Pakistan Journal of Criminology
Vol. 15, No. 03, July-September 2023 (29-44)

Digital Forensic Challenges in Jordanian Cybercrime Law

Noor Al-Khawajah[1], Tareq Al-Billeh[2]
& Majd Manasra[3]

Abstract

The research paper aims to establish the legal restrictions governing digital forensic analysis in cybercrimes, examine the methodology employed, and assess them from a legal standpoint. The study and evaluation of the legal systems in place in several developed nations in this area, as well as a thorough review of the legal literature and legal suggestions relevant to the field of digital forensic analysis in cybercrimes, were done. Digital forensic analysis is the practice of employing digital tools and technology to look into cybercrimes while maintaining fairness. Globally accepted legal rules are adhered to, ensuring that access to the digital evidence necessary is obtained in compliance with existing laws and obtaining a search warrant or other legal permission in order to maintain justice and moderation in this process. Digital evidence must be stored and recorded in a secure and trustworthy manner. This entails preventing the manipulation or change of evidence, guaranteeing its integrity and confidentiality of information, and checking the veracity of evidence and the legality of the technique used to gather it.

Keywords: digital evidence, forensic analysis, cybercrimes, detecting digital crimes, Information document

1. Introduction

The practice of employing digital technologies and tools to gather, examine, and interpret digital evidence from computers, phones, internet networks, and any other digital device as evidence in cybercrime cases is known as "digital forensic analysis." Additionally, the goal of digital forensic analysis is to examine legally accessible electronic evidence, gather digital data, and identify offenders of cybercrimes in order to give the necessary legal evidence for protection under the law. Identification of the digital criminal, data recovery from

[1]The Author is a Lecturer at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan. MEU Research Unit, Middle East University, Amman, Jordan. He can be accessed on n_alkhawaja@asu.edu.jo
[2]The Author is an Assistant Professor at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, and the author is a practicing lawyer in Jordan as well. He can be accessed on t_billeh@asu.edu.jo
[3]The Author is an Associate Professor at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, and the author is a practicing lawyer in Jordan as well. MEU Research Unit, Middle East University, Amman, Jordan. He can be accessed on m_manasra@asu.edu.jo

deleted files, analysis of the attack strategy, and monitoring of suspects' online activity are all included in the study of digital evidence. An essential step in the criminal investigation of cybercrimes is digital forensic examination (Al-Hajjar& Bashir, 2021).

As a result of technological advancement and the extensive use of social media and the Internet in the modern era, cybercrimes have substantially increased. Digital forensic analysis has therefore become crucial to preventing these crimes and delivering digital justice. Therefore, the rapid development of technology, which contributes to the complexity of cybercrimes and the difficulties in their analysis, is one of the most significant issues facing the criminal process in the field of digital forensics. Additionally, the variation in cybercrime laws and regulations among nations may make it challenging to gather evidence and utilize it against the accused (Fatih & Awwad, 2017).

The most significant of the many questions raised by this study is: What role can digital forensic analysis play in the fight against cybercrime? What instruments and methods are employed in the digital forensics' procedure? What difficulties do digital forensics procedures face, and how may they be resolved? What is the importance of international cooperation in the field of digital forensics and combating cybercrimes?

The study in the field of digital forensic analysis is of great importance for several reasons, including combating cybercrimes, as digital forensic analysis contributes to detecting cybercrimes, identifying the accused, and bringing them to justice. And data protection, as it helps protect personal data and information from hacking and illegal exploitation. And consolidating digital confidence, as it enhances confidence in the use of technology and the Internet by providing digital justice and protecting the digital society.

This study aims to identify the methods and tools of digital forensic analysis, assess the effectiveness of their use in combating cybercrimes, identify the challenges facing the process of digital forensic analysis, propose appropriate solutions, and explore the importance of international cooperation in the field of digital forensics and its role in combating cybercrimes.

2. Methodology

For this reason, the study adopted a descriptive and analytical approach. Through the descriptive approach, the position of the Jordanian legislator will be described by listing the various rules related to the importance of digital forensic analysis in the field of combating cybercrimes , indicating the tools and techniques used in the digital forensic analysis process, an explanation of the challenges facing the process of digital forensic analysis and how to overcome them, and an

explanation of international cooperation in the field of digital forensic analysis and combating cybercrimes.

In this study, an analytical approach based on reviewing academic sources and interviews with experts in the field of digital forensic analysis will be used, along with analysis and evaluation of the legal systems in force in some developed countries in digital forensic analysis of cybercrimes.

3. The Importance of Digital Forensic Analysis in Combating Cybercrimes

Digital forensic analysis is of great importance in the field of combating cybercrimes. Digital technology has become an integral part of our daily lives; however, the crimes that are committed using technology have also increased. Here are some of the benefits of digital forensic analysis:

3.1 Crime Detection: Digital forensic analysis helps detect cybercrimes and identify digital evidence related to them. By analyzing the digital data stored in electronic devices and networks, acts of hacking, data theft, and information manipulation can be identified (Al-Husseini, 2012; Al-Billeh, 2022a).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023) , dated 8June 2023 that: "In order for the crime of electronic forgery to take place, the information document must be prepared for proof, just as the forgery occurs in a written document in a specific language or In the manner of the image, it may fall into any of the computer extracts, even if it was printed on any unusual medium, including magnetic and recorded tapes, and what includes an image, or if the image had an effect in the information document that arranges a specific right or effect, as these tapes, which are magnetic and recorded on the paper extracts, are distributed. Information forgery crime is represented by the illegal activity that focuses on the data stored electronically in the information system with the aim of modifying it, whether by adding, deleting, modifying, or proving data contrary to the truth, such an act would cause harm to others" (The Jordanian Court of Cassation, 2023).

3.2 Evidence Collection: Digital forensic analysis collects digital evidence with the aim of proving or denying cybercrimes by analyzing data on devices, networks, and digital platforms, as evidence is extracted that can be used in prosecution (El Mahlawy, 2016; Al-Billeh, 2022b).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023), dated 8June 2023 that: "Whereas the Public Prosecution provided its evidence, which was represented by the testimony of the female witness (‘A), by virtue of her professional position as the head of a health center and she was the vaccination officer in that center, and she had a special username for managing the stock of vaccines, and one of her tasks was to report on the

numbers of people who received the vaccines, and while she was looking at the reports, it turned out that there were people vaccinated with the Pfizer type, which was prohibited on that day. It turned out that her username was used in order to enter some people who had to receive the vaccine, but they did not receive the vaccine, and they were recorded as having received the vaccine, and it turned out that her username had been hacked, and that the password at the beginning of the vaccination campaign was for all employees, and then each holder of authority was given a password, and he/she had the authority to change it, but it is known to all and accessible to everyone (a group of vaccination officers) in the Kingdom. And it is possible for anyone in the group to know the password of any username of any of the liaison officers within the group after making a (reset) for that username, and that the number of group members exceeded 100, and it was possible for any of the liaison officers to know the password of any liaison officer who made a reset for his/her username, and this can be changed, and this reset worked for any liaison officer who had a problem, and the word (reset) means resetting the original password. And that (Reset) was done on 9/14/2021, and it was possible for any normal person or liaison officer in the group, if he/she knew the national number of the liaison officer and the original password, to open the program and do anything, and that the person who entered the password of the witness (‘A) on 9/16/2021 did not change the password, as she was able to enter her password, and the person who issued the vaccination certificates he/she entered the public (original) password, and he/she may be from outside the group, and the information may have been leaked to him/her, and that the accused have been referred to the trial because of the use of the username of the female witness, and that the paper statements proved that they did not receive the vaccine, and it was possible that a defect occurred in the paper statement and it was not entered into in the electronic statement and that the list approved in the Crisis Cell is electronic, and it was possible that the liaison officer sent to the Crisis Cell that some of the names received the vaccination, and in fact, they did not receive the vaccination"(The Jordanian Court of Cassation, 2023).

3.3. Crime and Offender Tracking: Digital forensic analysis is an effective tool for tracking crimes and offenders. It can be used to identify sources of cyberattacks, track electronic hacking, and identify digital attackers (Al-Halabi, 2011; Al-Billeh, 2022c).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023), dated 8June 2023, that: "Electronic forgery is computer-related forgery, consisting of the unauthorized creation or modification of recorded data in such a way that such data would acquire a certain value different from the context of legal transactions, which is based on the validity of the data extracted

through this data, which can be subject to the deception of protected legal interests. Accordingly, the court found that prejudice to these official transactions is caused by accessing the existing database and modifying the data, whether by deleting existing data, adding new data, or even creating non-existent data. It is the subject of this lawsuit represented by: entering the database, using the password and username of the employee ('A), using her name, and issuing certificates of receiving vaccinations against the Corona virus. Referring to the concept of the crime of forgery, two conditions must be fulfilled for this crime to be established, which are: the written instrument and the essential statement as defined by jurisprudence, which is: "every written text conveys a certain or specific thought or meaning from one person to another when reading it or looking at it, whatever its material, type, or language in which it was written." Based on the definition of the written instrument in accordance with the appropriate law, it excludes each paper that, in its nature, is not officially edited or written, such as counters, machines, signs/plates, and pictures, as it is according to its nature that some of its parts include writings, signs, or numbers of any kind, and therefore the instrument must be written and that a change takes place in reality on this writing, which is the basis for protection of the instrument; the writing represents the content of the instrument, and this change should have a legal effect. The second condition is represented by the essential statement and determined by three standards. The first is the proof, meaning that if the written instrument were modified to prove these statements, it would have the power of proof. The second standard is generating a belief that contradicts the truth, so it must be likely to generate a belief that contradicts those who see this statement and believe it. As for the third standard, it is represented by the legal status that affects the rights and duties of one of the parties. The person committing the forgery by falsifying the written document represents the physical aspect of this crime, as long as laws specify how this change will take place, in addition to the criminal activity such as falsifying information when the perpetrator falsifies the data saved in the information device by using the information device. Thus, this crime falls under the classification of crimes that occur on the data and programs of the information system and that occur using the information device" (The Jordanian Court of Cassation, 2023).

3.4 Enhancing Digital Security: Digital forensics contributes to improving digital security by analyzing gaps, vulnerabilities, and attacks, providing solutions to fill these gaps, and providing more secure interfaces and networks (Al-Saghir, 2001; Al-Billeh, 2022d).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (3470/2021), dated December 20, 2021, that: Article 17 of

Jordanian cybercrime law stipulates that "Anyone who violates a law that is punishable by a penalty by using the Internet, a website, or another information system, or who participates in, obstructs, or encourages another person to violate a law by doing so, will be penalized with the punishment specified in that law. This implies that in the eyes of the law, crimes done over the internet or any other information system or website are treated the same as those committed in a physical setting since the legislature compared them with traditional crimes"(The Jordanian Court of Cassation, 2021).

In short, digital forensics is a powerful tool in combating cybercrime and protecting digital data, and helps in achieving electronic justice and developing a safe and reliable digital environment (Al-Ghafouri, 2009; Al-Billeh & Abu Issa, 2022).

Therefore, digital forensic analysis is considered an important matter in Jordanian legislation in order to combat cybercrime and protect Jordanian society from digital threats. Digital forensic analysis in Jordanian legislation achieves several things, the most important of which are:

3.5. Detection of Electronic Crimes: Digital forensics helps to discover digital evidence and information related to cybercrimes. Digital data extracted from electronic devices, such as computers and smartphones, is analyzed to provide the evidence needed to bring the accused to justice (Ibrahim, 2018; Al-Billeh & Al-Hammouri, 2023).

Article 4 of Jordan Cyber Crime Law No (17) for the year 2023 states that : "Anyone who intentionally accesses a website or information system in any way, whether it be without authorization, in violation of terms of service, in excess of an authorization, or accesses any portion of it that belongs to critical infrastructure, security services, financial institutions, public official institutions, or businesses owned by or contributing to any of these entities" (Article 4, Jordan Cyber Crime Law, 2023).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2021), dated 8 June 2023, that: "Since the Public Prosecution referred the defendants simply because it became clear to the witness that her username had been hacked, and that they had obtained certificates of receiving vaccinations without proving who hacked the username, and how the defendants could obtain the password of the witness without any of them being one of the liaison officers, and without any of them having the authority to view the mechanism of work of the group responsible for the vaccinations, or for the Public Prosecution to have programs of specialized technicians entrusted with the process of collecting evidence, equipped with programs, knowing how to use them and mechanism of work and their knowledge of information technology, and limiting

the use of the username and password to those persons who are allowed to use them, who have the right to use them, the place from which they were used, the time they were used, and their referral to court and that do not follow traditional evidence that evaded those who carried out these acts. As for what was presented by the Public Prosecution of the statements of the accused, each of (A.M), (B.M), (A.M), (M.Z) and (A.D) that they confessed about the crime ascribed to them, however, by reference to their statements before the investigator, the court found that they had paid sums of up to sixty dinars for each person in exchange for a statement that they had received the vaccinated in terms of appearance, but in reality they did not take the vaccination, and accordingly it was not clear from their statements who logged into the website of the witness (‘A), and who has accessed the database and used the password and username of the employee (‘A), and that they are not employees, and that they are not from the groups of vaccination officers, and it turns out that they have issued vaccination certificates and accessed by general (original) password”(Jordanian Court of Cassation, 2021).

3.6. Assisting Criminal Investigations: Digital forensics can support criminal investigations by collecting and analyzing digital evidence. Deleted or encrypted data can be retrieved and analyzed to understand the context of cybercrime and identify perpetrators (Al-Saghir, 2017; Khashashneh et al., 2022).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023), dated 8June 2023, that: “The court found that Article (148) of the Code of Criminal Procedure permitted the adoption of a statement by an accused against an accused person as evidence in the lawsuit, provided that there is another presumption supporting it, and since the judicial presumption is considered indirect evidence that the judge concludes from a known incident to prove the incident that he wants to prove, and this conclusion must be consistent with the logic and the facts of the lawsuit, and otherwise it is considered evidence and indications that do not rise to the rank of evidence intended in the Code of Criminal Procedure. Although the defendants supported each other's statements about the fact that they paid sixty dinars for each person in exchange for a statement that they had received the vaccine, this, and in the light of what we have shown, evidence and indications remain and does not amount to legal evidence in the sense stipulated in aforementioned Article (148) of the Code of Criminal Procedures, being the statements of the accused against the accused and does not rise to the rank of presumption, and on the other hand, the court found that it is not possible to be reassured about these statements or to be reassured about the circumstances in which they were taken, since through the discussions of the

defendants' representative with the investigators, they did not establish the circumstances that were extracted from their statements, as the investigators' answers were lack of knowledge and lack of recall, which makes the court not reassured about those statements and the circumstances in which they were taken. Whereas the Public Prosecution is the one that names and presents the evidence to prove the occurrence of the crime with its legal elements and attributes it to the defendant, and since the evidence of the Public Prosecution presented in this case, which was presented to prove the crime of forgery, does not include any legal evidence proving that the defendants are the ones who accessed the database and used the password and username of the employee ('A) and they issued vaccination certificates. Accordingly, what was presented as evidence by the Public Prosecution is not suitable and cannot be a reliable basis for establishing a criminal judgment of conviction. Therefore, and in the absence of any legal evidence that proves that the defendants have committed the crime, in this case the court must declare the accused innocent of this crime because there is no evidence"(Jordanian Court of Cassation, 2023).

3.7. Protecting Individuals and Institutions: Digital forensics enhances the security of society and protects individuals and institutions from digital threats. By identifying and understanding patterns of cyber-attacks, preventive measures can be taken to reduce risks and enhance digital security (Al-Husseini, 2015; Isa et al., 2022).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023), dated 8June 2023, that: "Information forgery may be physical, i.e. by accessing data, information and programs and modifying them by deletion or addition, or creating a written instrument or electronic document that did not exist, or the forgery may be not physical, by recording or adding data or information not issued by the owners of the document or information instrument, or by proving false or unrecognized facts improperly"

3.8 Supporting Judicial and Justice Procedures: Digital forensic analysis is an important support for judicial and justice procedures in Jordanian legislation. It provides robust and reliable digital evidence that can be used in court to bring the accused to justice in a fair and transparent manner (Abdel-Baqi, 2018; Alshible et al., 2023).

The Jordanian Court of Cassation, in its criminal capacity, issued its judgment No. (171/2023), dated 8June2023, that: "With regard to the evidence for the occurrence of the crime of electronic forgery, it is necessary to establish evidence that the accused committed forgery, and the evidence is the means that the judge uses to reach the truth he seeks, or it is everything related to the facts presented to the judge to implement the rule of law, or it is the incident from

which the judge derives evidence to prove his conviction in the ruling he concludes. Regarding electronic evidence, it refers to all data that can be prepared or saved in a digital format to enable a computer to complete a task. It can also refer to evidence that is derived from a legal or technical order placed by computer software and information systems, computer hardware and tools, or communication networks to be presented to the judiciary. After being subjected to scientific analysis or interpretation in the form of written texts, drawings, photographs, forms, and sounds to demonstrate the commission of the crime and determine the defendant's guilt or innocence. Thus, the crime of electronic forgery is not achieved through traditional means of proof. Rather, there are new evidences. The crime takes place in an environment that is not physical in nature, as dealing in the informational environment to commit such crimes must be proven by using programs of retrieving erased data, which the technicians from the Public Prosecution who are entrusted with the process of collecting evidence must be equipped with these programs and have knowledge of how to use them and their mechanism and their knowledge of information technology, and limit the use of the username and password to the persons who are allowed to use them and who have the right to use them and the place from which they were used and time to use them" (Jordanian Court of Cassation, 2023).

In general, digital forensics is essential in Jordanian legislation to combat cybercrime and ensure digital security in society.

4. Tools and Techniques Used in the Digital Forensic Process

In the process of digital forensics in information crimes, a set of tools and techniques are used to investigate and collect digital evidence. Among these tools and technologies are:

- **Hard Disk Scan Tools:** used to recover deleted or hidden data on hard disks. These tools include programs such as En Case, Forensic Toolkit (FTK), and Autopsy (Ladadoh, 2021).
- **File recovery tools:** used to recover files that have been unrecoverably deleted on the computer. Examples of these tools are Recuva and Photo Rec (Al-Husseini, 2015).
- **Digital Fact-Finding Tools:** used to collect digital evidence from computers and other electronic devices. Such as text and photo recovery tools, contact log, location and file recovery tools (Al-Saghir, 2017).
- **Memory Analyzers:** used to extract important information from the device's RAM. These tools help detect intrusive processes and malware that do not appear in the operating system, which may contain important information. Such as Volatility Framework and Magnet RAM Capture (Ibrahim, 2018).

- Advanced Analysis Tools: used to identify dates and times of suspected digital activities and enable traces of cyberattacks to be tracked. These tools include network monitoring systems, time stamps and sensors (Al-Ghafouri, 2009).

- Network Analysis Tools: used to analyze network traffic and check device behavior patterns and connections between devices. These tools include Wire shark, TCPDUMP, and various versions of advanced analyzers (Al-Saghir, 2001).

- Photo and Video Analysis Tools: help in the investigation and examination of digital photos and videos to extract information and evidence. Such as Exif Tool and Forensic Image Analyzer (Al-Halabi, 2011).

-Digital Impact Analysis Tools: used to analyze the digital impact of files and information on digital devices. Such as Hash Calc and Bulk Extractor (El Mahlawy, 2016).

- Digital Extraction and Analysis Software: These tools are used to extract digital data from mobile devices, computers, and other devices. Examples include En Case, Forensic Toolkit (FTK), Autopsy, Cellebrite, and Oxygen Forensic Suite (Al-Husseini, 2012).

These are some of the common tools and techniques in the digital forensics process, and there are many other tools and software that can be used depending on the nature of the case and the needs of the investigator (Al-Hajjar & Bashir, 2021).

Therefore, in the process of digital forensic analysis in Jordanian legislation, a set of advanced tools and techniques are used to collect and analyze digital evidence. Among these tools and technologies, the following can be mentioned:

- Digital Data Extraction: Data extraction tools are used on digital devices such as computers, smartphones, and electronic disks. Specialized software and hardware are used to copy and extract data in a legal and accurate manner (Abdel-Baqi, 2018; ALMANASRA et al., 2022).

- Analyzing Digital Data: The extracted data is processed using advanced techniques such as deleted data recovery, photo and video analysis, geographical data analysis, activity log analysis, and others (Ladadoh, 2021).

- Verification and Certification of Data: Verification and certification of digital data requires the use of tools for in-depth analysis of digital evidence and confirmation of its authenticity and provenance. Digital signature, record checking and watermarking techniques are used to ensure the authenticity and legality of digital evidence (Al-Hajjar & Bashir, 2021).

- Legal Analysis: In addition to the use of digital tools, digital forensic analysis in Jordanian legislation relies on legal analysis of digital evidence. This includes analyzing legislation and legal frameworks related to cybercrime and consulting legal experts (Fatih & Awwad, 2017; Al-Billeh, 2022e; Al-Husseini, 2012).

5. The Problems with the Digital Forensic Process and Solutions

The digital forensics procedure faces a variety of difficulties, such as:

- **Growing Volume of Digital Data:** The amount of data available for forensic analysis is expanding due to the increased usage of digital technology, hence methods and tools must be created to handle and examine this data quickly. (El Mahlawy, 2016; Al-Billeh & Abu Issa, 2023).
- **Technical Challenges:** Analyzing digital data requires high technical skills and in-depth knowledge of cybersecurity, encryption systems, programming, and others. Therefore, digital forensic analysts must be properly trained and highly technically qualified (Al-Halabi, 2011).
- **Pervasive Encryption and Privacy:** Advanced criminals use encryption tools and circumvent security systems to hide their digital activities. This means that new technologies and tools must be developed to deal with these challenges and be able to break or bypass encryptions (Al-Saghir, 2001; AL-KHAWAJAH et al., 2022).
- **International Cooperation and Information Sharing**: Oftentimes, digital crimes transcend national boundaries and require international cooperation to investigate and prosecute crimes. Cooperation between the competent authorities should be strengthened internationally and the exchange of information and expertise should be facilitated (Al-Ghafouri, 2009; Alkhseilat et al., 2022).

To overcome these challenges, investment in technology development and research related to digital forensics is required. Cooperation and communication between government institutions and the private sector must also be strengthened to exchange experiences and develop innovative solutions to meet these challenges (Ibrahim, 2018; Abu Issa & Alkhseilat, 2022).

5. International Cooperation in the Field of Digital Forensic Analysis and Combating Information Crimes

International cooperation plays a crucial role in the digital forensics process to combat cybercrime. Among its most important importance:

- **Sharing Information**: International cooperation helps exchange information and expertise between countries and organizations concerned with combating cybercrime. Sharing information on cyber threats, attack techniques, and technology developments can help improve countries' ability to tackle cybercrime (Al-Saghir, 2017; AL-Hammouri et al., 2023).
- **Joint Investigation:** International collaboration allows investigators and digital forensics experts to work together in conducting joint investigations. Such cooperation can include more cut-off points and

digital evidence in investigations, thus leading to more accurate and effective results (Al-Husseini, 2015).

- **Developing Laws and Policies:** International cooperation can help standardize the laws of different countries and improve policies related to combating cybercrime. In coordination between countries, effective legal systems can be put in place that deal more appropriately with the challenges of cybercrime, and protect the rights of individuals and institutions alike (Abdel-Baqi, 2018; Abu Issa & Khater, 2023).
- **Training and Cultural Exchange:** International cooperation provides the opportunity for joint training and exchange of experiences between countries and digital forensic investigators. This can help raise the level of skills and competence of investigators, and improve analytical capabilities in the field of combating cybercrime (Ladadoh, 2021; Abu Issa& Al Shibli, 2022).

In general, international cooperation enhances the ability of countries to tackle cybercrime, which usually transcends national borders. With the development of information and communication technologies, international cooperation becomes more important than ever in combating these crimes and protecting societies from digital threats.

6. Conclusions

A set of important legal controls have been identified in digital forensics in information crimes, including privacy rights, protection of personal data, and legal procedures required for the use of digital evidence. Analyzing and evaluating several methodologies used in digital forensics to determine best legal practices and warn against any illegal practices.

In fact, a clear set of legal controls related to digital forensic analysis in information crimes must be established and developed, to ensure the preservation of individual rights and to avoid any violations of existing laws. With the need to provide appropriate training and continuous updating of experts and investigators working in the field of digital forensic analysis to keep abreast of technological developments and legal challenges in this field, and to strengthen international cooperation in the field of digital forensic analysis and the sharing of experiences and knowledge related to legal controls between different countries.

Therefore, it is imperative to ensure that the rights and guarantees of suspects and suspects are respected, and digital investigators must be familiar with the tools and techniques used in digital forensic analysis and work in accordance with professional standards, and adhere to local and international laws related to information crimes and digital forensic analysis. Recognizing the complexities and

developments of technology and related laws, digital investigators, judges, and stakeholders must stay abreast of the latest developments and legal practices in the field of digital forensics.

References

Abdel-Baqi, M. (2018). Investigating and Proving Electronic Crime in Palestine: A Comparative Study. *Dirasat: Shari'a and Law Sciences*, 45 (4), 284-299. https://archives.ju.edu.jo/index.php/law/article/view/14120

Abu Issa, H., & Al Shibli, M. (2022). The Avenge as a Motive of Homicide Crimes in Jordan for the Period (2017-2021). *Pakistan Journal of Criminology,* 14(1), 112-127.http://www.pjcriminology.com/publications/2888-2/

Abu Issa, H., &Alkhseilat, A. (2022). The cyber espionage crimes in the Jordanian law. *International Journal of Electronic Security and Digital Forensics*, 14 (2),111-123. https://doi.org/10.1504/ijesdf.2022.121203

Abu Issa, H., & Khater, M. (2023).Distance Indecent Assault Crime in Jordanian Law Perspective.*Pakistan Journal of Criminology*, 15 (1), 125-138. https://www.pjcriminology.com/publications/distance-indecent-assault-crime-in-jordanian-law-perspective/

Al-Billeh, T. (2022a). Judicial oversight on the administrative contracts in the Jordanian legislation and the comparison: the modern qualitative jurisdiction of the administrative judiciary. *Indian Journal of Law and Justice*, 13 (2), 1-28. https://ir.nbu.ac.in/handle/123456789/4763

Al-Billeh, T. (2022b). The Correction of the Invalidity of the Civil Trials Procedures in Jordanian and Egyptian Legislation: The Modern Judicial Trends. *Kutafin Law Review*, 9 (3), 486-510. https://doi.org/10.17803/2713-0525.2022.3.21.486-510

Al-Billeh, T. (2022c). Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. *Pakistan Journal of Criminology*, 14 (1), 1-14. http://www.pjcriminology.com/wp-content/uploads/2022/08/1.-Legal-Controls-of-the-Crime-of-Publishing-a-Program-on-the-Internet-in-Jordanian-Legislation.pdf

Al-Billeh, T. (2022d). Freedom of Religious Belief and the Practice of Religious Rites According to the Jordanian Legislation: Difficult Balance Between International and Regional Requirements as well as the National Legislative Controls. *Balkan Social Science Review*, 20. 117-137. https://js.ugd.edu.mk/index.php/BSSR/article/view/5503/4660

Al-Billeh, T. (2022e). The Impact of the Comprehensive Ban Due to the COVID-19 Pandemic on the Quality of Ambient Air in Jordan. Study for 15th

March to 15th April of 2020 Period. Journal of Environmental Management and Tourism, 3(59), 802-811. https://doi.org/10.14505/jemt.v13.3(59).19

Al-Billeh, T., & Abu Issa, H. (2022). The Community Penalties in the Jordanian Criminal Law: What are the Alternatives to Liberty-Depriving Penalties? *Pakistan Journal of Criminology*, 14 (3), 1-18.http://www.pjcriminology.com/wp-content/uploads/2023/03/1.pdf

Al-Billeh, T., & Abu Issa, H. (2023). The Role of the Environment Committees in the Nineteenth Parliament for the Year 2020 in Studying Matters Related to Environmental Affairs in Jordan. *Journal of Environmental Management and Tourism*, 1(65), 168-175. https://doi.org/10.14505/jemt.14.1(65).16

Al-Billeh, T., & Al-Hammouri, A. (2023). Guarantees of Juvenile Trial Procedures in Jordanian Legislation: The International Standards towards Reformative Justice for Juveniles. *Pakistan Journal of Criminology*, 15 (1), 1-16. https://www.pjcriminology.com/wp-content/uploads/2023/07/1.Tareq_Billa_Paper_Final_Draft.pdf

Al-Ghafouri, H. (2009). *Investigating and collecting evidence in crimes related to the Internet*. Cairo:Dar Al-Nahda Al-Arabiya.

Al-Hajjar, A., & Bashir, F. (2021). Digital Evidence and Evidence of Cybercrime Between Origination and Interpretation. *Journal of Al-Istiqlal University for Research*, 6 (1), 29-152. https://journal.pass.ps/index.php/aurj/article/view/171

Al-Halabi, K. H. (2011). *Procedures for Investigation and Investigation of Computer and Internet Crimes*. Amman:Dar Al-Thaqafa for Publishing and Distribution.

AL-Hammouri, A., Al-Billeh, T., &Alkhseilat, A. (2023). The Extent of Constitutionalizing the Environmental Rights as One of the Anchors to Keep a Healthy, Clean Environment: A Difficult Balance between the International Agreements and the Jordanian Constitution's Restrictions. *Journal of Environmental Management and Tourism*, 1(65), 89 -97. https://doi.org/10.14505/jemt.v14.1(65).09

Al-Husseini, A. (2012).*Procedural aspects of crimes arising from the use of electronic*. PhD Thesis, Ain Shams University.

Al-Husseini, A. (2015). *Criminal investigation and modern means in detecting crime*. Lebanon:Al-Halabi human rights publications.

AL-KHAWAJAH, N., ALKHSEILAT, A., AL-BILLEH, T., MANASRA, M., & ALWERIKAT, N. (2022). Criminalization of the Transmission of the Coronavirus COVID-19 and Its Impact on the Right to a Healthy

Environment. *Journal of Environmental Management and Tourism*, 13(7), 1881-1887. https://doi.org/10.14505/jemt.v13.7(63).08

Alkhseilat, A., Al-Billeh, T., Almanasra, M., &Alwerikat, N. (2022). Criminal Behavior as a Basis for Criminal Responsibility for the Crime of Introducing Substances Hazardous to the Environment in Jordanian Legislation. *Journal of Environmental Management and Tourism*, 7(63), 1851 - 1858. https://doi.org/10.14505/jemt.v13.7(63).05

ALMANASRA, M., Alkhseilat, A., Al-Billeh, T., ALWERIKAT, N., & ALSHARQAWI, A. (2022). Criminal Responsibility for the Crime of Discharging Polluting Substances for Water Sources in Jordanian Legislation. *Journal of Environmental Management and Tourism*, *13*(7), 1948–1948. https://doi.org/10.14505/jemt.v13.7(63).15

Al-Saghir, J. (2001). *Evidence of criminal evidence, modern technology, radar devices, computers, genetic fingerprinting, a comparative study*. Cairo:Dar Al-Nahda Al-Arabiya.

Al-Saghir, R. (2017). *Criminal intent in Internet-related crimes, a comparative applied study*. Giza:Arab Studies Center for Publishing and Distribution.

Alshible, M., Abu Issa, H., & Al-Billeh, T. (2023). The Extent of Considering Environmental Crimes as A Manifestation of Economic Crimes. *Journal of Environmental Management and Tourism*, 1(65), 23-31. https://doi.org/10.14505/jemt.v14.1(65).03

El Mahlawy, A. (2016). *Judicial experience in information and digital crimes*. Alexandria:University Thought House.

Fatih, R., & Awwad, Y. (2017). Evidence of electronic crime with scientific evidence. *Tikrit University Journal of Law*, 1 (3), 476-506.
http://www.tujr.tu.edu.iq/index.php/t/article/view/113

Ibrahim, K. H. (2018). *The Art of Criminal Investigation in Electronic Crimes*. Alexandria:University Thought House.

Isa, H. A., Alwerikat, N., &Al-Billeh, T. (2022). The Concept of the Public Employee in Jordanian Law: Different Constitutional, Administrative, and Criminal Law Definitions. *BiLD Law Journal*, *7*(2s), 331–337. https://bildbd.com/index.php/blj/article/view/318

Khashashneh, T., Al-Billeh, T., & Issa, H. A. (2022). The authority of the criminal judge to assess digital (electronic) evidence in jordanian, egyptian, and french Legislation. *Journal of Southwest Jiaotong University*, *57*(5), 631–640. https://doi.org/10.35741/issn.0258-2724.57.5.51

Ladadoh, A. (2021). *The suitability of the provisions of the Jordanian Cybercrime Law to the general provisions of the Penal Code*. Master's Thesis, Middle East University.