Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences and Forensic Medicine
المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي
https://journals.nauss.edu.sa/index.php/AJFSFM

Handling E-evidence in Egyptian and Comparative Legislation: A Comparative Analytical Study

التعامل مع الأدلة الإلكترونية في التشريع المصري والمقارن: دراسة تحليلية مقارنة

Ramy Metwally El-Kady
Criminal Law Department & Associate Professor, Police Academy, Egypt.

Received 26 Aug. 2023; Accepted 23 Oct. 2023; Available Online 26 Dec. 2023.

Abstract

This article aims to introduce e-evidence, describe its characteristics, examine its legal authenticity in Egyptian law, shed light on the requirements for the collection of e-evidence and its admissibility before the criminal judiciary, and highlight how e-evidence is criminally protected in Egyptian law along with the procedures for gathering and documenting it.

The pervasive usage of technology in all spheres of life may be traced back to the significance of the research topic. We have come to the logical conclusion that it is improbable that a traditional or new crime would occur without leaving behind E-evidence that may be used to identify the offender thanks to the proliferation of electrical and technological equipment and the Internet.

The research concluded that the effect of the changing nature of intangible forensic evidence on its reliability before the criminal courts, in a way that requires a precise legal regulation of this issue. The legislator defines a set of conditions for the procedures for collecting and documenting E-evidence to achieve the idea of its reliability and then produces its impact on the formation of the criminal judge's doctrine.

It is recommended strengthening cooperation with international organizations to exchange information related to E-evidence.

Keywords: Forensic sciences, E-evidence, E-forensics, Admissibility of E-evidence, Documentation of E-evidence.

المستخلص

يهدف البحث إلى التعريف بالدليل الإلكتروني ووصف خصائصه، وبيان موثوقيته القانونية في التشريع المصري، وتسليط الضوء على متطلبات جمع الدليل ومقبوليته أمام القضاء الجنائي، وإلقاء الضوء على الحماية الجنائية له في التشريع المصري خلال مباشرة إجراءات جمع الدليل وتوثيقه.

وتبرز أهمية البحث في ضوء التنامي المستمر لاستخدام التكنولوجيا في جميع مناحي الحياة، بالشكل الذي أضحى منطقياً أن نخلص إلى أن أية جريمة تقليدية أو مستحدثة لن يخلو من أن يتخلف عنها دليل إلكتروني يمكن أن يستخدم في التعرف على الجاني بفضل استخدام الوسائل التكنولوجية والإنترنت.

وقد خلص البحث إلى تأثير الطبيعة المتغيرة للأدلة الجنائية غير الملموسة على موثوقيتها أمام المحاكم الجنائية؛ مما يتطلب تنظيماً قانونياً دقيقاً لهذه المسألة. وقد حدد المشرع مجموعة من الشروط لإجراءات جمع الأدلة الإلكترونية وتوثيقها لتحقيق فكرة موثوقيتها، ومن ثم إنتاج أثرها في تكوين عقيدة القاضي الجنائي. وأوصى البحث بتعزيز التعاون مع المنظمات الدولية لتبادل المعلومات المتعلقة بالأدلة الإلكترونية.

الكلمات المفتاحية: علوم الأدلة الجنائية، الدليل الإلكتروني، الأدلة الجنائية الإلكترونية، مقبولية الأدلة الإلكترونية، توثيق الأدلة الإلكترونية.

Production and hosting by NAUSS

* Corresponding Author: Ramy Metwally El-Kady
Email: dr.ramy_elkady@yahoo.com

doi: 10.26735/WGZY6322

1. Introduction

Electronic evidence (E-evidence) represents one of the most prominent means of criminal evidence in electronic crime, as it is the means through which the link between the accused and the crime is established, in addition to being considered the means upon which the judge relies in forming his judicial opinion in the case, whether conviction or innocence [1].

E-evidence has some characteristics that differentiate it from traditional physical evidence and its changing moral nature, and then the importance of dealing with it and taking care of the procedures for collecting it, documenting, and preserving it in preparation for submitting it to the concerned judicial authorities and working on relying on it in proving the crime by preserving its integrity and emphasizing its admissibility before the judiciary in the light of General principles governing criminal evidence in electronic crimes.

1.1. The importance of the research

The importance of E-evidence can be rooted in the fact that the widespread use of technology in aspects of life, and the spread of electrical and technological devices and the Internet has led to a logical conclusion, to the effect that it is inconceivable that a traditional or modern crime will occur, without leaving E-evidence behind, which through this E-evidence, the perpetrator of the crime can be identified.

It is expected that the importance of E-evidence will increase in the criminal field, with the widespread use of new technologies, such as the IOT (Internet of Things) [2], dark web networks, high-level encryption, and virtual currencies, which will require law enforcement agencies to make radical changes in the methods of collecting evidence and mechanisms of international cooperation in criminal proceedings, in a manner commensurate with the nature of this new type of forensic evidence [3], which It is characterized by its changing moral nature, as the information stored on computers or cloud computing servers via the Internet is volatile [4], and it is easy to tamper with and change during investigations.

Indeed, this E-evidence is fragile and is subject to destruction through mishandling or improper examination [5].

Hence, the importance of E-evidence is evident, as it is the means that enables law enforcement authorities to know how cybercrime occurred, prove it, and attribute it to the perpetrator, especially since it is committed in a non-physical virtual environment [6], and it was necessary to set specific rules and conditions for dealing with this E-evidence to ensure its admissibility before criminal justice, as well as taking special precautions to document, collect, preserve and examine it.

In modern criminal procedure law enforcement practice, the assessment of E-evidence is carried out according to the general rules for assessing evidence, regulated by the criminal procedure law.

At the same time, the courts often do not take into account the electronic nature of the type of evidence under consideration, which sometimes leads to an erroneous criminal legal qualification of the act or other incorrect conclusions in the final procedural decision.

Scientific comprehension of a new source of information in the system of normatively established evidence is in its active phase (and is still far from completion). However, this analysis of theoretical views and law enforcement, primarily judicial, practice makes it possible to put forward proposals for a phased reform of the criminal procedural law and adjusting

law enforcement based on obvious and the features of E-evidence, which do not cause fundamental objections, concerning their essence, the specifics of collection, verification, and evaluation [7].

1.2. Challenges during the study

The challenges of the study stems from the special nature of the electronic evidence and its difference from the traditional physical evidence and the traditional general principles of criminal evidence.

The changing moral nature of the electronic evidence may threaten its evidentiary value during the trial and reduce its acceptability and reliability before the criminal courts, which requires special care in dealing with and preserving it so that the court can rest assured of it and rely on it among other case evidence in conviction or innocence.

1.3. Research Inquiries

The research raises many inquiries related to:

RQ1: What is the definition of E-evidence?

RQ2: What are the characteristics of the E-evidence?

RQ3: What does E-evidence legality and admissibility mean before a criminal judge?

RQ4: How can law enforcement agencies collect the E-evidence?

RQ5: What are the conditions for accepting E-evidence before a criminal judge?

1.4. Objectives of the study

The research aims to achieve a main goal represented in shedding light on the provisions that regulate the use of E-evidence in Egyptian Law.

Some sub-goals emerge from this main goal, most notably the following:

- Introducing the E-evidence and explaining its characteristics.
- Examining the legal authenticity of the E-evidence in Egyptian legislation.
- Shedding light on the conditions for methods of collecting E-evidence and their admissibility before the criminal courts.
- Shedding light on the criminal protection of E-evidence in Egyptian legislation.
- Shedding light on the position of international conventions and comparative legislation regarding E-evidence collection.

1.5. Research Hypotheses

The study hypotheses are the difficulty of collecting E-evidence obtained from crimes, due to its special changing nature, which will place the burden on investigators and criminal justice agencies to collect the forensic evidence.

1.6. Difficulties of the study

The difficulties of the study center on the novelty of its subject, as it deals with the difficulties facing law enforcement agencies in collecting and extracting E-evidence obtained from crimes.

1.7. Research methodology

The methodology of the study was the use of the analytical descriptive approach, which deals with E-evidence in all its aspects and dimensions, with the use of the comparative method through the review of comparative experiments organized on this subject, The analytical descriptive method is defined as: "To study the phenomenon as it exists in reality and describe it closely and express it qualitatively or quantitatively to reach conclusions that contribute to understand and develop this reality" [8], this approach aims to research and analyze E-evidence from its legal aspects, and the preparation of this study has been assisted by

available legal references, from general literature in the field of criminal law or specialized in the subject of the study, whether Arab or foreign references related to the subject of the study.

2. Literature Review

The subject of E-evidence is one of the modern subjects that have been recently raised by jurisprudence and one of the last research studies entitled “Conceptual and theoretical problems of the category of "digital (electronic) evidence" in the criminal process” [9] focused on revealing the essence and legal nature of the concept of "digital evidence" in criminal procedural legislation, as well as analyze their place in the system of procedural sources of evidence, their relationship with other types of evidence, as well as investigate the issue of distinguishing the institution of digital evidence in the Criminal Procedure Code, and concluded that digital evidence in the criminal process is a rather controversial and complex category, due to the fact that there is no comprehensive position of the legislator on the normative dimension regarding this issue, and due to the active and heterogeneous discussion at the doctrinal level regarding the perspective of institutionalization of digital evidence in the criminal process, and the research emphasized on the need to highlight the concept of "digital evidence" at the level of criminal procedural legislation.

Another research entitled “Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence” presented a comprehensive study to examine the issues that are considered essential to discuss and resolve, for the proper acceptance of evidence based on scientific grounds, and explained the state of forensics in emerging sub-fields of digital technology, and reviewing the challenges which may complicate the process of systematic validation of electronic evidence, and emphasized on the development of best practices, reliable tools and the formulation of formal testing methods for digital forensic techniques are highlighted which could be extremely useful and of immense value to improve the trustworthiness of electronic evidence in legal proceedings [10].

3. Research Plan

The research is divided into several sections:

- The first section: is entitled “General Provisions for Defining Criminal Evidence and Electronic Evidence.”
- The second section: is entitled “Characteristics and types of electronic evidence.”
- The third section: is entitled “Stages of Digital Forensic Investigation.”
- The fourth section: “The credibility of electronic evidence and the conditions for its acceptance before the American judiciary”.

3.1. The first section: “General Provisions for Defining Criminal Evidence and Electronic Evidence”.

3.1.1. Definition of Forensic Evidence

Before defining E-evidence, we should define forensic evidence, which refers to the means that link facts to the conviction or innocence of individuals during criminal trials.

It is also a set of clues, through which a set of facts about the crime can be established, in addition to the ability to attribute it to a specific offender.

Or it is a set of proofs accepted by the rule of law that the facts of the crime cannot be proven except by using it before the judicial authorities, whether the courts or the Public Prosecution, and it varies according to the variety of crimes [11].

Hence, forensic evidence is every procedure recognized by law to convince the judge of the truth of the incident in question, and the evidence is obtained from the crime scene, which is defined as: “The place where the crime occurred or was committed".

Given the great importance of forensic evidence for the judicial authorities to reach the truth, it has been restricted by a set of restrictions and controls, and this means that this forensic evidence must be based on proof and logic, and the mind must be convinced of it [12].

3.1.2. Definition of E-evidence

Several legislations developed a definition of E-evidence, among which we mention the Egyptian legislation, which defined E-evidence as: “Any electronic data that is stored, communicated, extracted, or taken from computers, information networks, or other sources and has evidentiary value or power can be gathered and analyzed using specialized technological tools, programs, or apps.” (Art.1) of Law No. (175) of 2018 regarding combating information technology crimes).

The Emirati legislator adopted the same definition in its Federal Decree Law No. (34) of 2021 regarding combating rumors and electronic crimes (Art.1).

It is noted that the legislator was keen to highlight the essence of E-evidence, which is the information extracted from technical devices, whether they are computers, automation information networks, and the like [13].

3.1.3. Digital trace and E-evidence

The digital trace means everything that results from the user’s interaction with information technology means and computers, as this interaction produces a large group of digital traces (sometimes called digital fingerprints or artificial objects), but this trace turns into digital evidence if the technical experts succeed. Using special technological devices and applications to link him to the committed crime, and then prove the link between him and the perpetrator of the crime.

Particularly, a person utilizing information and communication technology (ICT) can leave a digital footprint, which refers to the data left behind by ICT users that can reveal information about them [14], including age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history and concerns, psychological disorders, employment status, affiliations, relationships, geolocation, routines, and other activities. This digital footprint can be active or passive.

- An active digital footprint is created by data provided by the user, such as personal information, videos, images, and comments posted on apps, websites, bulletin boards, social media, and other online forums.
- A passive digital footprint is data that is obtained and unintentionally left behind by the users of the Internet and digital technology (e.g., Internet browsing history).

Data that are part of active and passive digital footprints can be used as evidence of a crime, including cybercrime (i.e., digital evidence). This data can also be used to prove or disprove a matter being asserted; refute or support the testimony of a victim, witness, or suspect; and/or implicate or exculpate a suspect of a crime.

3.1.4. E-evidence and E-forensic Science

The E-evidence means any content in electronic or digital form resulting from the use of a computer,

information network, or any means of information technology.

Whereas, E-forensic Science is one of the branches of forensic science, which deals with searching for, obtaining, processing, analyzing, and reporting data stored in electronic devices.

Hence, E-forensic Science or digital forensic analysis means the retrieval and investigation of computer digital traces, and to track these traces, digital forensic experts benefit from the ability of computers to store, record, and save data on most of their activities, and therefore those of their users [15].

Therefore, the task of digital forensics experts is to find exact copies of the E-evidence, or undisturbed images of it, containing a copy as detailed as possible, and to examine and analyze the data, without any disturbance to it, in addition to the ability to recover deleted or damaged files [16].

Digital forensics is a vital part of almost every criminal investigation given the amount of information available and the opportunities offered by electronic data to investigate and evidence a crime. However, in criminal justice proceedings, these electronic pieces of evidence are often considered with the utmost suspicion and uncertainty, although, on occasion are justifiable.

Presently, the use of scientifically unproven forensic techniques is highly criticized in legal proceedings. Nevertheless, the exceedingly distinct and dynamic characteristics of electronic data, in addition to the current legislation and privacy laws remain as challenging aspects for systematically attesting evidence in a court of law [17].

The digital forensics process involves the: search, acquisition, preservation, and maintenance of digital evidence; the description, explanation, and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability, and relevance to the case; and the reporting of evidence pertinent to the case [18].

3.1.5. The international and regional framework for combating Cybercrimes and dealing with E-evidence:

It can be said that the international and regional framework for dealing with E-evidence is itself the framework for combating cybercrimes and among the most prominent international and regional instruments are:

3.1.4.1. European Situation

the European Convention (Council of Europe Convention) on Cybercrime of 2001, otherwise known as the Budapest Convention, and the Additional Protocol to the Convention on the Criminalization of Acts of a Racist or Xenophobic Nature Committed by Computer Systems.

It is worth noting that the European Commission is in the process of presenting a draft additional protocol attached to the Budapest Agreement in the field of securing electronic evidence, which aims to enhance cooperation between the parties in the fields of tracking cybercrimes and securing E-evidence.

Add to this the European Union Resolutions of 2001 on fraud and forgery in non-monetary payment media, of 2005 on attacks against information systems, the 2010 European Union draft directive on attacks against information systems, and the 2011 European Union Directive on combating sexual abuse, sexual exploitation of children and exploitation of children in pornography.

3.1.4.2. Arab Situation

The Arab Convention for Combating Information Technology Crimes of 2010, and the Arab Model Law for Combating Information Technology Crimes of 2004 (UAE Model Law).

3.1.4.3. At the African level

Draft African Union Convention on the Establishment of a Legal Framework to Assist in Cyber security in Africa of 2012, Draft Model Law of COMESA (Common Market for Eastern and Southern Africa) of 2011 on Cyber security, Draft Directive of ECOWAS (Economic Community of Western States) Africa) of 2009 on combating cybercrime within West African countries.

Add to these regional charters, the Convention of the Commonwealth of Independent States on Cooperation in Combating Computer-related Crime, and the Shanghai Cooperation Organization Convention in the field of international information security.

3.1.4.4. At the International level

In addition to the 2000 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography, and the 2010 Model Legislative Texts on Cybercrime and Electronic Evidence for the International Telecommunication Union, the Caribbean Community, and the Caribbean Telecommunication Union.

3.2. The second section: "Characteristics and types of electronic evidence."

3.2.1. Characteristics of the E-evidence

The E-evidence is characterized by several characteristics as follows, see Figure 1.

- Dealing with the E-evidence requires specialized scientific and technical knowledge, and it cannot be extracted or even discovered, except through specialized experts [19].
- The E-evidence is technical and consists of information that is embodied in an electronic image, which is not perceived except by using information technology [20], and therefore the E-evidence is only in a digital environment [21].

Figure 1- *Shows E-evidence Characteristics*

- The E-evidence consists of data and information of an intangible electronic form that is not perceived by the ordinary senses, but rather its realization requires the use of HARDWARE devices and equipment, and the use of SOFTWARE computer software systems [22], E-evidence is not only less physical than physical evidence, but also reaches the degree of imaginary in its shape, size, and undeclared location, which achieves this link between it and the perpetrator [23].
- The E-evidence is of a high-speed dynamic nature, moving from one place to another through communication networks that transcend the limits of time and space [24].
- The possibility of extracting Copies of E-evidence that are identical to the original and have the same scientific and evidentiary value and this matter is not available in traditional evidence. Which constitutes a highly effective guarantee for preserving the evidence against loss, damage, and change, using exact copies of the evidence [25].

- The E-evidence can be retrieved after erasing, repaired after being destroyed, and shown after concealment, which leads to difficulty Getting rid of it, which is the most important characteristic of the E-evidence, and this is done through the use of computer programs whose function is to recover data that has been deleted or canceled, which means that it is difficult for the perpetrator to hide his crime from the eyes of criminal justice men [26].
- Through the E-evidence, it is possible to monitor the information about the offender and analyze it at the same time. The E-evidence can also record the individual's movements, behaviors, and some personal matters about him [27].

3.2.2. Classification of E-evidence

Jurisprudence differed on the classification of E-evidence between two directions:

(First): E-evidence sees an advanced stage of physical evidence [28].

(Second): considers that E-evidence has a special nature, and constitutes a new addition to other types of evidence [29].

The researcher believes that the second opinion is the first to be supported due to the clear differences between the traditional physical evidence and the E-evidence.

3.2.3. Distinguishing between traditional and E-evidence

The E-evidence has several features that distinguish it from other traditional directories, the most prominent of which are:

- It is fleeting and changeable, which raises the problem of memorizing and obtaining evidence.
- In addition to the difficulty of accessing it when the suspects use an encryption system, it makes obtaining it without the encryption code difficult and time-consuming.
- In addition to its presence in multiple geographic locations, and therefore the difficulty of obtaining it outside the jurisdiction of states.
- In addition to many problems related to its admissibility before the criminal courts.

The most prominent features of the distinction between each of the two evidences are as follows:

- Traditional evidence has a tangible paper backing, unlike the E-evidence; its support is computer programs or any modern technical media, and then the E-evidence needs technical media to read it, while the physical evidence can be read easily and directly from its paper backing.
- The E-evidence is easy to search for, manage, modify, store, retrieve, and classify, using some of the characteristics of electronic programming, unlike the physical evidence that proves the state in which it was prepared.
- The E-evidence, according to its electronic support that accommodates large information depending on the size of the medium and the amount of information, provides the opportunity to display an unlimited number of documents, in a small area of the electronic medium.

3.2.4. Types of the E-evidence

Types of E-evidence vary; some are divided into three main sections:

- **First:** E-evidence related to computers and their networks.
- **Second:** E-evidence related to the international information network, the Internet.
- **Third:** E-evidence related to the protocols for

exchanging information between devices on the Internet.

Others refer to a second division decided by the US Department of Justice in 2002, into three groups, including [30]:

- **First:** Records kept on the computer, such as written and archived documents, such as e-mail messages, written text files such as Word, and Internet chat room messages.
- **Second:** Computer-generated records, which are considered outputs of computer programs that did not involve human intervention, such as phone records, and ATM bills.
- **Third:** Records part of which was saved by input and the other part was generated by a computer, such as financial worksheets that contain entries processed through worksheet programs, such as EXCEL, by performing calculations on them.

Hence, the diversity in the forms of the E-evidence assumes the diversity and multiplicity of the means of obtaining it from computers and information networks.

Therefore, some believe that the issue of extracting E-evidence from computer outputs and information networks is that the evidence derived from them remains digital, even if it takes another form, and the law's recognition of this other form is based on a hypothetical character based on the importance of the E-evidence itself, and its necessity in the process of proof criminal information technology crimes [31]. Hence, it is necessary to take the course of assumption in terms of considering it as original evidence.

3.3. The third section: "Stages of Digital Forensic Investigation."

Researchers divide the stages of collecting E-evidence in the virtual world into Four stages, see Figure 2:

Figure 2- *Stages of Digital Forensic Investigation*

- The first is the data collection stage.
- The second is the stage of examining and retrieving evidence.
- The third stage is data analysis and preparation of reports to present the evidence to the court.
- The Fourth stage is evidence documentation.
- These stages will be reviewed as follows:

In 2006, the US National Institute of Standards and Technology proposed a four-stage digital forensic model (see Figure 3) in its guide for integrating digital forensic techniques into the incident response [32]:

- **The collection phase,** which includes identifying evidence at the scene of the accident, its labeling, documentation, and final collection;
- **The examination phase,** where appropriate digital forensic tools and techniques are identified to extract relevant E-evidence while maintaining its integrity;
- **The analysis phase,** where the extracted evidence is evaluated to determine its usefulness and applicability to the case;

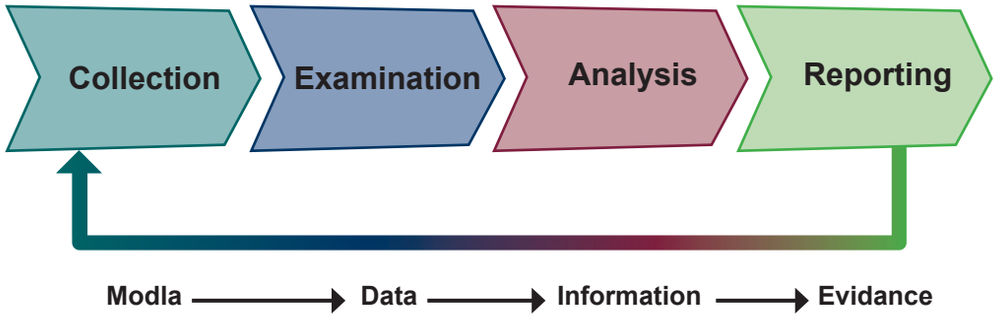

Figure 3- *Four-stage digital forensic model*

- **The reporting phase,** which includes the actions performed during the digital forensics process and the presentation of the results.

3.3.1. The phase of collecting Data

The first step in collecting E-evidence is to collect data on the occurrence of crime in the virtual world, which requires the need to identify the sources that appear to have E-evidence, which can be a physical device, an information system, or a service.

Then, the party involved in collecting the evidence (whether they are judicial officers or experts specializing in collecting electronic evidence) must obtain evidence from the sources, and ensure that it is in a format that can be easily copied while preserving the original state as an image while preserving the integrity of the data [33].

Some point out that, there is a relationship between physical evidence in the real world and their analogs of E-evidence in the virtual world.

Real-world data is a guide when investigating a case that occurred in the virtual world, so investigators will need to analyze all evidence from both worlds in some cases [34].

3.3.1.1. Challenges facing law enforcement agencies in dealing with E-evidence

The most prominent challenges facing law enforcement agencies in dealing with E-evidence are as follows:

A large amount of data and information

The expansion of the use of the Internet and the wide flows of data and information through the international network, the use of cloud computing by offenders, the dissemination of information on external servers, and huge databases are among the challenges facing law enforcement agencies, in a way that prompted them to develop tools A technology that relies on artificial intelligence algorithms to analyze the huge amount of data and information, to reach the data and information required to prove the link between the perpetrator and the crime, which undoubtedly constitutes digital forensic evidence.

Using encryption and other data obfuscation methods

(Art.1) of the Executive Regulations of Law No. (175) of 2018 defines both encryption and the encryption key, as Encryption: A computerized system that processes and transforms electronically accessible data and information using specific keys to make it impossible to access the data and information without a decryption key or keys.

Encryption Key: utilized in encryption and decryption procedures are a certain length of integers, symbols, or letters. Symmetric encryption, which uses the same key for both encryption and decryption, calls for the key to be kept a secret.

Asymmetric encryption employs a pair of keys coupled mathematically so that one is used for encryption and the other for decryption. One key must be kept secret while the other can only be disclosed under certain circumstances.

The informational offenders tend to hide any connection between them and the crime, to prevent them from being tracked down by law enforcement agencies, which leads them to use encryption techniques to anonymize their identity and obfuscate the data, which showed the widespread use of dark web networks on which various criminal activities are spread. There is no doubt that the use of encryption techniques is a real obstacle in tracing criminal activities on the part of law enforcement authorities. Offenders may use techniques to hide information within files, photos, and applications. Media files are ideal hosts for steganography, and hidden data may be identified by comparing the suspect's file and data streams with known assets.

A UNODC study on cybercrime indicated that E-evidence is often encrypted by suspects in the majority of countries (60-80%), that encryption may require specialized technical assistance and capacity, and that some countries have no way of dealing with an encryption problem without obtaining or possessing the keys from the suspect, and that if the suspect does not disclose the decryption keys, the investigators may use technical expertise and decryption software [35].

Data storage on external servers or the electronic cloud

Information offenders store and disseminate data and information on servers outside their countries and cloud computing servers, to facilitate their commission of crimes and at the same time secure themselves from the pursuit of law enforcement agencies that face legal difficulties in tracking E-evidence stored on these servers outside their jurisdiction. Cloud data storage is the process of recognizing, collecting, and analyzing electronically stored information [36].

3.3.1.2. Legal framework for data collection in comparative legislation

The data collection stage represents one of the most important stages of forensic evidence investigation. Therefore, legislators in comparative legislation were keen to establish a legal framework regulating it in a way that achieves the effectiveness of criminal procedures in dealing with this type of digital evidence.

Egyptian law has carefully regulated temporary criminal decisions and orders in Article 6, which are issued by the competent court upon the request of the Public Prosecution, in cases of seizing data and information and tracking them, or searching, inspecting, and accessing computer programs and databases, or ordering service providers to encrypt their data or information under its control or stored with it, and data of users of its service.

The Egyptian legislator has authorized Public Prosecution to issue some judicial orders to law enforcement agencies, to search for E-evidence, which consists of ordering entry into systems, programs, and websites, ordering their inspection, and seizing data or information that is useful to the investigation, to achieve the objectives of the investigation.

The law regulates temporary judicial orders issued to law enforcement agencies, for a period not exceeding thirty days, renewable once, in cases of seizure, withdrawal, collection, or reservation of data, information, or information systems, and to follow them with the delivery of their E-evidence

to the authority issuing the order, or searching, inspecting, accessing, and accessing computer programs and databases, while obligating the service provider to hand over whatever data or information it has related to an information system or technical device that is under its control or stored with it, as well as the data of its service users and the communications traffic that took place on that system. The technical body and the appeal of the orders shall be before the competent criminal court held in the consultation room.

The practical application indicates some problems related to the implementation of data collection orders and the implementation of permission to search networks and information systems, given that the implementation of the search warrant is originally to be limited to a specific spatial scope, which raises the problem of the extent to which it is possible to search and search for evidence in another place in an information system other than For which the search warrant was issued, especially since the nature of information crimes enables the perpetrators to easily hide and even destroy and erase evidence of the crime during the period that the investigative and evidentiary authorities need to obtain a second permit to search the other place, and what action can be taken if the owner of the place or the system refuses. The other is to allow the inspection to begin.

Part of comparative jurisprudence has argued that investigative authorities can overcome this problem by including permission to search with permission to search any other information system located anywhere other than the place of research, which is the same approach taken by some comparative legislation [37].

Among them, we mention the Dutch law, in which the Dutch Computer Crime Law, in Article 25, allows the possibility of extending the search of a residence to the search of an automated system located elsewhere to obtain data that can reasonably be useful in revealing the truth, and if this data is found, it must be handed over. This is about the first question, for the second question, which concerns the refusal of the person who owns the website or other electronic system to submit to the inspection procedure.

Part of comparative jurisprudence considers that in this case, it is not permissible to search unless the person consents to the search or there is a case of flagrante delicto that permits the evidentiary and investigative authorities to search the electronic system without requiring the issuance of a search warrant [38]. In this case, the order to extend the inspection may be issued orally by the investigating judge until written permission is issued. In all cases, the permission must be reasoned, so that the judicial authority can monitor the extent of its legality.

One of the procedural problems that hinders justice agencies is the case of conducting inspections in cross-border cybercrimes. Cybercrimes may occur through information networks, which connect many computers in many different countries. Therefore, the search warrant raises the problem of conducting it on a computer outside the country. The geographical scope of the state that issued the inspection permission, and then the problem of the legitimacy of this procedure and its infringement on the sovereignty of the other state arises.

Comparative criminal jurisprudence believes that this procedural problem can be overcome by strengthening international cooperation in combating information crimes by concluding bilateral and collective agreements regulating the initiation of this procedure [39], while a second side argues that it is not possible to conduct cross-border inspections without obtaining the permission of the other state.

Or the existence of an international agreement permitting this to be done [40].

Article (32) of the Budapest Convention permitted the possibility of entering devices or networks belonging to another country for inspection and seizure without its permission in two cases: (a) If the inspection relates to information or data made available to the public. (b) If the owner or holder of such data consents to such inspection." However, applying this provision can raise application problems [41].

Article 19 of the Budapest Convention stipulates the need for state parties to adopt procedural legislation that grants specific authority power to ensure the search for and seize evidence of a crime, and stipulates inspection and seizure procedures for data stored in a computer information system or an information storage support, whether this data is stored in a device. One or another in a communications system.

While Article (19/1) of the Budapest Convention stipulates that each state party must adopt legislation that grants the competent authority the authority to inspect or similar entry, defining the term inspection does not raise any difficulty, as it means searching and excavating evidence of the crime by examining the data and trying to find out its content or line. Her walk. As for the term access, and what is sometimes expressed as access, it is a term specific to technology and communication systems, which achieves access to stored data and is naturally required by conducting inspection and obtaining evidence.

Therefore, there is a difference between the two. Entry is a procedure for inspection, and inspection is a means of collecting evidence. Despite this distinction, they are considered among the investigation procedures that affect the rights of individuals. Therefore, its action must be based on a legal text, and this is what is stipulated in Article 19/2 of the Convention. The American legislator stipulated this procedure in Article (USC 2703 18), and the French Code of Criminal Procedure stipulated it in Articles 56 and 97 of Criminal Procedure [42].

One of the comparative legislations that regulated inspection procedures in the field of information crimes is the Belgian law. Article (88) of the Belgian Criminal Investigation Act, which was added to the law issued on 11/23/2000, stipulates that: "If the investigating judge orders the search of an information system or part of it, this search may be extended to another information system located in A place other than the original place of research, and this extension is carried out according to two conditions: (a) If it is necessary to reveal the truth about the crime in question. (b) If there are risks related to the loss of some evidence, due to the ease of erasing, destroying, or transferring the data in question. This allows the investigating authorities to obtain a copy of the data they need, without the permission of the state within whose territory the requested data is located.

Belgian jurisprudence justifies this text by saying that the investigating authority can enter the system and view the required data without realizing that this data physically exists outside the territory of Belgium. The alternative to this text is to send a judicial committee to the concerned state and ask its competent authority to seize the data that constitutes the crime scene and give it a copy of it. This takes time during which the accused may destroy this data [43]. However, jurisprudence recognizes that this text represents an assault on state sovereignty.

Some comparative legislation, including the Belgian law, has allowed the investigating judge - for fear of erasing, destroying, transferring, or losing evidence obtained through inspection - the authority to order its seizure, if it exists on Belgian territory, or to request a copy of this data from foreign authorities. The location of the crime, if located in a foreign country.

The data subject of the crime, as well as the tools used to commit it, or the traces left behind, are useful in revealing the truth (Article 88 of the Belgian Criminal Investigation Act added to the law issued on 11/23/2000), are kept. A copy of the seized information is extracted from the media of the public prosecution and remains at its disposal until the end of the trial. Some believe it is necessary to keep another copy with the court clerks, for fear of damage or loss of the only desired copy at the disposal of the public prosecution or the court [44].

Egyptian law indicates that law enforcement agencies are tasked with seizing, withdrawing, or collecting data or information, and all of these actions are included in the control process, given the presence of E-evidence within a virtual environment that may require those in charge of law enforcement to perform technical operations that include withdrawing or extracting data or information from the virtual digital environment to control it, as inspection and seizure sometimes represents an attack on the rights of others, or on the sanctity of his private life, which requires the necessity of taking the necessary guarantees to protect these rights and freedoms.

Among the comparative legislation that has been keen to achieve such guarantees for the accused in criminal procedures, the law Belgian; It authorized the Public Prosecution to order the closure of data to prevent access to it, or to the copy extracted from it held by those using the system, to ensure the preservation of the data in question and to ensure the possibility of comparing it with the copy extracted from the device if the accused denies it (Article 29 bis/3).

Belgian law also allows the investigation authorities to withdraw data, a copy of which has previously been taken, from the device in the following cases:

- If it is the subject of the crime or results from it.
- If it violates public order or good morals.
- If it represents a danger to electronic systems.
- If it represents a risk to the information stored, processed, or transmitted in these systems (Article 39 bis of the Belgian Criminal Investigation Code) [45].

There is old controversy among jurisprudence about the validity of data and information to be a subject of seizure, as traditional opinion has argued that computer data is not valid to be a subject of seizure, and this is based on the intangible nature of the data that is not consistent with the procedural texts that require them to be material things. There is no tangible material nature in this data, and there is no way to control it except by transferring it to a tangible physical entity, whether that is through photography, or by transferring it to a support or other physical means [46].

While a major aspect of comparative jurisprudence holds that the data and information contained in the computer are valid to be subject to control, based on the possibility of recording and storing them on physical media. This electronically processed data is electronic vibrations or electromagnetic waves, that can be recorded, preserved, and stored on physical media, in addition to the possibility of transferring, broadcasting, receiving, and reproducing them, and therefore their physical existence cannot be denied [47].

This trend is based on some legislative texts in comparative laws, such as Belgian and Canadian law. In Belgium, Article (39) of the Belgian Criminal Investigation Act, added to the law issued on November 23, 2000, stipulates that seizure includes physical objects and electronically processed data. In Canada, Article (29/7) of the Canadian Evidence Act stipulates that a search Seizing the books and records of a financial institution is limited to search-

ing the place to inspect it and take a copy of the written materials, whether the records are written or in electronic form [48].

Article (19/3) of the Budapest Convention stipulates that each state party must adopt legislation that grants the competent authority the jurisdiction to seize or obtain stored data. This jurisdiction includes the following procedures (seizing or accessing data - verifying and retaining a copy of the data - maintaining the integrity of Data - preventing access to this data or removing it from the information system. The procedures stipulated in Article (19/3) can be divided into two types:

- The first is the precautionary measures, aimed at preserving the stored data that the competent authority deems important in the investigation by keeping it in its place in the computer information system or the storage support and preventing access to it, canceling it, or disposing of it.
- The second is the control procedures, which are subsequent inspection procedures. Access means collecting data, whether by taking the information storage medium itself or making a copy of the data stored in it or in the computer information system on paper or disks, which is what American law stipulates in Article (USC 2703 18).

Among the comparative legislations that allow the seizure of digital evidence is Belgian legislation, as Article (39 bis) of the Belgian Criminal Investigation Law permits the copying of materials stored in automated data processing systems to present them to judicial authorities [49].

Egyptian law also permits the Public Prosecution to issue an order to the service provider or any person in possession or under his control of certain data to submit that data, whether this data relates to the content or the itinerary. This procedure, like other previous procedures, is issued by a competent authority and implemented by people who do not follow this authority. They are persons in possession or under their control of data stored within a computer system or in an information storage platform.

Meaning that the order is issued to the person in physical possession of the data and the person in control, even if he does not have physical possession of it. Therefore, this matter concerns the service provider or any other person who has any data or information that may help detect IT crimes.

Egyptian law stipulates that this order is to hand over the data or information he has related to an information system or technical device, which is under his control or stored with him, as well as the data of the users of his service, and the communications traffic that took place on that system or technical device, while the article stipulates (18) of the Budapest Convention on the need for countries to adopt legislation obligating the service provider and other persons to provide certain data that is in their possession or under their control and stored in the computer system or storage support, which is what the American legislator followed by stipulating this procedure in Article (USC 2703 18).

3.3.1.3. Rules to be observed in proving E-evidence

The E-evidence is characterized by a special nature, which is its ability to be modified, and therefore this evidence is often characterized by a volatile nature [50], which requires a speedy investigation, and taking the necessary legal measures to control, inspect or seize this E-evidence, and therefore the investigation plan is based on this category of crimes depends on several factors, the most prominent of which are:

- Examining the nature of the automated data processing environment within which

the investigator will practice his work, and determining the quality and manner of dealing with it and its impact on the nature, scope, and timing of his procedures.

- Limiting sensitive sites and places in a building for processing or transferring data, such as the library of documents and places where tapes and magnetic disks are stored, and identifying those responsible for their security.
- Learn about the operating rules of the computer system, how to organize the electronic data processing cycle, and the centrality of tasks and knowledge in this regard.
- Determining the methods of auditing, processing, and other operations that can be performed with the help of the victim, and those that need to be performed through another computer.
- Taking into account the security of the information that the investigation may require obtaining from the electronic data processing system, which can only be available for a limited period within the data processing department.
- Examining the different possibilities of the type of support or receptacle remaining used to obtain and maintain evidence (paper, microfiche, receptacles, or magnetic media).
- Preparing a list of people who should be questioned, and specifying the points that must be clarified about them [51].

3.3.2. The phase of Examination and Retrieval of E-evidence

The phase of examination and retrieval of E-evidence includes extracting and evaluating crime-related data elements from the collected raw data set. The collected data may be in a form that cannot transmit meaningful information due to coding, coding, or compression. It also contains the process of neutralizing those that hinder the interpretation of the data.

When a service compresses or encrypts the data for protection or to increase storage efficiency, research is required to interpret the data. For data provided by the provider in the service using an independent type of infrastructure, it is specified Procedures for extracting and evaluating data according to the type provided by the Provider.

3.3.3. The phase of data analysis and preparation of reports on E-evidence

The analysis stage is based on analyzing the data and evidence extracted from the virtual world. On the most data and outputs to be examined at the outset, which depend on the type of crime committed in the virtual world, prioritization and the order of data analysis and the obtained outputs depend on the investigator's intuition and experience.

The reporting phase indicates how to present and explain the conclusion that results from the analysis phase.

Finally, those in charge of criminal investigations face some related challenges, the most prominent of which are: the reliability of the evidence obtained from the virtual world, and the amount and quality of the main data collected.

In addition, the investigators - at the phase of collecting information from the virtual world - about their direct access to data sources, are restricted to the extent of cooperation of the companies that own data and information.

Since these companies may reserve cooperation with the investigation authorities and provide the required data from them, unless the company is directly involved in the case, due to the lack of a legal obligation on it to cooperate with the investigation and trial authorities.

And then it refrained from disclosing any data about users, even if it was related to existing investigations or trials. For example, in 2016, Apple refused to cooperate with the FBI when it was asked to analyze the iPhone data of a dead terrorist due to its considerations of user privacy [52].

On the one hand, If the analysis technology is not fully developed, the analyst will not be able to collect or analyze data from the input or output device. This is in addition to the issue of protecting the privacy of users in the virtual world, and the extent to which investigators can be allowed to access information and evidence recorded on Hardware.

3.3.4. E-evidence documentation

The stage of documenting and characterizing digital forensic evidence comes at a later stage in the process of collecting and extracting evidence.

It is a stage in which the information stored on one of the devices or networks is produced into information in the form of hard copies, by printing copies of the stored files or photocopying them by any visual or digital means.

(Art.10) of the executive regulations of the law specifies how to document E-evidence, as the aforementioned article stipulates that: “The E-evidence is described and documented by printing copies of the files it is stored on or photographing them using any visual or digital method, getting their approval, and then writing the following information on each of them:

- The printing and copying dates and times.
- The name and signature of the person who printed and copied the document.
- The operating system's kind or name and version number.
- The program's name, the kind of version, and the commands that were used to create copies.
- Data and details concerning the precise evidence's content.
- Information on the tools, equipment, software, and devices utilized”.

There is no doubt about the sufficiency of this data, which was required by the regulations, to authenticate the process of collecting and documenting E-evidence.

3.3.4.1. E-evidence documentation tools

Digital forensics experts - in the framework of their technical work - use tools, software, or technical devices that help to create an image of E-evidence.

Among the most prominent of these devices are the anti-write device, which prevents any changes from being made to the original data [53], and "data or file carving" programs, which recover deleted or damaged files from the remnants of the initial data that remain on storage devices even after the original file is gone [54], and work to create a "step-by-step" copy of the stored information,

Sometimes digital forensic experts use cryptographic hash analyzers to deal with encrypted files. Any small change in the data results in a different encryption.

It is worth noting that the hardware, software, and technical tools used by experts to collect E-evidence differ according to the type of technical media used.

They also require different technologies to achieve the E-evidence, as mobile devices have different scanning tools than those used to scan a desktop computer or a network server.

The process of collecting E-evidence may include examining and analyzing electronic devices, desktop, and laptop computers in homes and workplaces, which usually contain large-capacity hard disks that store a large amount of information, including photos and videos.

as well as web browsing histories, emails, and instant messaging information, which typically run a small number of operating systems; such as Windows, Mac OS, and Linux.

The process of examining mobile devices includes small portable devices that operate with low power, have less storage capacity, and have simpler programs to facilitate phone calls and browse the Internet [55].

It is noteworthy that mobile devices and tablets - which are often upgraded versions of mobile devices - may constitute for investigators a huge treasure of information related to the commission of crimes, given their distinctive features, their ability to move, their presence in the company of its owner at all times, and its constant connection to communications networks, which helps in obtaining a reasonably accurate geographical location monitoring, in addition to what it contains the contact list and call logs, as well as the flow of all information and data through the networks of service providers Mobile Internet [56].

Forensic techniques related to information networks are also of great importance, through their association with mobile phones and computers, and their use in Internet services and cloud storage, where data is stored on the Internet through data centers, instead of being stored on the user's device, which calls for the use of systems to analyze information on these networks to arrive at the amount of information that can be aggregated, to obtain and store detailed information regarding the activities taking place in the network, the data must be actively collected and stored for later analysis.

This process may include an analysis of log files from network devices, such as firewalls and intrusion detection, as well as prevention systems, as well as an analysis of the content of recorded network data transmission, if available [57].

3.3.5. Standards and best practices for digital forensics

In 2012, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published international standards for digital evidence handling (ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence).

These guidelines included only the initial handling of digital evidence. The proposed four phases for digital evidence handling are as follows:

- **Identification:** This phase includes the search for and recognition of relevant evidence, as well as its documentation. In this phase, the priorities for evidence collection are identified based on the value and volatility of evidence.
- **Collection:** This phase involves the collection of all digital devices that could potentially contain data of evidentiary value. These devices are then transported back to a forensic laboratory or other facility for acquisition and analysis of digital evidence. This process is known as static acquisition. However, there are cases in which static acquisition is unfeasible. In such situations, live acquisition of data is conducted, for example, the systems of critical infrastructures (i.e., industrial control systems). These systems cannot be powered down as they provide critical services. For this reason, live acquisitions are conducted that collect volatile data and non-volatile data from live running systems. These live acquisitions, however, can interfere with the normal functions of the industrial control system (e.g., by slowing down services).
- **Acquisition:** Digital evidence is obtained without compromising the integrity of the data. This was highlighted by the United Kingdom

National Police Chiefs Council (NPCC), formerly known as the United Kingdom Association of Chief Police Officers, as an important principle of digital forensics practice (i.e., Principle 1: "No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court") [58]. This obtainment of data without altering it is accomplished by creating a duplicate copy of the content of the digital device (a process known as imaging) while using a device (write blocker) that is designed to prevent the alteration of data during the copying process. To determine whether the duplicate is an exact copy of the original a hash value is calculated using mathematical computations; here, a cryptographic hash function is used to produce a hash value. If the hash values for the original and copy match, then the contents of the duplicate are the exact same as the original. Understanding that there are certain "circumstances where a person finds it necessary to access original data [i.e., during live acquisitions]," the United Kingdom National Police Chiefs Council notes that "the person [accessing this data] must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions" (Principle 2) [59].

- **Preservation:** The integrity of digital devices and digital evidence can be established with a chain of custody, which is defined as "the process by which investigators preserve the crime (or incident) scene and evidence throughout the life cycle of a case. It includes information about who collected the evidence, where and how the evidence was collected, which individuals took possession of the evidence, and when they took possession of it" [60]. Meticulous documentation at each stage of the digital forensics process is essential to ensuring that evidence is admissible in court.

3.4. The fourth section: "The credibility of electronic evidence and the conditions for its acceptance before the American judiciary."

3.4.1. The legality of the E-evidence

The E-evidence requires that the means of obtaining it be legitimate, that the procedures for obtaining it were implemented due to the law [61], and that access to it was done through free will without any assault on the will of the accused or the will of others, such as the use of violence with the suspect to decode an information system, access the encryption solution circuit, or access stored data files [62].

The legality of the procedures for obtaining it is limited to merely following the established legal rules, rather, it must also agree with the established rules in the conscience of society [63].

From the comparative judiciary, see the position of the Belgian Court of Cassation, which ruled that: "The description of the illegal act is not limited to the act that the law expressly prohibits, but rather includes all an act that contradicts the fundamental rules of criminal procedures, or legal principles" [64].

Among the judicial applications about the legality of procedures for obtaining evidence, what was decided by an American court regarding the legality of law enforcement agencies collecting information about the occurrence of a crime, among the information and data that the accused shares with his friends on social networking sites, where the court ruled that: "If the settings related to privacy on the social networking site (Facebook) allow viewing of correspondence by "friends" so that state agencies

can access this information through the cooperation of one of the "friends" of the accused on the social networking site without this violating the Fourth Amendment [65].

While the accused undoubtedly believes that his account will not be shared by law enforcement, there is no justification for expecting that "friends" will keep the account confidential, and the larger the circle of "friends", the greater the likelihood that the accused's correspondence will be seen by someone He is not expected to see it and that the accused's legitimate expectations of maintaining his privacy end when he publishes his correspondence to his "friends"; Because these "friends" are free to use this information however they like, including sharing that information with state agencies" [66].

3.4.2. Admissibility of E-evidence before Criminal Courts

The criminal judiciary in some countries tended to set some rules or standards to assess the acceptability of E-evidence and ensure its reliability, and to examine the extent to which it can be relied upon in judicial procedures.

The most important rules for determining the admissibility of E-evidence before criminal courts are The need for the court to be certain of the integrity and authenticity of the E-evidence, and not to be subjected to any attempt to tamper with it, and then is the responsibility of the accusing authority to prove that this evidence was initially obtained by a legitimate means, and secondly to prove what is called the continuity of the evidence; That is, the status of the digital information as evidence has not undergone any modification or change that casts doubt on its credibility in revealing the facts of the crime throughout judicial procedures, from the date of its seizure until the issuance of a judgment in the case [67].

Before a digital device can be introduced in court as direct or circumstantial evidence it must be authenticated (i.e., it must be shown that the evidence is what it purports to be). To illustrate authentication practices, consider the following general categories of digital evidence: content generated by one or more persons (e.g., text, email or instant messages, and word processing documents, such as Microsoft Word); content generated by a computer or digital device without user input (e.g., data logs), which is considered as a form of real evidence.

User-generated content can be admitted if it is trustworthy and reliable (i.e., it can be attributed to a person). Device-generated content can be admitted if it can be shown to function properly at the time the data was produced, and if it can be shown that when data was generated security mechanisms were present to prevent the alteration of data. When content is both generated by a device and user, the trustworthiness and reliability of each needs to be established.

Those in charge of collecting E-evidence from the crime scene must take the necessary measures to preserve the integrity of the E-evidence, starting from the moment of its creation and up to the stage of its submission before the court, which is known as the continuity of the evidence and the stability of its condition and that it is not subject to modification, distortion or tampering with it, as they must preserve Continuity of evidence on both the physical devices containing the data (when it was received or captured) and the data stored on the devices [68].

The investigating authority must present to the court the procedures applied to preserve the integrity of the E-evidence, indicate the mechanism applied to preserve the evidence and document its chronological history, and that it has not undergone any change or tampering.

So, the Public Prosecution must present to the court that the data obtained from the device is a true

and proper representation of the original data contained in the device (health) and that the device and the data to be presented as evidence are the same as those that were originally discovered, preserved and documented in their chronological history (safety), because of this having a direct impact on the court favored the idea of reliability and trustworthiness of the E-evidence [69], see Figure 4.

Then its admissibility before the criminal judiciary and the court in its investigation of the case in the session may hear the witnesses and experts who collected and extracted the E-evidence and discuss with them what they proved in their reports to verify its validity and integrity and that access to it was done legitimately [70].

In sum, for the acceptance of E-evidence before the criminal courts, the evidence collection procedures must be carried out in a manner that guarantees the legal validity of the collection procedures, the preservation of the integrity of the evidence, the non-change of its form, and the continuity of its condition throughout the entire period separating its seizure and its use in the trial.

The importance of addressing the issue of the reliability of the E-evidence before the criminal courts is evident in the precedent of an appeal before an American court regarding the reliability of

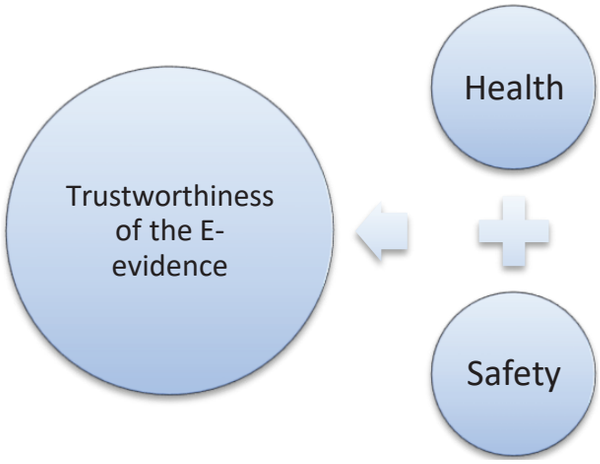

Figure 4- *Trustworthiness of the E-evidence*

Figure 5- *Conditions for accepting E-evidence*

computer-generated and stored information based on security gaps in operating systems and programs that could lead to threats to the integrity of digital information, where the court considered the issue of the vulnerability of digital information to manipulation during the submission of electronic evidence, and the need to demonstrate the validity of the computer about its ability to retain and restore the information in question [71], It ruled that: The acceptability of computer-generated information (such as log file records) gives details of the activities of the computer, network, and other devices that could be vulnerable if the system generating the information did not contain strong security controls [72].

Finally, some point out that the American judiciary relied on five basic conditions for accepting E-evidence before it, of any kind [73], see Figure 5 and these conditions are:

- It is related to the incident to be proven, whether directly or indirectly;
- It must be original; That is, the extracted evidence should be the same as the original data that was seized, without any change since it was seized and compiled.

- It must be reliable, and it must not have been tampered with or altered.
- It must be best, that the evidence presented be an original copy, as it is one of the best data and information available on which courts can rely in their judgments, which is a rule established in Article 1002 of the US Federal Rules of Evidence, which provides that: The original is required when proving the content of messages, records or images.
- Article 1003/3 of the aforementioned rules stipulates that: If the information is stored on a computer or similar device, any print or extract from it that is visually readable and shows the data accurately is considered an original copy.
- It should not be an auditory testimony; That is, E-evidence cannot be accepted if it is a word sent or just a rumor.

The approval of these conditions is due to what was decided by an American court in a case between Lorrinace and Markel American Insurance, as this ruling is an important judicial precedent.

For dealing in detail with the requirements for the admissibility of evidence extracted from electronic devices; such as e-mail and Internet sites, the contents of chat rooms and recordings are stored and transmitted [74].

3.4.3. The authoritativeness of the E-evidence in proof and international cooperation in its collection

3.4.3.1. The authoritativeness of E-evidence in criminal proof

Computer and electronic communications data - that may be related to a crime - contain many pictures, videos, e-mail messages, conversation records, and system data, and this data and information constitutes, to a large extent, E-evidence, However, in the context of criminal law, the question arose whether these new E-evidences enjoy the same legal authority as traditional evidences in proving crime, despite the moral nature of these evidences, which differs from traditional evidences?

Legislators have answered this question in anti-information technology legislation, by giving it the legal authority prescribed for traditional physical evidence over E-evidence of an intangible nature in criminal evidence.

We mention among them the Egyptian legislator who decided in (Art.11) of Law No. (175) of 2018 that: “When it satisfies the technical requirements outlined in the executive regulations of this law, evidence derived from or extracted from apparatus, machinery, media, electronic supports, information systems, computer programs, or any other information technology has the same value and authority as physical forensic evidence in criminal cases”.

The Saudi judiciary took this approach, as the General Authority of the Supreme Court in the Kingdom of Saudi Arabia issued Decision No. 34 of 4/24/1439 AH regarding E-evidence and its validity, which stipulates that: “When e-evidence is devoid of symptoms and varies in strength and weakness depending on the incident, its circumstances, and the evidence it contains, it is a valid argument in support of a claim”. Safety from accidents means that the evidence is free from modification and change and that it is reliable.

3.4.3.2. Conditions to be met to determine the authenticity of the E-evidencex

The authenticity of the E-evidence is of great importance about the role that the E-evidence plays in proving the crime, so the evidence must have important elements, to be relied upon in the process of proving the crime.

Therefore, the evidence must have important elements for it to be relied upon in the process of proving the crime.

The Egyptian Law on Combating Information Technology Crimes deals with the determinants related to the authenticity of criminal evidence related to the crimes stipulated in the law. As the law requires, to take into consideration, the E-evidence and consider it authoritative in the process of proof, the availability of some technical conditions in this evidence.The law referred the clarification of these controls and conditions to the executive regulations of the law.

(Art.9) of the executive regulations of the law specifies the technical aspects and conditions for dealing with this type of forensic evidence.

The aforementioned article stipulates that: “Evidence of usefulness online and reliable content If the following requirements and controls are satisfied, forensic evidence can be obtained in criminal cases:

- The process of gathering, obtaining, extracting, or eliciting e-evidence at the scene of the incident is carried out using techniques that guarantee non-change, update, erasure, or distortion of writing, data, and information; or any change, update, or damage to devices, equipment, data, information, or information systems; or any change to software or electronic supports; and other especially Write Blocker, Digital Images Hash technique, and comparable technologies.
- By the parameters of the decision of the investigating authority or the competent court, the E-evidence should be relevant to the incident and within the context of the subject to be proven or denied.
- That the E-evidence be gathered, extracted, preserved, and impounded by the judicial police officers who are qualified to handle this kind of evidence, or by experts or specialists designated by investigation or trial authorities, provided that it is noted in the control reports or technical reports on the types and specifications of programs, tools, and devices. The tools that were employed, together with the documentation of the Hash code and method obtained from the extraction of similar and identical copies of the E-evidence in the control report or the technical examination report, while assuring that the original is still kept without being tampered with.
- That the location of the evidence's seizure, the location of retaining it, the location of dealing with it, and its specifications be recorded in a record of procedures by the expert before the examination and analysis operations for it.
- The original of the E-evidence must be inspected if the copy cannot be examined and the devices being examined cannot be retained for whatever reason. All of this information must be noted in the seizure report or the examination and analysis report”.

It is clear from the previous text that the regulation required special requirements represented in the use of technical programs concerned with preserving the state of the E-evidence at the time of its extraction, as well as identifying those in charge of collecting and extracting the evidence among the competent judicial officers and experts assigned by the investigation authorities or the court to deal with this E-evidence.

The regulation limited the process of collecting evidence to E-evidence related to the incident - to the exclusion of others - according to the framework specified in this regard by the investigation authorities or the competent court. Extracting and collecting them, with an emphasis on the necessity of proving the case that the E-evidence could not be examined, and establishing this in the seizure report or examination report.

It should also be noted that the conditions and controls set by the executive regulations of the Law on Combating Information Technology Crimes must all be available in the E-evidence for it to be authoritative in the criminal evidence process, and if one of these elements fails, the evidence loses its necessary strength to invoke it and use it in the evidentiary process.

It must be noted here that with the loss of these conditions, the evidence loses its full ability in the process of proof, but that does not mean that what this process has led to is completely excluded, as it is possible to take into account what the evidence has led to, under other legal descriptions, however, it is not as strong as the evidence required by the Law on Combating Information Technology Crimes to be available.

To sum up: the researcher believes that the executive regulations of the law should have dealt with the procedures, techniques, and tools for collecting E-evidence in more detail, to achieve a detailed and integrated organization of the procedures for collecting and documenting E-evidence, which is one of the new evidence that requires the need to organize the provisions for dealing with it in detail, in the form which achieves its reliability before the criminal judiciary, and then enhances its utilization in the field of criminal evidence.

The executive regulations of the law on combating information technology crimes did not talk about the implications of the failure of the conditions that must be met in the digital forensic evidence, or the controls related to the procedures related to the process of collecting and documenting the evidence in the various stages, in addition to the absence of controls related to cases of damage to evidence at any stage of the investigation or trial, therefore, jurisprudence will have a great role in bridging legislative gaps, either by applying the rules in force in criminal evidence in general, or by establishing new judicial precedents. This is in addition to the discretionary space that the judiciary enjoys in determining the validity and authoritativeness of the digital forensic evidence presented.

3.4.3.3. The Egyptian judiciary's approach to relying on E-evidence

It is noteworthy that the Egyptian judiciary has relied on E-evidence obtained from information technology crimes, as one of the criminal departments relied on evidence derived from an electronic conversation via the Internet, and the Court of Cassation approved it [75].

The judiciary also used to provide evidence from the victim, whether it was his mobile phone, his computer, or by seizing it from the accused's device, as follows:

- **First hypothesis:** Providing evidence from the victim's device

About the first hypothesis, the judiciary relied on it if it was presented by the victim, and relied on it without permission because it was the phone of the victim who presented it with his full consent, even if it had a recording of the accused.

The Court of Cassation ruled that: (The legislator requires that the procedures described in the article be taken, placed under surveillance, the phone that the perpetrator used to direct insults and slander to the victim, according to those procedures imposed as a guarantee to protect the private life and personal conversations of the accused.

Hence, these procedures do not apply to recording insulting and slanderous words from the victim's phone, which he has of his own will, and without the need to obtain permission from the President of the Court of First Instance to record them, without this being considered an assault on anyone's private life, and therefore there is no blame on the plaintiffs.

Civilians if they put a recording device on their phone line, to record the insults addressed to them

so that they can identify the person who used to direct insults and slander at them over the phone.

Since this was the case, and the contested judgment concluded that the evidence derived from the tape recorded by the civil rights plaintiffs from their telephone device was invalid, it would have erred in the application of the law in what is defective and requires it to be overturned and repeated) [76].

- **Second Hypothesis:** Obtaining Evidence from the Accused's Device

As for the second hypothesis, the request is made to obtain the evidence by seizing it from the accused's device or monitoring it, which requires permission from the competent judicial authorities to do so.

The Penal Code contained a large number of presumptions of evidence against the accused until the Supreme Constitutional Court ruled that it was unconstitutional because it violated the principle of innocence of the accused, including the presumption that Article 195 of Penalties put in place, which assumed that the editor-in-chief was aware of all that was published in the newspaper he supervises. And the impermissibility of denying this presumption except through specific means stipulated in Article 195 of the same penalties, therefore, the crime must be proven by the accused without assuming it or establishing evidence against him.

Numerous rulings have been issued by the Egyptian judiciary stating that it has relied on E-evidence without taking a rigid stance and require that it be done in a traditional form such as an editor or witness testimony.

One of the famous cases was the case of burning the Egyptian scientific complex, where the court used compact discs and recordings proving the perpetrator of the crime, which it was reassured about.

Likewise, in the case of bribery that was presented to the judiciary based on recordings, the Court of Cassation ruled that: (Since it is proven from the records of the contested judgment that the court relied in convicting the appellant on the recordings of the two meetings that took place between the whistleblower and the appellant on November 26 and 28, 1996, the ruling expressed its confidence in it, then added by saying that, assuming the recordings are invalid, there is nothing to prevent the court from considering them as an element of proof in the case in the status of demonstration of evidence.

It is clear from what the judgment stated that the court did not originally base its judgment on those recordings, but rather relied on them as a presumption that strengthens the evidence that it provided, and this is not considered a contradiction or a disturbance in the judgment) [77].

Hence, it is clear that the judiciary had previously relied on E-evidence in several cases before the issuance of the Information Technology Crimes Law.

This is a praiseworthy approach to the Egyptian judiciary, which established these rules at a time when there was no legal regulation of this issue.

3.4.3.4. International Cooperation for Collecting E-evidence

The importance of international cooperation in criminal matters related to E-evidence is evident, given the transnational nature of these crimes, which are most often used to commit the Internet, and E-evidence exists, resulting from these crimes outside the legal jurisdiction of law enforcement agencies, which requires the existence of legal rules regulating issues of cooperation between countries, taking into account the unstable nature of E-evidence, which requires a quick response on the part of the investigation authorities, and the ability to request investigative measures Specialization requires strengthening the mechanisms of international cooperation on a large scale between different countries.

In this context, it is worth noting that the UNODC - in one of its studies on cybercrime - rightly believes that relying on traditional means of formal international cooperation in matters of cybercrime, is not currently sufficient to respond promptly to the requirements Obtaining ephemeral and changing E-evidence, located in multiple geographic locations, which will constitute a procedural problem for all crimes, not just cybercrimes [78].

The aforementioned study indicated that the majority of countries (over 70%) use the mechanism of formal mutual legal assistance requests, which usually takes about 150 days, to respond to these requests, and that often these periods may exceed the period of retention of the data by the service provider, or during which the perpetrators of the crime may be able to destroy E-evidence.

The importance of international cooperation in combating Cybercrimes is due to its special nature as a transnational crime, which requires rapid investigations characterized by unprecedented experience and cooperation, which requires the need for law enforcement agencies to cooperate quickly and effectively across national borders [79], as well as Cloud computing poses an increasing challenge to international cooperation because computer services are increasingly moved to geographically distributed servers and data centers, making it difficult to locate E-evidence [80].

In addition to limiting the scope of applicability of criminal rules to the territory of the state (the principle of territoriality of the criminal rule), which results in procedural difficulties in confronting these crimes, represented in the inability of the judicial authorities in the country to conduct some procedural judicial acts within the territories of other countries, such as inspection and seizure procedures to others. This is a criminal procedure [81].

Most bilateral, regional, and international agreements often include provisions requiring the need to resort to mutual judicial assistance, to achieve speed and effectiveness in the prosecution of offenders, and the collection of E-evidence [82].

The exchange of information in the field of Cybercrimes is one of the most prominent forms of international cooperation in confronting them, and it may take place bilaterally or multilaterally, through the International Criminal Police Organization or other counterpart bodies at the regional level such as Europol, Afripol, and the Arab Bureau for Combating Crime, and it means the exchange of information International security cooperation, which takes place through the exchange of information between the security agencies about the criminal activities undertaken by informatics criminals, to achieve effective security cooperation in confronting them.

Given the special nature of cybercrimes, international cooperation in combating them should not be limited to international security cooperation in the field of information exchange and international judicial cooperation in the field of judicial delegation and extradition of criminals. Rather, it requires international cooperation in the field of training security and judicial cadres to detect and investigate cybercrimes.

The international community has been interested in activating international cooperation in the field of combating cybercrime through several solutions, most notably: the Budapest Agreement, the European Union's framework decision, legislative activities, and capacity-building activities in the field of combating, which are supported by some regional international organizations such as the Organization of American States, and the Asia-Pacific Group, as well as the efforts of the International Working Group on Training in Cybercrime, and the efforts of the International Criminal Police Organization (INTERPOL) [83].

3.4.3.5. The role of INTERPOL in dealing with E-evidence

INTERPOL is working to enhance international police cooperation among its members - who num-

ber 195 countries - by providing field support services, where specialized assistance in the field of forensic evidence can be provided in the INTERPOL Digital Forensic Laboratory, and the field by fielding incident response teams. The INTERPOL also assists and guides member countries in setting up and maintaining state-of-the-art laboratories, in line with procedures adopted at the international level, to better support investigations and prosecutions.

The INTERPOL develops training programs that focus on unified curricula and solutions in the field of digital forensics, in close collaboration with the INTERPOL Capacity Building Unit and its partners from law enforcement agencies, the private sector, and university circles, and to achieve communication between specialized experts, as the INTERPOL Forensic Laboratory provides links between experts in all fields, around the world to share their knowledge and discuss ways to improve their daily work.

The INTERPOL works in combating Cybercrimes by preparing publications related to dealing with E-evidence, the most prominent of which are: Global Guidelines for Digital Forensic Laboratories, which present the procedures for establishing and managing a digital forensic laboratory, and provide technical methods for managing electronic evidence and its handling, and the Guidelines for First Insights in Digital Forensics, which provide advice on the search, seizure, identification, and treatment of E-evidence using methods to ensure its integrity to be admissible in the context of judicial proceedings.

In the same context, the INTERPOL organizes several forums related to dealing with E-evidence, most notably: the INTERPOL Digital Forensics Expert Group Meeting (annual meeting), which is open to specialists and managers from law enforcement agencies, government agencies, digital forensics companies, and university institutions to which you are invited, and the meeting is a suitable place for establishing relationships, exchanging experiences, and providing updated information on technology and new techniques in the field of digital forensic evidence.

4. Conclusion

The study reviewed the issue of digital forensic evidence and the procedures for collecting and extracting evidence obtained from crimes committed. The research resulted in a set of results and recommendations, as follows:

4.1. Results

- The increasing importance of E-evidence at present due to the communications and information revolution and the spread of the use of the Internet and computers, in a way in which E-evidence has become conceivable to exist in all forms of traditional and modern crimes.
- The emergence of a new type of E-evidence requires complex scientific and practical understanding.
- E-evidence in the criminal process is a rather controversial and complex category because there is no comprehensive position of the legislator on the normative dimension regarding this issue, and due to the active and heterogeneous discussion at the doctrinal level regarding the perspective of institutionalization of digital evidence in the criminal process.
- The relationship of E-evidence is considered with other types of evidence, in particular physical evidence and documents.
- The effect of the changing nature of intangible forensic evidence on its reliability before the criminal courts, in a way that requires precise legal regulation of this issue.
- The legislator defines a set of conditions for the procedures for collecting and documenting E-evidence to achieve the idea of its reliability and then produces its impact on the formation of the criminal judge's doctrine.

4.2. Recommendation

- The need to highlight the concept of "E-evidence" at the level of criminal procedural legislation.
- law enforcement officers must perform all their actions in compliance with the rules that apply specifically to the circulation of electronic evidence.
- Following best practices and guidelines for E-evidence collection, preservation, analysis, and presentation is crucial to ensure the integrity, reliability, and admissibility of E-evidence in court.
- Directing the Egyptian legislator's attention to amending the executive regulations of Law No. (175) of 2018 issued by Prime Minister's Resolution No. (1699) of 2020, by adding an article to Regulation No. (6) that was present in the draft regulation, which was regulating Procedures for collecting E-evidence by judicial police officers.
- The aforementioned article (according to the draft regulation) stated that: "The competent judicial officers, according to the reasoned order from the competent investigation authority, must carry out the procedures mentioned in Article No. (6) of the law, according to the following controls: The process of seizing, collecting, or obtaining Extracting, or preserving E-evidence at the scene of the incident, and extracting digital forensic images from such evidence with devices, equipment, software, digital forensic research tools, and technical methods such as Write Blocker or similar, to ensure that writing or data is not altered, updated, erased, or distorted. Including information, as well as any modification, revision, or harm to tools, machinery, data, information, information systems, software, programs, electronic supports, and others. The procedures must be documented in the seizure report and the initial examination report according to the following:
- The process of searching, inspecting, entering, and accessing computer programs, databases, devices, and information systems should be by the scope specified by the decision of the competent investigation authority or the court, or with written permission from the person concerned and be linked to Just by the fact.
- Inspecting, describing, and photographing the seizure process and the crime scene or the incident before the examination and analysis operations, and documenting the place of seizure.
- Documenting and recording the serial numbers of the seized devices and equipment, specifying their types, specifications, and any other accessories. With a statement of systems, programs, applications, and their data, if possible.
- Describing the manner and method of preserving and seizing evidence, and the place where it is stored until it is delivered to the examination and analysis authorities, along with documenting the Hash code and algorithm resulting from extracting similar and identical copies of E-evidence.
- In cases of seizure in which it is evident that there is encryption used on devices, equipment, data, information, or information systems, the examination shall be carried out during the seizure process and documented and evidenced in the minutes of seizure and initial examination. The ISO 27037 standard is used as a reference model for dealing with E-evidence".
- A need to strengthen cooperation with international organizations working in the field

of exchanging information related to Cybercrimes and E-evidence, such as Interpol and Europol, and to take advantage of the facilities they provide to countries to deal with this range of crimes.

- A need to strengthen international judicial cooperation through bilateral and multilateral agreements to facilitate the task of law enforcement officials in collecting and extracting E-evidence, especially in countries where the main servers of information networks are located.
- Moving forward in refining the capabilities of the human element dealing with E-evidence, including law enforcement officers and their assistants (police - prosecution - judiciary - experts) to enable optimal dealing with information technology crimes and the resulting E-evidence.

Conflict of interest

The authors declare no conflicts of interest.

Source of funding

The authors received no financial support for the research, authorship or publication of this paper.

References

1. Mahdi, A. Explanation of the General Rules of Criminal Procedure (In Arabic), Cairo, Dar Al-Nahda Al-Arabiya, 2003, p. 1277.
2. Arshad H, Jantan AB, Abiodun OI. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems. 2018 Apr 1;14(2).
3. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference 2013 Oct 23 (pp. 127-140).
4. Quéméner, M. Les spécificités juridiques de la prevue numérique AJ Pénal (1), 2014, p.63.
5. UNODC (United Nations Office on Drugs and Crime): Study on Cybercrime, New York, United Nations Organization, 2013, p.230.
6. Al-Saghir, J. Criminal Evidence and Modern Technology (In Arabic), Cairo, Dar Al-Nahda Al-Arabiya, 2002, p.11.
7. Voronin MI. Characteristics of electronic (digital) evidence assessment. Actual problems of Russian law. 2021 May 11;16(8):118-28.
8. Obeidat T. et al. Methods and Techniques of Scientific Research (In Arabic), Amman, Dar Sana'a for Publishing, 1996, p. 220.
9. Riabushchenko D. Conceptual and Theoretical Problems of the Category of "Digital (Electronic) Evidence" In the Criminal Process. Слава Україні! Героям Слава!. 2015 Oct 12:47.
10. Arshad H, Jantan AB, Abiodun OI. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Op. cit.;14(2).
11. ElKady R. Digital Forensic Evidence in the Egyptian Legislation: In light of the provisions of Law No. 175 of 2018 and its Executive Regulations, Comparative Legislation and International Covenants. Jolets [Internet]. 2022 Apr. 10 [cited 2023 Dec. 18];2(1):177-246. Available from: https://jolets.org/ojs/index.php/jolets/article/view/9
12. El-Kady RM. Investigating Forensic Evidence in Metaverse: A Comparative Analytical Study. In Forecasting Cyber Crimes in the Age of the Metaverse 2024 (pp. 227-258). IGI Global.
13. ElKady R. Explanation of the Law on Combating Information Technology Crimes No. 175 of 2018: compared to comparative legislation and international conventions (In Arabic), Cairo, Arab Studies Center for Publishing and Distribution, 2020, p.322.
14. Antwi-Boasiako, A. and Venter, H., 2017. A model for digital evidence admissibility assessment. In Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January

30-February 1, 2017, Revised Selected Papers 13 (pp. 23-38). Springer International Publishing.

15. UNODC. Study on Cybercrime, op. cit., p.230.
16. Gutmann P. Secure deletion of data from magnetic and solid-state memory. In Proceedings of the Sixth USENIX Security Symposium, San Jose, CA 1996 Jul 22 (Vol. 14, pp. 77-89).
17. Arshad H, Jantan AB, Abiodun OI. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Op. cit.;14(2).
18. Marie-Helen M. Computer Forensics: Cybercriminals, Laws, and Evidence.
19. Younis, O. Crimes arising from the use of the Internet (In Arabic), Cairo, Ain Shams University, Ph.D., 2004, p.977.
20. Naguib, H. The Authenticity of the Electronic Evidence (In Arabic), National Criminal Journal, Volume 57, Issue 1, March 2014, Cairo, National Center for Social and Criminological Research, 2014, p.52.
21. Ibrahim, K. Electronic Evidence in Criminal and Civil Matters (In Arabic), Alexandria, Dar Al-Fikr Al-Jamei, 2020, p.40.
22. Farghali, A. Criminal Evidence with E-evidence from the Legal and Technical Points - A Comparative Applied Study (In Arabic), Riyadh, Naif Arab University for Security Sciences, 2007, p.14.
23. Younis, O. Notes on Criminal Evidence via the Internet (In Arabic), Cairo, League of Arab States, the E-evidence Symposium organized by the League of Arab States, during the period (5-8 March 2006), p.14.
24. Naguib, H. The Authenticity of the Electronic Evidence op. cit., p.55.
25. 23- Farghali, A. Criminal Evidence with E-evidence from the Legal and Technical Points (In Arabic), op. cit., p.15.
26. Al-Husseini, A. Procedural aspects of crimes arising from the use of electronic networks (In Arabic), Cairo, Ain Shams University, Ph.D., 2013, p.157.
27. Abdul-Muttalib, M. Using the TCP IP Protocol in Researching and Investigating Computer Crimes (In Arabic), Dubai, Center for Research and Studies at the Dubai Police Academy, 2003, p.649.
28. Ahmed, H. A-A. The Authenticity of Computer Outputs in Criminal Evidence, Cairo, Dar Al-Nahda Al-Arabiya, 1 ed., 1997, pp. 14-22.
29. Minshawi, M. A. The Authority of the Criminal Judge in Appreciating Electronic Evidence (In Arabic), Journal of Law, Kuwait University, Volume 36, Issue 2, June 2012, p. 529.
30. Lawarem, W. The Digital Guide in the Field of Criminal Evidence According to Algerian Legislation (In Arabic), National Criminal Journal, National Center for Social and Criminological Research, Cairo, Volume 57, Number 2, July 2014, p.83.
31. Younis, O. Notes on Criminal Evidence via the Internet (In Arabic), op. cit., p.12.
32. Kent K, Chevalier S, Grance T. Guide to integrating forensic techniques into incident. Tech. Rep. 800-86. 2006.
33. Seo S, Seok B, Lee C. Digital forensic investigation framework for the metaverse. The Journal of Supercomputing. 2023 Jan 16:1-9.
34. Seo S, Seok B, Lee C. Digital forensic investigation framework for the metaverse, op. cit., p.9469.
35. UNODC. Study on Cybercrime, op. cit., pp.236-237.
36. Reilly D, Wren C, Berry T. Cloud computing: Pros and cons for computer forensic investigations. International Journal Multimedia and Image Processing (IJMIP). 2011 Mar;1(1):26-34.
37. Meunier, C. (2002). La loi du 28 Novembre 2000 relative à la criminalité informatique. Rev. dr. pen. Crim. P.664.
38. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. pp. 665-668.
39. Podovo, Y. (2002). This lot is against cybercriminalism in France. R.S.C. 2002, pp. 765-778.
40. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. pp. 676-677.
41. Al-Marsafawi, Hassan Sadiq (2000). Al-Marsafawi in the Principles of Criminal Procedure, Alexandria, Dar Al-Maaref facility, p.460.
42. Taha, Walid Nabil (2011). Cybercrimes according to the Budapest Convention, is a working paper presented to the symposium (Security Reality “Respon-

sibilities - Achievements") held on 1/9/2011, Police Research Center, Police Academy, Cairo, p. 29.

43. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. pp. 665-668.
44. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. pp. 669- 673.
45. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. P. 674.
46. Kaspersen, H.W.K. (1993). Computer crimes and other crimes against information technology in the Netherlands. Rev. int. Dr. pen. pp. 474-502.
47. Spreutels, J.P. (1993). Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en belgique : rapp. Rev. Int. dr. pen. pp. 161-170.
48. Piragaff, D.K. (1993). Computer crimes and other crimes against information technology in Canada., report, Rev. int. dr. pen., pp.201-340.
49. Meunier, C. (2002). La loi du 28 Novembre 2000, art. préc. pp. 669- 673.
50. Mianishi, K. Network of National Reference Points, The Sixth International Conference on Cybercrime, 13-15/4/2005, published by the Police Research Center, Cairo, pp. 95-98.
51. Rustom, H. M. F. Procedural Aspects of Information Crimes (In Arabic), Modern Machines Library, 1994, p. 34 et s.
52. Seo, S., Seok, B. & Lee, C. Digital forensic investigation, op. cit., p. 9481.
53. UNODC. Study on Cybercrime, op. cit., p.231.
54. Guttmann, B. (1996): Secure Deletion of Data, op. cit., p.25.
55. UNODC. Study on Cybercrime, op. cit., p.232.
56. UNODC. Study on Cybercrime, op. cit., p.232.
57. Chappell L. Wireshark® Certified Network Analyst Official Exam Prep Guide. Protocol Analysis Institute, Chappell University; 2012.
58. UK Association of Police Chiefs. (2012). ACPO Good Practice Guide for Digital Evidence, p. 6.
59. UK Association of Police Chiefs. (2012). ACPO Good Practice Guide for Digital Evidence, p. 6.
60. Marie-Helen M. Computer Forensics: Cybercriminals, Laws, and Evidence, p.377.
61. Naguib, H. The Authenticity of the Electronic Evidence op. cit., p.56.
62. Naguib, H. The Authenticity of the Electronic Evidence op. cit., p.56.
63. Minshawi, M. A. The Authority of the Criminal Judge in Appreciating Electronic Evidence (In Arabic), op. cit., p.552.
64. Al-Saghir, J. Criminal Evidence and Modern Technology (In Arabic), op. cit., p. 110.
65. El-Kady RM. Investigating Forensic Evidence in Metaverse: A Comparative Analytical Study. InForecasting Cyber Crimes in the Age of the Metaverse 2024 (pp. 227-258). IGI Global.
66. United States v. Meregildo, No. 11 Cr. 576 WHP, 2012 WL 3264501, at *2 S.D.N.Y. Aug. 10, 2012.
67. El-Kady R. Digital Forensics in Metaverse Technology, AJSS. Naif University for Security Studies. 2023;39(2):4–20.
68. US Department of Justice, E-evidence in the Courtroom Handbook, A Guide for Law Enforcement and Prosecutors, National Institute of Justice, 2007, p.16.
69. Greenfield, R. S. & Marcella Jr. AJ. Electronic Forensic Evidence, A Field Guide to Collecting, Studying and Preserving Computer Crime Evidence, Boca Raton, CRC Press, 2002, p.136.
70. El-Kady R. Digital Forensics in Metaverse Technology, AJSS. Naif University for Security Studies. 2023;39(2):4–20.
71. The case of Debtor American Express Travel Land Services v. Fei Vinhe Company, Session 16/12/2006.
72. Chaikin D. Network investigations of cyber-attacks: the limits of digital evidence. Crime, Law and Social Change. 2006 Dec; 46:239-56.
73. Al-Awjali, S. Admissibility of E-evidence in Criminal Courts, Journal of Legal Studies, Benghazi University, Libya, Issue 19, January 2016, pp. 31-40.
74. Sugisaka KL, Herr DF. Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual. Wm. Mitchell L. Rev.. 2008;35:1453.

75. Court of Cassation Judgment, on 5/5/2015, Appeal No. (31330) for the 83rd judicial year.
76. Court of Cassation Judgment, on 5/18/2000, Appeal No. (22340) for the 62nd judicial year, set of the Court of Cassation Judgments, p. 481.
77. Court of Cassation Judgment, on 3/14/1998, Appeal No. (16137) for the 67th judicial year, set of the Court of Cassation Judgments, p. 563.
78. UNODC. Study on Cybercrime, op. cit., p.15
79. Pinter, C. The threat posed by information crime and the need for international cooperation, Cairo, Police Academy, paper presented to the Sixth International Conference on Information Crime organized by the International Criminal Police Organization "Interpol", 13-15/4/2005, translated (into Arabic) by the Police Research Center, p. 66.
80. UNODC. Study on Cybercrime, op. cit., p.216.
81. Al-Shorbaji, A-B. Prospects and Mechanisms of International Cooperation against Crime (In Arabic), Cairo, Egyptian Judges Club, Judges Quarterly Magazine, Year 53, 2003, p. 10.
82. Al-Saghir, J. Procedural Aspects of Internet-related Crimes (In Arabic), Cairo, Dar Al-Nahda Al-Arabiya, 1999, p. 79.
83. Pinter, C. The threat posed by information crime op. cit., p.66.