly, testimony, over time, is subject to forgetting, making its reliability questionable. It is essential to assess the witness's ability to recall events accurately[20]. Fingerprints can also be erased.However, digital evidence is different. Even after deletion, it can often be recovered and repaired. Numerous computer programs are designed to restore erased data.

Many computer programs, such as Photosetm, Foremost, and Recover Peg, are designed to recover erased data[21]. Electronic evidence can also be reproduced through computer disks.

The Iran-Contra case[22] highlighted the robustness of electronic evidence. In this case, the administration recovered data by restoring the email backup system, revealing the involvement of some officials in the Office of the US President[23].

One of the most important characteristics that digital evidence shares with genetic or DNA evidence is its ability to record any attempt to hide it. Any such attempt is documented within the computer and can be extracted as evidence of guilt. This applies whether the removal is done by the delete command or by reformatting the hard drive using the format command. This information can include photos, drawings, writings, or other data[24].

Digital evidence can simultaneously monitor and analyze information about the perpetrator. It can record an individual's movements, behaviors, and certain personal information[25].

4. **Digital evidence is diverse and evolving**

It does not have a single character and continues to develop alongside electronic advancements. This evolution can complicate access to digital evidence. Major international internet sites often surround stored data with technical protections. These measures prevent illegal access, destruction, alteration, or copying of the data.

5. **Digital evidence is binary in nature.**

It consists of an unlimited number of binary numbers, unified as ones and zeros (0-1). Despite this unity, these binary numbers are characterized by their dissimilarity. Everything in the digital world consists of zeros and ones, which are continuous rhythmic pulses deriving their vitality and interaction from energy. The amount of binary data (0-1) varies from one file to another[26].

Data inside a computer, whether in the form of texts, letters, numbers, symbols, sounds, or images, turns into a digital nature. Modern information technology works with the numbering technique, converting any information document consisting of text or images into a binary system. This system represents numbers using the two digits (zero) and (one). Consequently, some programs may prepare information evidence, such as hacking programs[27].

The traces left by a user of an information system are in digital form. These traces include messages sent and received by the user, as well as all communications made from the computer and through the communication network[28].

6. **The global breadth of the digital evidence landscape is vast.**

Evidence users can exchange digital knowledge at high speed across different regions of the world. This capability contributes to the relatively quick identification of perpetrators or their actions. Ultra-fast digital evidence travels from one place to another through communication networks that transcend the boundaries of time and space.

b. The Status of Digital Evidence Among Other Evidence:

Digital evidence is a distinct type of evidence due to its special technical nature. Its content involves scientific issues and complex technical processes, such as manipulating intangible electronic pulses and vibrations. These processes are invisible and can only be understood by specialized experts. Digital evidence relies on the digital or technical world, represented by data and information stored in computers or other electronic means. Therefore, it is considered distinct from traditional evidence. Digital evidence holds great importance in criminal investigations, especially in proving information crimes, due to its modernity and development.

Second Requirement: Obtaining Digital Evidence to Prove Cybercrime

The technical development of automated data processing systems, along with the specificity and distinction of technical evidence from traditional evidence, has altered prevailing concepts regarding the procedures for obtaining digital evidence. This necessitates a re-evaluation of the effectiveness of some traditional procedures and their compatibility with these changes. For instance, inspection and seizure procedures outlined in the Code of Criminal Procedure must be reconsidered in light of advancements in science and technology, particularly in the field of the information revolution[29]. The development of evidence and its methods is crucial to addressing this new type of crime. In this regard, we will explain the procedures for obtaining digital evidence in the first part and the conditions for its acceptance in the second part.

Firstly: Procedures for Obtaining Electronic Evidence

Dealing with a crime scene, whether regular or electronic, requires specific procedures to protect the evidence and highlight its evidentiary value. These procedures differ between physical and electronic crime scenes. Applications, programs, and digital data are essential elements that law enforcement agencies and forensic experts must collect and extract. Traditionally, investigation authorities rely on methods designed for physical crime scenes. However, the electronic environment presents different challenges, making it difficult for

investigation authorities to adopt the same methods.

Since the September 11, 2001 attacks in the United States, the relationship between terrorism, organized crime, and the use of the Internet has led to the enactment of new procedures. These procedures aim to increase the effectiveness of criminal justice in detecting and prosecuting crimes committed via the Internet[30].

The search for more effective criminal justice began with the introduction of new investigative procedures. The Budapest Convention, held on November 23, 2001, introduced these procedures in Part II under the title "Procedural Law Articles 16 et seq." These procedures were adopted by the laws of several countries. Algeria, like these countries, defined these procedures in Law 09-04, Chapter III, under the title of procedural rules. These rules include the inspection of information systems and the seizure of information data. The procedures can be summarized as follows:

1. **Order to Preserve Stored Data:** This procedure enables the investigating authority to issue an order to the service provider to preserve stored electronic data pending further investigation procedures.

2. **Order to Provide Stored Data:** This procedure enables the competent authorities to investigate the extent to which service providers are obligated to provide the data in their possession. This includes all traffic-related data, which is mostly in the possession of the service provider, and data related to content transmitted by electronic means.

Secondly: Conditions for Acceptance of Digital Evidence

Digital evidence holds strong authority in legal proceedings. However, it is not immune to doubts regarding its integrity, such as potential tampering or alteration. There is also a margin of error in obtaining digital evidence, which may arise from the machine used or the extraction process itself[31].

Electronic evidence is subject to the same rules as other types of evidence. This includes the judge's authority to accept and evaluate electronic evidence[32]. For digital evidence to be accepted and considered by a criminal judge, two conditions must be met: the certainty of the digital evidence and the obligation to discuss it.

a- Certainty of Digital Evidence:

The judge reaches certainty regarding the evidence presented by examining it. The British Police and Evidence Act of 1984 requires that digital evidence be accurate and properly generated by the computer. Some American laws stipulate that copies extracted from computer data are considered among the best evidence available for proof. Thus, the principle of certainty is realized for this evidence.

Given the technical nature of digital evidence, it must be examined according to specific rules established by specialists. This involves using technical means to evaluate the evidence, ensuring it has not been tampered with through computer

science. Technical information helps understand the content of the digital evidence, analyze it, and confirm its integrity. This can be achieved by using neutral digital evidence unrelated to the crime, algorithmic calculations, and technical expertise[33]. Additionally, the digital evidence must be evaluated in terms of its technical value.

b- The Digital Evidence Must Be Discussed:

The second condition for the acceptance of digital evidence in criminal proceedings is that it must be discussed in a public session. This ensures the rights of the defense and guarantees a fair trial in accordance with the principle of publicity and confrontation. For digital evidence to be adopted, it must be presented for discussion in a public session, allowing each party to prepare their defense.

Another crucial aspect is the authenticity of digital evidence. Digital evidence, by its nature, exists in a digital environment and is recorded on electronic means that can only be read or extracted using electronic devices. This raises questions about the authenticity of digital evidence. Comparative legislation has adopted the presumption of digital evidence. The American Evidence Act, in Article 1001/3, stipulates that if data is stored in a computer or similar machine, any printed output or output readable by the naked eye that accurately reflects the data is considered original data. The American Replica Act recognizes the probative value of copies, suggesting that the authenticity of digital evidence should be acknowledged, as it remains available wherever it is called upon[34].

From the above, it appears that the judge's role in examining this type of evidence is limited. This limitation arises from the judge's lack of information literacy and his reliance on the opinions of specialized experts, rather than forming his own judgment.

Second Section: Obstacles Facing the Recovery of Digital Evidence

Digital evidence exists in a digital environment, and its creation or tampering can occur in a fraction of a second before justice can intervene. The seizure process is often carried out by law enforcement agencies that may lack sufficient technical knowledge in cybercrime. In contrast, the seizure or processing of evidence is typically performed by technical or specialized experts. This disparity raises the issue of the difficulty in extracting digital evidence, posing a significant challenge for security personnel[35].

The extraction of digital evidence faces numerous obstacles that hinder its collection and analysis. These obstacles may relate to the nature of cybercrime and its privacy concerns, or to the digital evidence itself within its digital environment. We will present these challenges through the following two requirements:

First Requirement: Difficulties Related to the Nature of Cybercrime

Due to the special nature of information crimes, proving them is surrounded by many difficulties in extracting digital

evidence. The most significant challenge is detecting these crimes, as they do not leave external traces, involve no violence, and have no physical evidence. Traditional examination methods are often unable to detect their effects. Additionally, victims may be reluctant to assist competent authorities in proving and revealing the crime, fearing harmful publicity and loss of shareholder confidence. This is particularly true for banks, financial institutions, or large industrial projects that prioritize maintaining customer trust and reputation over uncovering the crime.

Thus, the special nature of cybercrime is a major obstacle to extracting digital evidence. This is due to the large volume of information and the nature of mobile devices, which we will address in the next two parts.

Firstly: The Sheer Volume of Information

The enormous amount of information and data circulating in information systems poses significant challenges in collecting technical evidence. Printing all the data stored on the magnetic supports of an average computer center would require hundreds of thousands of pages, which do not necessarily prove anything. Faced with this difficulty, an untrained investigator may resort to one of two methods: either reserving data beyond human capacity to review or overlooking this data altogether in the hope of obtaining a confession from the accused[36].

Regardless of all technical matters, searching a computer is theoretically similar to searching paper files. However, the capacity of a filing cabinet is limited, while the capacity of computers continues to increase. For example, a standard 40 MB hard disk drive contains approximately 20,000 pages of information. Computer storage devices, such as disks, tapes, and laser disks, can generally store the equivalent of thousands of pages of information and data[37].

The solution is to use technical expertise to determine what must be viewed and seized. Alternatively, methods available in automated data processing systems can be used for structured or systematic auditing and examination. These include selection and review systems and methods, as well as examination methods specifically focused on the case or incident in question.

Secondly: Difficulties Related to the Nature of the Devices

Mobile devices include laptops, tablet computers, smartphones, GPS units, and other modern devices. A significant amount of information can be extracted from these portable digital devices. The difficulties in extracting digital evidence from these devices are as follows:

1. **Losing the Power Source of the Mobile Device:** One of the most significant difficulties facing digital forensic experts is the nature of the unsustainable memory in which data is stored on mobile devices. It is crucial to maintain the power source of the mobile device to prevent the loss of digital evidence when the power is lost.

2. **The Use of Data Hiding and Destruction Programs:** The use of data hiding and destruction programs, also known as hiding digital evidence, is a major challenge in extracting digital evidence. Hackers use anti-examination tools in forensic examination programs to conceal important digital evidence.

Digital evidence concealment techniques involve hiding the evidence used by the cybercriminal to commit the crime, either by encrypting stored data, making it unrecoverable, or by hiding files.

3. **Power and Data Connectors:** The issue of data connectors for mobile devices presents another challenge. Many devices, such as GPS units, smartphones, and tablets, use a variety of charging connectors. These cables are used for connecting, charging, and extracting information from the devices.

4. **Constant Updating of Operating Systems:** The rapid development and constant updating of operating systems present a significant challenge for technical experts. This challenge affects the methodology used in collecting technical evidence. Companies continuously produce new versions of mobile operating systems, requiring experts to modify their examination methodologies to keep pace with these constant updates[38].

5.

6. **Connection of Mobile Devices to Cloud Services:** Another issue in extracting digital evidence is the connection of most mobile devices to cloud computing services. Manufacturers often integrate mobile devices with cloud services to reduce the device's battery energy consumption. This poses a difficulty because most of the work is done remotely on a server with an unknown location. This presents a real threat in obtaining digital evidence, as it is challenging to extract it from a cloud server in an unknown location.

Second Requirement: Obstacles Related to the Nature of Digital Evidence and the Digital Environment

The obstacles related to the formative nature of digital evidence refer to its invisible and dynamic characteristics[39]. These issues negatively affect the collection procedures, making it easy to hide digital evidence and difficult to obtain it. The following are the difficulties related to the evidence itself in the first part and the difficulties related to the digital environment in the second part:

Firstly: Difficulties Related to the Evidence Itself

The seriousness of cybercrimes stems from their nature, which combines artificial intelligence and human intelligence, making them very difficult to prove criminally. Crimes committed through information networks are often invisible, and sometimes the victim does not even notice their occurrence. This is due to the

absence of physical evidence and the need for high technology. These difficulties are reflected in the evidence, including the lack of visual evidence, the ease of hiding it, and the difficulty of obtaining it.

a. Absence of Visual Evidence:

In traditional crimes, evidence is visible and tangible. However, in crimes involving electronic operations, the evidence pertains to moral aspects related to the automated processing of data. Establishing evidence is difficult due to the intangible nature of the crime scene. Most information and data circulating through computers are in the form of codes and pulses stored on magnetic media. Electronic operations, such as e-finance, rely on encryption, secret codes, pulses, numbers, and electronic storage[40].

b. Evidence is Easy to Conceal

Criminals who use electronic means to carry out their crimes are characterized by high intelligence and technical sophistication. This enables them to conceal their illegal acts and crimes. They use invisible manipulation of electronic pulses or vibrations to record data[41]. Additionally, they engage in acts such as spying on stored data files and copying them to obtain and use copies for their own interests.

Furthermore, they hack databases and change their contents to achieve specific purposes or sabotage systems. This sabotage can appear as if it results from an error in the program, hardware, operating systems, or the overall design of the system that processes information automatically.

c. Difficulty in Obtaining Digital Evidence

Perpetrators of cybercrime often use various means to hinder the collection of evidence. These include encryption technology[42] and security measures to prevent inspection, access, and seizure of evidence. They use passwords and hide their identity, especially when using the Internet. Many programs and applications work to obscure their identity.

d. Inadequate Procedures for Obtaining Digital Evidence

For evidence to be accepted in proving a crime, it must be legitimate. This requires that the authorized party collecting it complies with the conditions specified by law. However, the procedures for obtaining digital evidence face difficulties due to the inadequacy and unsuitability of traditional crime investigation methods. Despite the tremendous development of automated data processing systems, the search, collection, and examination of digital evidence are still conducted within the framework of traditional procedures stipulated in penal texts.

It is a principle that a suspect may not be obliged to provide evidence that would prove their guilt. Thus, the offender cannot be forced to provide a password or secret code to access files or data. Additionally, some offenders store data and information abroad, making it difficult to retrieve due to the obstacles posed by inspection issues.

Secondly: Difficulties Related to the Digital Environment

The digital environment is represented by a vast transnational Internet network. The Internet, or cyberspace, consists of numerous interconnected computer networks scattered across the globe. Despite its universality and transnational routes, the Internet is not owned by any individual, institution, or state[43]. Anyone can connect to the Internet with the necessary communication requirements, such as a computer with a modem.

The Internet is a union of existing networks covering almost the entire globe. The cost of its infrastructure was gradually funded by various bodies and entities, each owning its own network. These networks were later connected to the Internet. Therefore, no one can claim ownership or control over it. The Internet has no owner, supervisory body, or central authority that controls it. Many parties work in the field of the Internet and its services on several levels, namely:

1. **The First Level:** This includes parties involved in financing, organizing, and implementing the Internet network. These parties are headed by states, public authorities, and public and private Internet network operators.

2. **The Second Level:** This includes Internet service providers who offer subscribers Internet connectivity services under subscription contracts.

3. **The Third Level:** This includes content providers and publishers of value-added services and information on the Internet.

4. **The Fourth Level:** This includes ordinary users, who are the most important and effective parties in the Internet network. An ordinary user is a person who connects to the Internet through an Internet service provider.

The Internet offers a range of services, including email, the World Wide Web, search engines, online communication, discussion forums, newsgroups, and file transfer services[44].

The complexity of the digital environment, its vastness, and the multiplicity of its actors, as well as its transcendence of national borders, further complicate the issue of extracting digital evidence. This emphasizes the need to strengthen international cooperation to ensure greater effectiveness in collecting and obtaining digital evidence.

Conclusion :

In conclusion, digital evidence is an important and effective tool in criminal investigations. This highlights the need to equip law enforcement agencies with the necessary tools, resources, and technical expertise in technology to handle this type of evidence. Digital evidence is used not only to prove cybercrime but also traditional crimes.

As society's use and reliance on modern communication technologies increase, there is a growing need to train investigators and those responsible for collecting digital evidence. Special training

in the digital criminal field is essential. With increasing crime rates and the multiplicity of its means, the challenges for authorities tasked with combating crime have also increased.

The investigation of cybercrime usually begins with digital forensic research to obtain and extract digital evidence from the digital environment. This involves dealing with an infinite amount of data and information, requiring technical knowledge of technology. Through our study, we reached several results and proposals, which we include below:

Results:

- The legitimacy of digital evidence requires that the procedures for obtaining it comply with legal rules. Such evidence must be based on certainty and is subject to the judge's discretion.
- There is an absence or inadequacy of laws regulating the procedural aspects of collecting and processing digital evidence. Only general procedural rules exist, which are not commensurate with the nature of digital evidence and the digital environment.
- There is a lack of scientific expertise and technical know-how on automated data processing among law enforcement agencies responsible for collecting, analyzing, examining, and discussing digital evidence.
- There is a lack of material and financial resources to extract, transcribe, and present digital evidence for discussion before judicial authorities, given its invisible and intangible nature.

Recommendations:

- Digital evidence should be incorporated as a recognized type of criminal evidence, ensuring clarity and avoiding any doubts about its validity. This should be explicitly stated in procedural laws, aligning with fair trial principles.
- Technical training courses should be offered for investigators on handling, extracting, and preserving digital evidence for court presentation. This will help prevent errors due to a lack of technical expertise, which could lead to the destruction of digital evidence and render it inadmissible.
- Forensic laboratories should be established equipped with advanced technologies for analyzing, opening, and decrypting files. These labs should be managed by specialized technical teams under judicial supervision.
- International agreements should be promoted and cooperation for the exchange of information and seizure of digital evidence, especially when such evidence is located outside national borders.
- Awareness should be raised among individuals to report cyber-attacks promptly, ensuring the timely and proper seizure of digital evidence.

Bibliography :

-Law 66-155 amending and supplementing the Code of Criminal Procedure.

-Law 09-04 of August 05, 2009, containing the special rules for preventing and combating crimes related to information and communication technologies.

-Ashraf Abdul Kader Kandil, Criminal Evidence in Cybercrime, New University House, Alexandria, 2015.

-Ahmed Yousif Al-Tahtawi, Electronic Evidence and its Role in Criminal Evidence, Arab Renaissance House, Cairo, 2015.

-Khaled Hazim Ibrahim, The role of security agencies in criminal proof in crimes related to the international information network - the Internet - a comparative study, Safwa Printing, 2014.

-Khaled Mamdouh Ibrahim, Digital Criminal Evidence and its Authenticity in Evidence, first edition, University Thought House, Alexandria, 2020.

-Khaled Hassan Ahmed Lutfi, Digital evidence and its role in proving cybercrime, University Thought House, Alexandria, 2020.

-Khaled Hassan Ahmed Lutfi, Modern criminal evidence in proving cybercrime, first edition, University Thought House, Alexandria, 2023.

-Rafah Khudair Jiad Al-Ardi, Electronic evidence and its impact in the field of criminal evidence theory - a comparative study, first edition, Zain Law Publications, Lebanon, 2019.

-Rashida Boker, Crimes of Assault on Automated Processing Systems in Comparative Algerian Legislation, first edition, Halabi Law Publications, Lebanon, 2012.

-Samy Galal Faqi Hussein, Computer Evidence and its Authenticity in Criminal Evidence - A Comparative Study, Dar Al-Kutub Al-Qanuniya, Egypt, 2011.

-Abdel-Fattah Bayoumi Hegazy, Criminal Evidence in Computer and Internet Crimes, Special Edition, Bahgat for Printing and Binding, Egypt, 2019.

-Omar Mohamed Abukar Younis, Crimes arising from the use of the Internet, Arab Renaissance House, Egypt, 2004.

-Ali Aboud Jaafar, Modern Information Technology Crimes Against Persons and Government - A Comparative Study, first edition, Zain Legal and Literary Library, Lebanon, 2013.

-Mostafa Mohamed Morsi, Criminal Investigation of Cyber Crimes, first edition, Police Press, Cairo, 2009.

-Mahmoud Ibrahim Ghazi, Criminal Protection of Privacy and E-Commerce, first edition, Al-Wafa Legal Library, Alexandria, 2014.

-Robert Moore,Cybercrime.Investigating High-tech Computer Crime,Welly press,London,2018.

-Abderrahman Mohammed Bahr, Obstacles to the investigation of Internet crimes, Master's thesis, Institute of Graduate Studies, Naif Academy for Security Sciences, 1999, p. 27.

- Khadija Abdellawi, The impact of the application of remote trial on the guarantees of the accused, Al-Bassaer Journal of Legal and Economic Studies, Special Issue December 2021,