# THE PROCEDURAL FRAMEWORK FOR THE ELECTRONIC BLACKMAIL CRIME IN THE JORDANIAN CRIMINAL LEGISLATION

**IbtIsam Al Saleh, Amman Arab University**


## ABSTRACT

*Investigating the electronic blackmail crime and how to seize and collect digital evidence from emerging topics in Jordan. The nature of digital evidence and how to deal with it by the investigation authorities is one of the issues of legal and practical importance. The Public Prosecution is investigating it, assisted by a judicial officer specialized in cybercrime, which is the Cybercrime Prevention Department in the Criminal Investigation Department, which exercises its jurisdiction according to the traditional rules of verification and evidence.*

*The problem of the study is represented in the difficulties raised by the electronic blackmail crime from a procedural point of view in terms of legislative shortcomings and the inadequacy of the Criminal Procedure Code of 2017 for the investigation and collection of evidence for this type of crime. The aforementioned law does not include texts explaining how to deal with digital electronic evidence, or its value in proof. Therefore, the study dealt with the investigation procedures and the most important methods of proof that pertain to the electronic blackmail crime, which is the digital evidence, by defining it and determining what it is, and the difficulties that the investigation authorities face in considering the evidence Digital and dealing with it as proof.*


**Keywords*:*** Blackmail Crime, Criminal Proof, Digital Evidence, Investigation

## INTRODUCTION

Electronic blackmail is a process of threatening and intimidating the victim by publishing pictures or film materials or leaking confidential information belonging to the victim. This is in return for paying money or exploiting the victim to carry out illegal acts for the benefit of extortionists, such as disclosing confidential information about the business or other illegal acts. Victims are usually trolled by e-mail or various social media such as Facebook, Twitter, Instagramand other social media due to its wide spread and great use by all segments of society. Electronic blackmail operations are increasing in light of the growing number of social media users and the acceleration witnessed in the number of different chat programs.

The Electronic blackmail crime, like other crimes, passes after its occurrence, and in the stage of inference and criminal investigation, which aims to reach the discovery of the crime and its perpetrator, and to stand on all the facts and circumstances that the crime has undergone, and its perpetrator, whether he is a sole perpetrator of the crime or they were perpetrators of it, and all this research And the investigation is one of its most important goals to reach the truth. The legal truth needs evidence to confirm the attribution of the accusation to the accused, or the denial of the crime from him, and perhaps in order to complete the privacy of this crime. We had to admit that the evidence in the electronic crime, and especially in the electronic blackmail crime, is unconventional evidence, evidence related to computers, mobile phones and accessories, software and technological applications. In the electronic blackmail crime, the evidence is symbols, codes, devices and electronic addresses, and these evidences have a heroic role in the proof that passes through There are many stages, including the stage of legal evidence, and the legislator is the one who determines for the judge the evidence that he may accept in a particular case and prohibits him from accepting other evidence.

**Initial Investigation Procedures**

The procedures for investigating the blackmail crime are similar to the procedures for investigating the traditional crime, in that both require inspection, inspection, interrogation, evidence collection and examination, (except that one of the most important rules that the investigator must be keen on preserving the evidence that was seized at the crime scene from tampering or losing it (Hassan, 2012).

What is meant by investigation: "It is the set of procedures carried out by the investigator, which lead to the discovery of the crime and the knowledge of the perpetrator, in preparation for his submission to the trial in order to receive his punishment. These procedures may be practical, such as inspection, or technical, such as fingerprinting, or software to determine how to access data stored in computers (Al-Mutairi, 2015).

## Preview

Inspection means the careful and careful examination of the scene of the accident and related objects and persons, carried out by the investigator or one of his assistants. This is with the intention of collecting evidence and proving the status of each of the crime scene, the person of the accused, the victim, and the things related to the crime that took place (Abbas, 2008).

Examination in its legal meaning for electronic crimes does not differ from its prevalent meaning in the jurisprudence of criminal procedures. It is one of the investigation procedures carried out by a competent authority in order to access the automated data processing systems, including its inputs, storage and outputs, in order to search for illegal acts that have been committed and constitute a felony or misdemeanor, and through this to find evidence that proves the crime and attributes it to the perpetrator (Ahmed, 2021).

In the electronic blackmail crime, we talk about the inspection of automated processing systems, which includes all the intangible elements necessary for the operation of the physical entity, such as programs, operating systems and databases.

Thus, we find that inspection is less important in the electronic blackmail crime than in the traditional crime, due to the lack of material effects left by the offender when committing the crime, due to the long period of time between the commission of the crime and its discovery, which makes the offender manipulate evidence and traces to obliterate the features of his crime (Maamesh & Ghanem, 2013).

## Inspection

It is the search for evidence and things related to the occurrence of the crime in the defendant's residence, or searching for it in his clothes, the things he wears, or the tools. The search, then, is the search for the truth in the secret repository that he uses, and it is an investigative procedure owned by the investigation authority and infringes on personal freedoms, and therefore it is not permissible to conduct it unless its cause

The principle in the law is that the search warrant is one of the investigation procedures that may not be issued except after the occurrence of a felony or misdemeanor and its attribution to a specific accused is likely. Besides, there are strong signs or presumptions that there are things that are useful in revealing the truth to the accused or others. Therefore, two conditions are required for the search according to Article 81 and Article 34 Criminal Rules.

1) Committing a crime: If it becomes clear from the nature of the crime that the documents and things in the defendant's possession may be evidence of the commission of the crime, the public prosecutor, or whoever he designates, may move immediately to the defendant's residence to search for the items he deems leading to revealing the truth.
2) Existence of evidence against a specific person. The search may not be carried out unless the investigator has sufficient evidence that the place or the person to be searched has tools that were used in the commission of the crime, items obtained from them, or any electronic documents or documents that may be useful in clarifying The truth about the person accused of the crime. And the signs mean; Certain signs

based on reason and starting from circumstances or facts from which it can be concluded that a crime has occurred, and that a specific person is the perpetrator of it, and then they are just assumptions that may not alone be a reason for conviction, but they justify taking some measures affecting individual freedom in order to ensure the proper course of justice (Farghali & Al-Mismari, 2007).

The Jordanian legislator has determined the powers of the judicial police to enter places, inspect and seize devices and operating systems, and authorize the inspection through two conditions:

1) The objective conditions for inspecting the information system for evidence of its use in any of the crimes stipulated in the law.
2) The formal conditions and these conditions must be observed when conducting the search, in order to preserve individual freedoms and rights, and they are represented in obtaining the permission of the public prosecutor or the competent court, and then the judicial police assistants must organize a seizure of the seized items and submit them to the public prosecutor. In the inspection, it is necessary to:

Therefore, Article 13 of the Cybercrime Law No. 27 of 2015 states:

A. Subject to the terms and conditions stipulated in the legislation in force and taking into account the personal rights of the defendant, the judicial police officials may, after obtaining permission from the competent public prosecutor or the competent court, enter any place that evidence indicates that it was used to commit any of the crimes stipulated in. They may also inspect devices, tools, software, operating systems, the information network, and the means that indicate their use to commit any of these crimes. In all cases, the employee who conducted the inspection must organize a report of this and submit it to the competent public prosecutor.

## Setting

Seizure is of great importance in the field of criminal proof of electronic evidence, in terms of the seizure record, it only responds to material things because intangible things are not suitable to be the subject of seizure. The necessary condition for the validity of the seizure is that the thing is useful in revealing the truth. It is suitable to control it just as it only responds to things. As for people, it is not suitable for a place of control, but the more correct term is arrest and arrest is completely different from controlling things (Abu Al-Wafa, 2006).

The purpose of the search is to seize objects, and it is intended to lay hands on something related to a crime that has occurred, which is useful in revealing the truth about it and its perpetrator, and in terms of its legal nature, it may be one of the investigation or inference procedures, and this is determined according to the method in which the seized thing is seized. If the thing at the time of its seizure was in the possession of a person and it was necessary to strip it of its possession, then the seizure was an investigation procedure.

In the seizure, it must have been taken for a specific purpose, which is to reveal things related to electronic crime or useful in revealing the truth and taking into account the removal of suspects from the crime scene - the location of the devices that contributed to the crime events - so that all electronic devices related to the crime are inspected and components and data are known It is useful in revealing how the crime occurred by identifying the contact number or the transfer, copying or destruction of the information and data. It is thus possible to set a standard specifying the things that may be seized as “all things – whatever their nature – that the investigator estimates are useful In revealing the truth, “the criterion is the link or link between the thing and the crime, and the investigator must extract evidence of conviction or innocence from it (Mustafa, 1988).

The dispute arose in the comparative legislation in the matter of controlling and inspecting the moral components or the inspection of the computer. Opinions varied in this regard, and the opinion went that if the purpose of the inspection is to seize the physical evidence that is useful in revealing the truth, then this concept should be extended to include electronic data to give the investigation authorities the possibility to do anything that is necessary to collect and protect the evidence, which means seizing the stored data or Processing automatically and electronically in

his internal memory. This is done by giving the investigator an order to the expert to collect data that can be accepted as evidence for criminal prosecution._ (Youssef & International Internet Crimes, 2011).

## Article 13/b of the Cybercrime Law states

B. Subject to Paragraph (A) of this Article and the rights of others in good faith, with the exception of those licensed in accordance with the provisions of the Telecommunications Law who did not participate in any crime stipulated in this Law. Judicial police officials may seize devices, tools, software, operating systems, the information network, and the means used to commit any of the crimes stipulated or covered by this law, and the funds obtained from them, and seize information and data related to committing any of them.

Discipline must be useful in revealing the truth. To accomplish this, the Public Prosecution issues the warrant for the search, which permits the search of the device or devices involved in the crime and all computer data and components, provided that the permission is precisely and clearly defined in terms of the location of the search (the crime scene), the person's address, his description, and the things being searched. It is mentioned that the search in electronic crimes, including Electronic blackmail, deals with accessing a computer or phone and seizing the data and information it contains that are useful in accessing the crime leads. Through these procedures, the control is carried out so that the seized information and electronic data and the evidence obtained from the seizure process are entered, classified and kept in the envelopes and boxes prepared for this, and they are distinguished by marking them, then the process of examining the evidence that was found and trying to try it through other devices until The original evidence is not compromised by professionals specialized in this type of crime. All these procedures are documented in the investigation report on the date and day on which it was carried out so that it includes all the information and procedures that were carried out in order to uncover the circumstances of this crime.

## Hearing of Witnesses

Testimony is the witness's acknowledgment of something he witnessed, heard, or perceived by any of his senses, and thus deviates from the concept of testimony the witness's personal beliefs and opinions and the extent of his appreciation of the gravity of the incident or his appreciation of the extent of the defendant's responsibility. The public prosecutor must listen to the testimony of anyone who has information about the crime he is investigating, which was confirmed by Article 68 of the Jordanian Code of Criminal Procedure (Al-Abdullah, 2020).

And testimony does not differ in its meaning from that related to electronic crime, as the matter of hearing witnesses remains left to the intelligence of the investigator, and is linked to the circumstances of the investigation and what results from it. The principle is that the litigants ask whom they see as witnesses, and the investigator may call for testimony those whose testimony is deemed important and he has the right to hear any witness who comes forward on his own Himself (Dia, 1984).

The witness in the electronic blackmail crimes is that technical person with expertise and specialization in computer technology and science, and who has essential and important information necessary to access the automated data processing system, if the interest of the investigation requires the search for evidence inside it. This witness is called the informational witness, in contrast to the traditional witness (Saedani, 2013).

As for the technical witness, it may be one of the following categories:

1. Computer operators who are responsible for operating the computer and related equipment.

**2. Programmers are Specialists**

Among the technical and professional rules for hearing testimony, the public prosecutor must take into account the formalities required by the legislator when listening to the testimony of any witness. Among these rules is to verify the identity of the witness by reviewing it and

clearly confirming the name, age and address of the witness and the extent of his knowledge of the parties to the case, reading the testimony to the witness, his signature on each of its pages, or putting his fingerprint on it if he is illiterate, and the signature of the public prosecutor and his writer on each page of the testimony (Kander, 2202).

## 3. The difficulties facing the investigation bodies in the blackmail crime

The investigation of blackmail crimes is not an easy matter because of the difficulties facing the investigator in front of a crime that is still mysterious, and surrounded by many obstacles, so that the inability to control the course of the investigation may lead to a loss of confidence in society and an increase in the crime rate. Perhaps we can list the difficulties that the investigation authorities may face, as follows:

### The Human Right to Privacy

Many legislations in countries criminalize the infringement of a person's private life by using the Internet. It was stipulated in the Charter of the United Nations in 1948, including Article 15: "No person shall be subjected to arbitrary interference with his privacy, family, home, or messages, or to launch campaigns against his honor and reputation. Every person has the right to seek the protection of the law from such interferences or campaigns."

And all the international human rights declarations affirmed their keenness to protect privacy and private life, and Arab constitutions and regulations ratified what these declarations said.

The Jordanian constitution stipulates in Article 18 that the freedom and confidentiality of postal and telegraphic correspondence and other means of communication are guaranteed." It is not subject to monitoring, inspection, arrest or confiscation except by judicial order in accordance with the provisions of the law.

### Lack of Experience of Employees Working in the Investigation Authorities

The investigation bodies still suffer from a lack of technical expertise for their staff. As well as the lack of training in dealing with digital evidence, how to search for it, and how to obtain this evidence, which is a major gap in the criminal system. Modern technology has language and vocabulary that must be learned and used. Also, the experience of interrogating an intelligent and knowledgeable criminal such as the criminal in Electronic blackmail crimes has a special nature, especially since this criminal eludes and tries to escape from his crime, perhaps by drowning the investigator in details he does not know well, as the criminal investigator in Electronic blackmail crimes must have a different skill formation, Where he must combine the skill of using modern technology. As well as the skill of evaluating cybercrime and the extent of the criminal risk of its perpetrator, and whether he is an amateur criminal or is involved in the crime and has a criminal record in it. This acquired experience helps justice to quickly access the criminal, as well as the skill of identifying the hardware components of the devices and the ability to identify their accessories such as printers, scanners and cameras, in order to ensure their connection to the original device or not, and to evaluate the media for storing digital evidence to determine the extent of its connection to the Internet and whether it is part Of the tools of crime or not. The investigator must also know the basic systems for the work of networks, as well as distinguish the operating systems of different computer systems (Al-Bishri, 2004).

### Physical Evidence does not Appear

Most of the traces left by electronic crimes, including the blackmail crime, are electronic traces, and these traces are electronic impulses that are not visible to the naked eye. It is almost non-existent in size and shape so that it can only be seen through the use of technical devices and means that make it visible (Mansour, 2002). The huge volume and quantity of electronic data and files that exist in the electronic environment makes it difficult to identify criminal electronic files and data, among that huge amount to separate them from innocent ones. It often leads to the discovery task clashing with the right of individuals to personal privacy, and the information environment is often composed of networks spread all over the globe and linked to each other through the Internet, so that it provides the opportunity for the information criminal to remotely access the electronic data stored in Any part of the world (Al-Tamimi, 2019).

The reason for the lack of traditional effects of the blackmail crime is that there are some processes whose data is entered directly into the computer without that depends on the documents or documents from which it is transferred, as if the program was prepared and stored on the computer. Thus, the means by which the electronic crime is committed is placed within an unconventional template, since it is committed by transmitting information in the form of invisible electronic impulses that flow through parts of the computer and criminal entities benefit from the material traces and landmarks through which it can be inferred that the occurrence of a material crime is attributed to a specific person or persons. (http://aitmag.ahram.org.eg/News/86864.aspx)

This is what prompts us to say that the concept of digital evidence is limited to what is extracted from the computer and from other evidence such as telephones, photocopiers and other digital evidence and devices that rely on digital technology in their operation so that they are a source of electronic evidence.

## Evidence in the Blackmail Crime

### The Concept of Criminal Proof

Evidence is defined as establishing an argument, proof and evidence, and it is the predominant suspicion, but it does not reach the degree of certainty that does not accept doubt. Evidence has several uses, including that it is a means used to prove a fact, as well as a means of defense if the evidence is in favor of the accused, and to show the truth of an act committed by the plaintiff. The accused denies that proving the criminal incident is the axis around which the search for the perpetrator of the crime revolves, and what the security services target. Criminal proof is intended to establish evidence of the occurrence of the crime and then attribute it to the accused of committing the crime, and the evidence in traditional crimes is different from the evidence in electronic crimes, and this privacy it is manifested in the digital evidence that characterizes cybercrime (Qawari & Ghanem, 2020).

As for criminal proof, it is: a procedural activity directed directly to obtaining judicial certainty according to the criterion of factual truth, regarding an accusation or other affirmation or denial, upon which a judicial procedure depends. In other words, it is: establishing evidence of the occurrence of the crime and attributing it to a specific perpetrator (Al-Sanad, 1998). The evidence aims to indicate the extent of congruence between the legal model of the crime and the presented incident; In order to do so, he uses certain means, namely the means of proof, and the means of proof, which are: everything that is used to establish the truth - it is an activity that is made in order to discover a situation, issue, person, thing, or something that is useful in showing the various elements of proof - *i.e.*, the evidence - Transferring it to the tangible realm (Tawalbah, 2009).

As soon as the crime has occurred, criminal police and investigation officers begin to collect inferences for the purpose of establishing evidence, searching for the culprit, and investigating different Electronic blackmail crimes, which require experience in dealing with digital crime evidence, despite the different electronic crimes in general from traditional crimes,

which places a burden The investigation authorities should adapt the investigation procedures to suit the investigation of electronic crimes in general, and electronic blackmail in particular. Also, the system of criminal procedures in the rules of investigation in the system of criminal procedures prevails, with the need to consider the objective differences in the investigation, as there are Difficulties raised during the investigation stem from the nature of the blackmail crime. Evidence in blackmail crimes is not an easy matter because of the difficulties facing the investigator in front of a crime that is still mysterious, and surrounded by many obstacles, so that the inability to control the course of the investigation may lead to a loss of confidence in society and an increase in the crime rate. The electronic blackmail crime, like other crimes, passes through the stages of inference after its occurrence (Swilam, 2019).

## Forensic Digital Evidence

### Concept of Forensic Digital Evidence

The digital evidence means that it is "evidence taken from computers and it is in the form of magnetic fields or electrical impulses that can be collected and analyzed using special programs, applications and technology (Al-Hawamdeh, 2016).

He defined it as "a set of data or information that is able to prove that a crime has occurred or that there is a link between the crime or the offender or the existence of a relationship between the crime and the victim. Then this aspect of jurisprudence gives a definition of digital data as "a set of numbers that represent all information, including sound, images, and written texts" (Al-Hamdani, 2016).

The reason for calling this evidence digital is that the data inside the virtual crime scene, whether images or recordings, take the form of numbers inside computers, in the form of digital (0,1) with a specific coding so that these symbols can be converted upon display to an image or recording (Al-Assadi, 2015). And electronic evidence is also defined as evidence that includes all digital data that can prove that a crime has been committed or that there is a relationship between the crime and the victim of it, and digital data is a set of numbers that represent various information including (written texts/graphics/Maps/Audio/Photo (Al-Hawamdeh, 2016).

We define electronic evidence as: "evidence derived from or by computer software and information systems, computer hardware, equipment and tools or communication networks through legal and technical procedures to be submitted to the judiciary after scientific analysis or interpretation in the form of written texts, drawings, images, shapes and sounds to prove the occurrence of crime or to determine innocence and conviction therein.

### Characteristics of a Digital Guide

**First**: The digital evidence is evidence that has its own environment in which it is located, and this environment is a virtual environment, and it is characterized by several characteristics, and we present them as follows: Evidence or change it. The digital evidence is extracted from a complex environment, which is the virtual world, and it is not possible to extract that evidence except by scientific means through information laboratories

**Second**: The evidence produced by electronic devices is characterized by its high speed when moving in the communication network, and the expert can copy the digital evidence several copies so that they are identical to the original, and have the authority of proof and scientific value as the original itself. This is what distinguishes the digital evidence from the traditional evidence, and this method has a guarantee against manipulation, tampering and distortion of the original (Farghaly & Al-Mismari, 2007).

Third: Through the digital guide, it is easy for the competent authorities to monitor the cybercriminal, search for him, and know his personal information

Fourth: The digital evidence is not seen through the natural senses of the human being, because it consists of electrical impulses that cannot be touched. It is intangible evidence, that is, non-material. Therefore, translating the evidence into material and tangible does not change its digital character, because converting it from digital to the form of the body is inferred. It is based on specific information, and some say that the digital evidence is less material than the physical evidence, but their saying is incorrect because it depends on imagination in its form and the location of its indefinite existence and its size (Al-Bashri, 2015).

The rule in criminal or criminal cases is that it is permissible to prove by all legal methods of proof. The plaintiff has the right to prove his claim in all these ways, and the judge has the right to form his conviction from any evidence, indication, or procedure submitted to him, or he examines it himself. Then the necessity required restricting the means in a number of ways, and the restriction on this rule: that the evidence must be one of the evidence accepted by the law, and thus shows the importance of the law's recognition of evidence of an electronic nature. And information, though its value more and more exceeds assets and energy; It is not material to accept evidence in proof, and its storage media - other than paper as output - does not receive in terms of its content acceptance as material evidence, hence the legal research in many countries tends to recognize the legal validity of computer files and extracts and electronic messages with informational content not in its image placed within A physical vessel, but of a purely electronic nature (Al-Hiti, 2015).

Evidence with modern technologies is considered authoritative in writing, electronic documents and signatures, and therefore it is taken from this that these electronic documents are considered as evidence that can be invoked in the event of a dispute. Dr. Yunus Arab says: Evidence of an electronic nature must be equated with evidence of a physical nature - evidence based on writing and paper - in terms of admissibility and authenticity. Whenever the physical behavior in the real environment is considered, the corresponding moral behavior in the digital environment must be acknowledged, as the electronic signature requires its equating with the physical signature. And electronic certification must be equated with physical certification, and so on, provided that the digital environment is achieved in terms of standards and procedures related to intangible behaviors or the behavior of the virtual environment, which provides the confidence that physical behaviors possess) from criminal means dominated by this modern technical character (Al-Husseinawi, 2009).

The researcher believes that he should accept the evidence derived from the computer to prove the facts of the case that deal with information crimes, and he is helped in this matter by the general methods, rules and principles of proof, and the personal conviction of the judge in the criminal field. On the other hand; The judge should have the ability to legally adapt the new criminal acts, with the existing penal/criminal legislation, and despite the recognition of the privacy of electronic crimes, including the blackmail crime, but it is still a prohibited act that constitutes criminal behavior that the contemporary legislator has criminalized, and stipulated his punishment, stressing this penalty in Certain conditions and for reasons stipulated. Therefore, the competent authorities in detecting crime can obtain digital evidence in the traditional crime scene or virtual theater by extracting evidence from the devices.

**Difficulties Facing Digital Forensic Evidence**

Among the difficulties encountered in the digital evidence, the difficulties that the authorities face in proving the use of digital evidence vary, due to many reasons, including:

**First**: Ease of erasing the evidence, as the perpetrators after committing the crime are keen, especially since the cybercriminal, in the crime of extortion, after threatening the victim, erases the traces of his crime, which makes access to evidence difficult, and sometimes impossible (Al-Afifi, 2013).

**Second**: Obstacles related to revealing the identity of the perpetrator through the digital evidence. The electronic blackmail crime differs from the traditional blackmail crime, in that the

first takes place in a virtual world governed by symbols and data, devoid of violence and physical effects such as the traditional blackmail crime, which makes it difficult to reach physical evidence such as a fingerprint, or a point of blood, which makes access to the offender objected to obstacles, including obstruction of access To the evidence Sometimes the offender puts technical obstacles to prevent the detection of his crime and the discovery of its evidence, such as encryption systemswith the intent of blocking information from public circulation, and preventing access to the source of the transmission.

**Third**: The lack of experience of some workers in the investigation authorities. Among the difficulties facing the process of obtaining digital evidence in the electronic blackmail crime is the lack of experience among some employees of the criminal police and members of the investigation bodies, with regard to computers and their accessories, computer language, and skills related to interrogating a smart criminal such as the electronic criminal in the blackmail crime (Jerada, 2009).

**Fourth**: Difficulties related to the victim's reluctance to report the blackmail that he is exposed to.

The researcher believes that it is necessary to pay attention to training and qualifying the human element, such as investigators and support agencies, in order to keep pace with the rapid progress in matters of electronic crime in general and electronic blackmail in particular. One of the difficulties is the reluctance to report from the victim: the reason for this is due to the victim's fear of reporting so that his matter will not be exposed. This crime was committed mainly because of the victim's fear that his secrets would be revealed, and therefore this reluctance helps to disappear the digital evidence that indicates the offender, which makes this reason a serious obstacle standing in the way of proof through digital evidence. As well as the absence of a unified legislative mechanism: as the different legislation, in criminalizing the acts of electronic blackmail, is different in one country from another, which makes the prosecution of the offender pass through obstacles and obstacles, what one country sees as permissible, another considers criminal. We see the urgent need to establish unified international criminal legislation, more Flexibility to keep pace with the pace of progress in cybercrime.

We also find the difficulties that pose a challenge to prove blackmail through the forensic digital evidence the availability of technical expertise when detecting and verifying the digital evidence, as expertise is a procedure related to a subject that requires knowledge of a specific science or art in order to extract evidence from it. Therefore, the experience assumes the existence of a material thing or fact that can be memorized from it. Experience is one of the means of direct evidence in which the judiciary resorts to others to seek assistance in technical matters that are difficult for him to know in order to reach a discovery.

## RESULTS

Electronic blackmail crime is one of the new crimes, and it is called in criminology soft crimes, which are devoid of violence, and it is one of the forms of electronic crime, and Electronic blackmail is the other side of the traditional blackmail crime that arises and is committed in a physical world, and in a traditional crime scene, where the offender leaves a fingerprint, Or a drop of blood, while Electronic blackmail takes place in a virtual world full of symbols and ciphers. The challenge grows when we find the obstacles and difficulties that the investigation agencies face in investigating them and in dealing with the digital evidence. In our study, we reached a number of results, which we list as follows:

1) The rules of the Code of Criminal Procedure that dealt with the investigation of traditional crimes are prevalent when investigating the electronic blackmail crime, with the need to consider the objective differences in the investigation, as there are difficulties that arise during the investigation stemming from the nature of this crime.
2) Electronic blackmail crime has privacy in the investigation, and it requires a team of specialists or qualified and trained to absorb recent developments in the investigation with an intelligent criminal who has different characteristics from the traditional criminal

3) In the electronic criminal proof of the electronic blackmail crime, the evidence extracted from the electronic means, which is called the digital forensic evidence, is relied upon, as the search for evidence is the goal sought by the justice systems, and in order to search for this evidence, it is actively seeking and diligently searching for everything that may arise on the Crime scene from evidence, whether in traditional or electronic crime,
4) The electronic blackmail crime is a crime that is difficult to prove, as it is easy to erase its traces easily, and it requires hard work until it is proven.
5) The digital evidence is the most important evidence in the blackmail crime, but dealing with it requires certain expertise, specialized devices and an integrated work team.

## REFERENCES


Al-Tamimi, D. (2018). *Electronic blackmail crime/Comparative study*. Master's thesis, Faculty of Law, Al-Quds University.

Muhammad, M.I. (2002). *Cybercrime in Islamic Sharia and Man-made Laws*. Dar Al-Nahda Al-Arabiya, Cairo.

Rahman, H.A. (2012). *Modern evidence and its role in criminal proof*. Unpublished Master's Thesis, Middle East University.

Marzouk Al-Mutairi, S. (2015). *Criminal responsibility for electronic blackmail in the Saudi system*. Unpublished Master's Thesis, Naif Arab University, Riyadh.

Tawfiq, A.A. (2021). *Explanation of criminal procedures*. House of Culture for Publishing and Distribution, Amman.

Hussein, A.A. (2008). *Criminal evidence and cybercrime*. Research Presented to the Second Regional Conference on Intellectual Property Applications in the Arab World, two days, 4/27/2008, Arab League headquarters.

Maamesh, Z., & Ghanem, N. (2015). *Criminal Evidence in Information Crimes*. unpublished master's thesis, Algeria, unpublished master's thesis, Riyadh.

Farghali, A., & Al-Mismari, M. (2007). Criminal proof with digital evidence from the legal and technical perspectives: An Applied Comparative Study, the First Arab Conference for Forensic Sciences.

Mahmoud, M. (1988). Explanation of the code of criminal procedure, Cairo, Dar Al-Nahda, Cairo, 1988

Hassan, Y. (2011). *International internet crimes*. National Center for Legal Publications, 2011

Saidani, N. (2013). *Mechanisms of research and investigation of information crime in Algerian Law*. Unpublished Master's Thesis, Hadj Lakhdar University, Algeria.

Al-Amin Al-Bishri, M. (2004). Investigation of Newer Crimes. Riyadh.

Ali Swailem, M. (2019). *Combating Cybercrime*. University Press, Cairo.

Al-Hamdani, M. (2016). *The legitimacy of electronic evidence in criminal evidence*. Research published in the Journal of the College of Law, Al-Nahrain University, Iraq, *18*, 2.

Saeed Al-Hawamdeh, L. (2016). *Information crime*: *Its Pillars and Mechanism for Combating it*. Research published in Mizan Journal, University of Islamic Sciences.

QaderJarada, A. (2008). *Encyclopedia of criminal procedures in Palestinian Legislation*. Afaq Library, Gaza.

Khalil Al-Afifi, Y. (n.d). *Cyber crimes in the Palestinian Legislation*. An unpublished master's thesis, the Islamic University, Gaza.

Hammad Al-Hiti, A. (2015). *Modern technology and criminal law*. House of Culture for Publishing and Distribution, Amman.

Jabbar Al-Hussainawi, A. (2009). *Computer and internet crimes*, Al-Yazuri Publishing and Distribution House, Amman.

Electronic websites.