ISSN 2349-7831

International Journal of Recent Research in Social Sciences and Humanities (IJRRSSH)
Vol. 11, Issue 3, pp: (19-38), Month: July - September 2024, Available at: www.paperpublications.org

Electronic Evidence Methods in Jordanian Law

Dr. Mohammad Saleh Alqudah

(Assistant Professor of Civil Law)

Faculty of Law/ Zarqa University

DOI: https://doi.org/10.5281/zenodo.12699756

Published Date: 09-July-2024

Abstract: **Information and communication systems are now breeding grounds for electronic-evidence (eevidence) in audits, investigations, or litigation. Increasingly organizations are being ordered by law or lawsuit to preserve, retrieve, and hand-over relevant electronic records (e-records) because "the courts are uniformly recognizing the discoverability of electronic communication and documents" [Nimsger and Lange, 2002]. This trend is an outgrowth of aggressive tactics by regulators to ensure corporate accountability and deter fraud. In cases ranging from Securities and Exchange Commission probes of corporate malfeasance and insider trading to employment lawsuits, e-records are subpoenaed. Investigations conducted by the National Association of Security Dealers, Department of Justice, and Department of Homeland Security routinely require companies, their business partners, or third parties to preserve and disclose e-records, including internal e-mail and instant messages (IM). A highprofile example is the probe into alleged White House leaks of a covert CIA agent's identity in which White House employees received e-mail stating: ''You must preserve all materials that might in any way be related to the department's investigation.'' E-mail, telephone logs, and other electronic documents were mentioned specifically.**

Keywords: **Electronic Evidence Methods, Information and communication systems.**

1. INTRODUCTION

This thesis deals with the laws of Jordan regarding the admissibility of electronic evidence in court. The Jordanian Evidence Law 2001 is a replica of the Jordanian Evidence Law of 1937. In 2001, the law was amended to allow for many changes in society that had occurred since 1937. But the evidence law had not kept up to date with technological changes and thus does not specifically provide for admissibility of electronic evidence in court. The law simply states that "evidence consists of confessions, witness statements and real evidence. Real evidence may be omitted…" but fails to define what real evidence actually is. ESI is very real in the sense that it is used in place of traditional evidence to prove or disprove events and it may indeed be real in the sense that it may be a computer used in a crime that could be confiscated from an accused person. An admissibility framework for this evidence must be developed so that the courts can discern what evidence may be admitted and how to deal with it.

The computer has become a more integral part of society; it is used as a tool in crime, to record evidence of crime and to store information about the crime and it is used by the courts. Still, information pertaining to crime or civil wrong can be recorded on any electronic medium; ESI is more prevalent and easily accessible and it is those advantages that ESI use over traditional forms of evidence that makes it necessary to understand it in a legal context today.

Electronic evidence plays a vital role in today's legal system. It is not just a growing form of evidence; it is a new medium for evidence. Compared to evidence law, electronic evidence is a relatively new area of law. It can be very complex and costly yet extremely beneficial to a case. The very nature of electronically stored information ("ESI") makes it an attractive evidence source. It is easy to edit/delete and can be stored virtually anywhere, however it is those same qualities that make it a risky source of evidence and a collection/preservation nightmare. But traditional paper evidence is rare and becoming rarer. Hence, understanding how to deal with this ESI such as computer records, emails and even social media is crucial for lawyers and law students in today's legal system.

1.1. Overview of electronic evidence

The presence of this new evidence certainly has its own problems because the law now must be applied differently than what was used in the provisions of general evidence previously. It only needs to be amended or interpreted back to be able to use it as evidence. This is because existing rules do not provide a special setting for electronic evidence. This is certainly a challenge on its own, how the law based on the opinion and existing rules is reformulated now in order to create qualified judges and legal practitioners who understand, process, and make decisions regarding electronic evidence. This may require a new construction or interpretation of the law. In addition, a large number of electronic evidence contains data that is still stored for a particular purpose. This means that electronic evidence has the possibility of being manipulated, deleted, or hidden by someone. This undoubtedly will also create more problems for legal practitioners because the judge should be critical in assessing the electronic evidence and making decisions regarding the truth of the data from electronic evidence. All the problems that exist clearly indicate the need for a special provision on electronic evidence as a new thing that is increasingly monopolizing the existence of previous evidence in this world.

When it was confirmed in the rule of law in Indonesia, then the electronic evidence globally has a great threat to conventional evidence. This is confirmed by the resolution in the Third United Nations Congress on the Crime Prevention and Criminal Justice in April 2000. In the event, this resolution stated the need for formulation and reform of an international legal instrument against conventional crimes and cybercrime. This led to the conventional utilization of electronic evidence competing with conventional evidence as a way to prove something. This is increasingly supported by the presence of international organizations as influential intergovernmental organizations in the development of the world's most use of electronic evidence, such as the European Union and the United Nations.

The Act No. 48 of 2009 on the Electronic Information and Transactions (UU ITE) in Article 5 said that the data message is evidence. This law makes it clear that if there is a legal dispute related to the data contained in an information system, the message data can be used as evidence in the court. This is reinforced by the Information and Electronic Transactions (ITE) law which is in a new system of criminal justice in Indonesia. This happens because the evidence in the form of electronic information is regulated in Article 30 to Article 38 UU ITE. The regulation states that if the evidence is Electronic Information, it is a valid evidence and has the same legal power as conventional evidence.

The electronic evidence has made a huge impact in the legal system. In this context, evidence is considered as a medium which can be used by a prosecutor and defendant in an attempt to prove the truth of facts existing which are related to an issue before the court. Evidence can take many forms including documents, testimony, and tangible items that help to prove the statement. The traditional form of evidence is known as conventional evidence. The development of technology has brought a change in the form of evidence. This change has come to pass because the world today uses technology in many aspects of life. This change has led to the presence of a new form of evidence, which is known as electronic evidence. This evidence has various forms including information contained in digital form that can be stored in various media such as computers, mobile phones, and others, and then appear as the result of computer process, and image and sound in digital form.

1.2. Importance of electronic evidence in legal proceedings

The first impact is the relevance that digital evidence has to the issue at hand. Judging from the nature of how information is stored today, digital evidence is more likely to be the best evidence available. For instance, in a banking investigation on certain illicit bank transactions, the best evidence would be a copy of transaction data in that particular time which is stored in a database. Any attempt to print out the data and it is no longer a computer entry is actually a double-copy of the evidence. This doesn't mean that printouts are not admissible at all, but when the authenticity of the printout is questionable, the original electronic data can be compared and it can be determined if it is actually the same data.

One must understand that the technology revolution has created a new environment for record keeping. This is especially true for business transaction data. In the past, everything was written on paper, usually multiple copies with the copies distributed among the parties involved. Today, the same data is entered into a computer once, usually to be stored in a database and never see paper form.

The importance of electronic evidence in legal proceedings came from the fact that the main two resources of information, which are the internet and computers, became an essential part of human life. Such information is used to make decisions

or perform certain actions in human daily life. Similarly, in legal proceedings (investigation and trials), this evidence is being used significantly to prove the truth, especially in this era of information-related crime. With the fast development of technology, the use of digital evidence in the court has become more relevant. So, what are the impacts of electronic evidence towards the traditional system of evidence and is it better?

1.3. Scope of the study

This research focuses on the methods of admissibility of electronic evidence in Jordanian legislation. It will determine the security and trustworthiness of such evidence in compliance with the Jordan Evidence Law and also weigh the importance and impact of electronic evidence in comparison to general evidence. This paper will also compare the legislation in Jordan to that of other nations who have already gone through the integration of electronic evidence and assess the success in which this method is being implemented. A detailed explanation of e-evidence and its various forms will be given, as it is important to clarify the wide scope of e-evidence as it is currently perceived. This is an important factor as it is necessary to determine the different types of e-evidence and thus deduce the general impact and importance a specific type of e-evidence may have on a trial or case. Recommendations will be given on how to improve the system so that it is more efficient for use of the courts and hopefully enable legislation to facilitate the acceptance of e-evidence. This paper will be conclusive with a suggestion of a model system for admissibility of e-evidence into trials and whether it is necessary to have a segregated system or a better interpretation and understanding of the current evidence law is sufficient.

2. LEGAL FRAMEWORK FOR ELECTRONIC EVIDENCE IN JORDAN

With regards to admissibility, Article 40 of the Jordan Evidence Law states, "Every record whether written or oral made by a person in private capacity or as a public official, in exercise of official functions or on the occasion of such functions, or by a direct order from a superior official or in execution of such order, is deemed to be an official record." This definition is wide enough to encompass electronic records. However, these records must pass the general tests for admissibility in Jordan mentioned at the beginning of this paper and will be subjected to additional tests specific to the nature of electronic evidence. Furthermore, Article VIII of the UNCITRAL model law states that there should be a general rule admitting evidence is admissible regardless of the fact that it is electronic.

A legal framework is required for the admissibility of electronic evidence. In the absence of specific rules and laws regarding electronic evidence, parties may face difficulties in establishing the authenticity, originality, and reliability of the electronic records retrieved during the discovery process or at trial. Jordan has no specific rules or regulations relating to the admissibility of electronic evidence. This may be due to the fact that the growth of electronic commerce and evidence worldwide has taken the legal community by surprise and that current laws do not adequately deal with the issue. In the absence of specific laws or rules regarding electronic evidence, the Jordanian courts will have to resort to existing laws and procedures in assessing whether electronic evidence is admissible.

2.1. Applicable laws and regulations

Upon examination of the laws and regulations in Jordan, there was minor evidence related to e-evidence. It is evident that the laws and regulations that are in place are seriously lacking and are in need of updating. According to the UNCITRAL model law on electronic commerce 1996, Jordan adopted this law on April 2nd, 2001. However, upon examination of this law, it focuses on e-commerce, not e-evidence. However, in article 13 of the model law, it indicates that a party seeking to introduce an electronic communication as evidence shall be required to meet the same requirements as the original form; this refers to the underlying data message. Currently, Jordan is looking to adopt the UNCITRAL model law on e-evidence. Hicks & O'Neill (2007) state that it is important for Jordan to adapt the model law and provide for the admissibility of computer evidence, and the reliability of the evidence depending on the manner in which the data was generated, stored, or communicated, and in particular whether the information was generated, communicated, or stored in paper form or other form of data compilation.

2.2. Definition of electronic evidence

Electronic evidence is any probative information stored or transmitted in digital form that a party can use at trial. It encompasses an array of media types including text, images, audio, and video. These source data can be found on local hard drives, floppy disks, CDs, DVDs, and on servers located on local area networks, wide area network, and the internet. The definition for what constitutes electronic evidence is very broad. This is because the term "electronic evidence" does not

require the existence of a distinct body of law. Rather, electronic evidence is any evidence that is stored or transmitted using electronics which can be used as any other evidence can be used. The only difference is that due to its intangible nature and its ability to be easily manipulated, authenticating electronic evidence and determining its admissibility is often more complicated than its paper-based counterpart. As a party to the UNCITRAL Model Law, Jordan has followed the definition of electronic evidence set out in Section 2(h) of the Model Law. Article 4(1) of the Jordanian Law on Information Technology Crimes defines electronic documents and states, "An electronic document and electronic signature shall have the same legal significance as the written document and the manual signature as provided in all laws and regulations unless it is stated differently in this law." A plain reading of this law indicates that any data that can be exclusively attributed to a specific person in the form of a text, sound, still, or moving picture can be considered electronic evidence. The significance of the law on information technology crimes affects the general law on electronic evidence and means practically any digital information that is relevant to a case has the potential to be electronic evidence.

2.3. Admissibility of electronic evidence

The admissibility of electronic evidence in Jordan is evaluated in line with the provisions laid down in the Jordan Evidence Law (Articles 19 and 63), Article 11 of the Security Law, and Article 11 of the IT Law. Electronic evidence is permissible in judicial proceedings, provided that it satisfies certain conditions. According to Article 63 of the Jordan Evidence Law, evidence is defined as everything by means of which a fact is established. This is inclusive of speech, documents, objects, messages, and any other kind of human or mechanical evidence. Article 11 of the Jordan IT Law provides further clarity on admissibility and states that electronic messages, records, and other forms of data are admissible in evidence in legal proceedings. This is, however, subject to the requirements detailed in this law or any other law. Therefore, evidence that is electronic in nature is admissible, provided that it meets the necessary conditions. These are that it must be relevant to the case, genuine, accurate, and not forming a general rule. This is a duty upon the offering party to satisfy the judge as to the fulfillment of these requirements. This duty upon the offering party to satisfy the judge as to the fulfillment of these requirements is, in essence, the burden of proof and is in line with the general principle of the Jordan Evidence Law, being that the burden of proof is upon the party who claims the existence of a particular fact. Therefore, in determining when electronic evidence is admissible, it is the party who is offering the evidence who must satisfy the judge as to the fulfillment of the said conditions.

3. TYPES OF ELECTRONIC EVIDENCE

Social media has gained tremendous popularity worldwide for various reasons and is considered self-incriminating. This type of evidence can be a deciding factor in some cases regarding an individual's lifestyle or behavior at a certain point in time. The success of acquitting or finding an individual guilty often depends on the court's ability to retrieve social media posts and messages, especially those belonging to an allegedly involved party in litigation. This evidence is considered strong if the data still exists on the social media server, as it can be recovered through the service provider. It is similar to email evidence in terms of being sent and received with the creation of logs or timings, cached and stored data. Time and date identification are important variables, as they show the exact time of malicious posts or messages and provide specific information about an individual. This evidence is considered plausible when an advocate attempts to create a printout or other form of static capture of the data to prevent deletion or substitution, as it follows the same principles and success as the currently collected evidence.

Digital documents and files are created through programmed actions rather than directly setting in motion the creation of files. The evidential value of digital files can become a matter of concern when it is difficult to determine the age of the file and the time and date it was created. If it is shown that the file was created after the action began or after the action that the file is claiming to record, there is a possibility of alterations or manipulation of the file. The evidence will show that digital files are only successful when the action is reflected in an outcome that produces the file. It is much harder to argue that the file was created specifically to affect the outcome or result in later litigation.

In contrast, carrier media is considered to be weak evidence and only reasonable to doubt. Messages sent through carrier media are cut up into packets of data and then recompiled at the receiver terminal. The data is stored in buffers at all times. The weakness of carrier media is that the data is only temporarily stored in RAM and is overwritten once the message is completed. Since the data does not exist on the hard drive, it can only be found in slack and unallocated space, which is difficult and costly to retrieve. This applies to both saved and unsaved draft messages, as they only exist on the hard drive

and buffer spaces are temporary. It is important to note that incoming and outgoing emails have the same evidential value. Emails are considered strong and reliable evidence when the exact time and date are shown, beginning with identifying information of the sender and receiver and ending with proper identification of the source.

Emails as a form of communication are the most widespread evidence used in Jordanian courts. They are commonly used in correspondence between companies and are therefore considered reliable. Emails have unilateral access, meaning that incoming and outgoing messages can be stored on a hard drive or external file and can be printed out. This is strong evidence because it shows that the messages have been stored and can be brought to trial. Additionally, deleted emails can be recovered using software, as the data still exists in slack and unallocated space.

3.1. Emails and electronic correspondence

It is trite to say that the admissibility of email evidence depends upon its relevance to the issues in dispute. Email evidence is subject to the same considerations as all other evidence, e.g. under Article 29 of the Jordan Civil Evidence Act. Email evidence can be excluded if the cost of proving the email would be disproportionate to the value of the email as evidence.

The provisions of Article 14 of the UNCITRAL Model Law and Article 9 of the EU Directive could be taken to signify that email is a "data message" and therefore electronic evidence. However, it is submitted that email is more appropriately categorized as "indirect evidence" or "circumstantial evidence". Email is often a secondary medium which is used in order to create a record of some other primary activity. For example, one might use an email to arrange a meeting or a telephone conversation. Email can be tendered as evidence of the making of an oral agreement as to the terms of the contract. This would be an illustration of email as indirect evidence because the email conversation is used to prove the existence of the alleged oral agreement.

Email can be used as evidence in Jordanian courts. There is no special procedure for the admission of email evidence. Email is admitted in the same manner as all other evidence. The party seeking admission must authenticate the email and establish its relevance and materiality. This is usually done through the testimony of the recipient of the email.

3.2. Digital documents and files

It is not difficult to find digital documents and computer data in today's computers. Most of our information has been digitized in one form or another and this creates a potential source of evidence for either litigant to utilize. Also, due to the ease of duplicating and altering electronic documents and computer data, it is difficult to be certain as to their authenticity. Therefore, the courts have to consider its probative value against its prejudicial effect and determine whether to admit or to exclude the evidence.

Basically, these data files can be categorized into two, which are electronic documents and computer data. Electronic documents are word-processed files in the form of texts and images. These are the same as traditional documents which are typed on papers and stored in files, except electronic documents are created using various kinds of text editing software, for instance Microsoft Word. Computer data means data stored in a database format. This can be easily understood by looking at a school examination result slip. Each of the students has their own piece of slip. That slip can be considered as an electronic document and all of the students' information on a table summary can be considered as the computer data. Both types of digital documents and files are admissible as evidence in court.

Digital documents and files are considered as data files which hold information in the form of texts, images, videos, audios, and databases. Digital documents and files can be created in the computer, handheld devices, mobile phones, and others. Digital documents and files consist of file properties such as file size, date and time created, date and time last modified, file location, and others which can be retrieved using file viewers or file management programs, for instance "My Computer".

3.3. Social media posts and messages

Some social media postings can be collected as simple screenshots, whereas others may be obtained by using the "share" methods available in the social media page itself. Once a useful posting is found, you should keep in mind that postings can be edited or deleted by the author, and in such cases, it would be useful to have other evidence to show what the posting looked like at an earlier time. At times, metadata from social media postings or edits to social media pages can be useful when trying to authenticate the posting and prove who the author was. Data found within the metadata of the social media

post is examined using the methods described above, while it is possible to take a screenshot of the metadata in order to preserve it for later use. Social media postings have been used in case law as evidence to show the mental state of the author of the posting, due to the fact that social media evidence is relatively easy to obtain and can be quite revealing. Any posting made on social media can be admissible in court and found to be relevant if it is sufficient to prove or disprove a fact. The proper capture and preservation of social media evidence is a compelling issue due to the potential importance of such evidence in court. When scraping or otherwise collecting data from the internet, there is a possibility for spoliation if not done correctly. Collection from social media sites is usually done by a third-party vendor or software, and it is important to hire a reputable vendor to collect such evidence. An article by Bowmans LLC notes that using a vendor will allow for the establishment of a proper chain of custody for the evidence and the possibility for the vendor to testify if the evidence is challenged in court. In an ABA article, they note Rule 902(14) will allow for authentication of data copied from a website using printouts or other images, and it is best practice to capture a duplicate image of the web page. With the ever-increasing use of social media evidence in court, it is advisable that all lawyers have a competent understanding of social media and its various forms.

4. COLLECTION AND PRESERVATION OF ELECTRONIC EVIDENCE

Methods for preserving the electronic evidence can be done directly or indirectly, sometimes it's done by a combination between these two methods. Direct preservation is to ensure the evidence doesn't have changes occurring and ensure its availability when it's needed. This is usually conducted for the data that has immediately known can be the evidence. For example, an email data containing a criminal conspiracy can be protected by backing up the email data to another media and making a synchronization to the email programs to another PC to ensure the data availability. This can also be done with a more complicated method, by applying certain software to the data that can record any changes to the data. When the data is computer data, there is a very simple method to protect it while ensuring its availability, just by making a printout of the computer data, but this is not recommended.

While computer technology has such rapid development, any IT equipment from hardware to software has an uncertain lifespan. This will be a problem while preserving the electronic evidence. Usually, the evidence is in the form of files or data on the IT equipment. Compared to the conventional evidence, files and data on IT equipment have the risk of being damaged, changed, and deleted. This can make the evidence become partial, and when it's damaged, changed, or deleted when it calculated with calculation day, the evidence may be lost. On the other hand, the conventional evidence preservation, if stored in the right place and proper way, has the durability and lifespan as long as the evidence type itself. To preserve the electronic evidence, it can be done in many ways, depending on the type of evidence itself. The main purpose is to prevent the evidence from any changes occurring and ensure its availability.

Legal requirements basically vary among different countries, and from the conventional evidence law which has its own nature specific to its country. Japanese law, for instance, has already implemented the electronic evidence specific regulation, which based on their statement wants to accommodate the technology development. As for this law regulation in Article 230–230 sex from Evidence Act Chapter 24, mentioning evidence gathered from the computer, or from the other similar means, it can be submitted as electronic evidence. The purpose is for having special regulation for the evidence that obtained from the computer.

With the rapid development of computer technology, the crimes committed using this technology have also been widespread. Electronic evidence has its own nature regarding its very fragile, volatile, intangible, and easily tampered characteristics. This makes it very vulnerable to open such big opportunities to be manipulated and erased. The most common case, as mentioned in Law Number 11 year 2008 regarding Electronic Information and Transaction, which its Article 5 verses (1) has a correlation with Article 56 verses (2), explains an employee from a company committed an email data manipulation into its company partner. Data manipulation can easily result in data loss or corruption. Data loss and corruption have the biggest impact on the evidence that has its own nature and type. When it has an impact on the criminal case in which the data contains the electronic evidence, it may be impossible to bring the evidence to general trial. The legal requirements for collecting the electronic evidence throughout the world have not yet been set uniformly, but the basic idea is to get the evidence that is authentic, in other words, the evidence can be accountable and can be supported with sufficient proof.

4.1. Legal requirements for collecting electronic evidence

CCP Article 152 states that for evidence to be accepted as legal it must be documented and the evidence must be clear in its meaning and not contradictory. This is to ensure that the evidence can be used effectively during litigation. This also prevents fabricated evidence being used to incriminate parties. This can prove to be problematic for electronic evidence given the ease at which it can be modified or deleted, it can be difficult to prove its credibility. Wahbeh (2001) states that in Jordan a judge can appoint an expert to verify if the electronic evidence has been tampered with. This can be an expensive and time-consuming task, and if the evidence is found to be inadmissible so late into dispute, it may delay the trial and prove costly for one of the parties. This may discourage parties from using electronic evidence.

The Jordanian legal requirements for the collection of evidence are found in the Jordanian Code of Criminal Procedures (CCP). There is no specific mention of electronic evidence within the legislation, and therefore it is the general consensus that the laws be applied to electronic evidence as they would to traditional documentary evidence.

4.2. Methods of preserving electronic evidence

The second method of preserving electronic evidence involves isolating the device containing the evidence and making an image of the entire device. This is often the best method for preserving electronic evidence. An image is an exact copy of the entire device and is by far the best way to preserve evidence. This method is not suitable, however, if only particular data on the device is relevant and the rest of the data is beyond the scope of a search warrant. Making an image of a device with irrelevant data could be seen as collecting more than necessary with a search warrant. An image of a device with a large amount of data could also be impractical to store.

The first method of preserving electronic evidence involves simply making a copy of the data on the original medium. This could involve, for example, copying the contents of a hard drive to another hard drive. While this is the simplest method of preserving electronic evidence, it is not always the most appropriate. Using a simple copying method may alter data in a way that makes it inadmissible in court. This could happen if, for example, data is copied from a hard drive, altering the access/modification dates on the copied files. If this method has the potential to alter the evidence, it is clearly inappropriate.

Electronic evidence may be collected and preserved by various methods. These methods are not unique to electronic evidence, but are commonly used to preserve other forms of evidence, with some modification. The best method to collect evidence in some cases may be to use more than one of these methods.

4.3. Chain of custody for electronic evidence

"Chain of custody" is little used at either of the larger two ISPs, and then only to distinguish its use with ISPs from how it might be applied with traditional evidence. Additionally, a common backdrop to methods of maintaining the chain of custody in network investigations is distrust in information systems personnel and investigators not trained in digital methods to recover electronic evidence, leading law enforcement to conclude that only their personnel should handle or acquire digital evidence. Prior to actual network-based investigations, the best opportunity to address these issues is in outlining specific procedures wherein the responsibility for evidence collection can be transferred from the custodian of the records to the investigator, and further among multiple levels of investigators, while providing documentation and verification at each step. These procedures can vary greatly between different types of investigations, and the different custodians of the evidence and investigators; however it is useful to refer to existing models for chain of custody in traditional evidence. It is important in any legal system to show that the electronic evidence presented in court is the same as the evidence that was originally seized or obtained, given the ease at which electronic data is modified, whether intentionally or inadvertently. A fundamental principle of Anglo-American law holds that in order for evidence to be admissible at trial it must be shown to have been in continuous possession of a party with no opportunity for tampering. When authentication of electronic records occurs with a printout produced as the output of a computerized record, judges and lawyers are often uncomfortable with the inability to directly tie the printout to the data, and subsequently to the system producing the data. This has led to the suggestion that to make electronic records more readily admissible, a system be developed to equate the printout with the data by being able to show that it is in fact the same data, and has not been altered, by tracking the printout through its own chain of custody back to the data. This however can only be a partial solution to the problem if the printout is ever disputed.

5. AUTHENTICATION AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

Despite the move away from the traditional notion that authentic evidence must be proven to be in its original form, a reliance on the originality of electronic evidence and the sheer volume of electronic data and systems can still pose issues of authentication. This is a result of the fact that the only way to properly demonstrate the reliability of an electronic method or system will be through its evidence being so clearly reliable that it cannot realistically be challenged. At best, the proponent of electronic evidence will need to demonstrate the integrity of the system and the maintenance of the evidence throughout its existence. This can again pose significant difficulty given the complexity of technology and many systems that are constantly evolving.

The Federal Rules of Evidence in Rule 901(1)(3) provide that authenticating evidence can be established by identifying evidence through distinctive characteristics and the appearance of the matter in question, including evidence containing public information and printouts of electronic communications, provided that the proponent of the evidence can account for the integrity and reliability of the method of storage and printing of the communication. The UNICTRAL Model Law adopts a similar approach in Article 9, providing that no signature, original or original to the document in question, needs to be proved for an electronic communication to be deemed reliable and subsequently admissible. This approach has also been supported by the American Law Institute, the Australian Law Reform Commission, and the Singapore Ministry of Law, all of whom have supported the view that the authentication of electronic evidence is best achieved by focusing on reliability of the source.

Authentication of electronic evidence, as we mentioned before, is crucial given the ease with which evidence can be altered or fabricated, and the dramatic consequences of relying on such evidence. There is general consensus that the best means of authenticating electronic evidence is to demonstrate the reliability of the process or system which generated the evidence. This method is consistent with the approach taken in the UNICTRAL Model Law and the Federal Rules of Evidence to authentication of electronic records, neither of which require the evidence to be in its original form, nor prove the integrity of the electronic record for it to be deemed authentic.

5.1. Standards for authenticating electronic evidence

One aspect of authentication shared by traditional evidence and electronic evidence lies in the requirement to demonstrate the genuineness of an item. In relation to a document, this might be taken to involve showing that the document is what it purports to be, i.e. dated and sent by the person named as the sender, or that it comes from a genuine source such as a web entry from an official site or an email from a registered company. However, the traditional manner of demonstrating this using expert testimony is becoming less useful and efficient when applied to the abstract nature of electronic evidence. Rather than oral evidence, it is likely that electronic evidence will be better authenticated using inferences from its reliability and integrity and/or through the second category of authentication described above.

There are no Jordanian statutes or case law specifically addressing the authentication of electronic evidence. Articles 49-60 of the Law of Evidence 2001 includes general provisions on the authentication and admissibility of documents but these are inadequate when applied to electronic evidence. Articles 68-71 of the Electronic Transactions Law 2001 contain a somewhat more detailed, albeit limited, treatment of the admissibility of electronic communications.

5.2. Challenges in authenticating electronic evidence

The burden of authentication of electronic records is not peculiar to Jordan; it is a common-law countries in the principle that the best evidence rule applies equally to all kinds of evidence. Where electronic records are sought to be adduced in litigation, it is universally necessary to establish that the particular records are what they are proffered to be. This is most commonly achieved by direct evidence of a witness to the circumstances of the making of the records, or by evidence tracing the custody of the records to ensure their integrity and security from the time of creation with some reliable form of audit trail.

In the context of Jordanian legal practice, there are many apparent or admitted difficulties in authenticating electronic records. Yet these are not unique to the Hashemite Kingdom. Equally cogent issues arise in the authentication of electronic data under other legal systems, and it is submitted that Jordan can find some guidance in the solutions that have been advanced elsewhere.

5.3. Factors influencing the admissibility of electronic evidence

Jordan has adopted a functional and flexible approach to determine the admissibility of electronic evidence, this being testament to the developing witness which has been shown in other common law and civil law jurisdictions. This test is best shown in the Electronic Transactions Law 2002. Art 11 states that "Information shall not be denied validity and effect merely on the grounds that it is in the form of an electronic record or electronic data". This indicates that there is no preference for evidence which is not in electronic form, giving the evidence equal chances of being admitted.

"The developing nature of the technology enables the judiciary to have a more flexible approach to the admissibility of evidence. It is viewed more as a continuum between the weight and the admissibility of the evidence, as opposed to a simple test for admissibility. Evidence of a lower weight is likely to be admitted so long as the technology which produced it is shown to be credible. This is an important distinction from the rigid rules of admissibility for some forms of evidence, for example, the hearsay rules.

Using evidence in trial depends upon the quality and applicability of the evidence to the case. This also applies to electronic evidence. The wide-ranging admissibility of electronic evidence is largely attributed to the relative infancy of the technologies which produce it. However, there are many country-specific reasons for evidence being admitted or rejected. This is especially apparent with Jordan.

6. ROLE OF FORENSIC EXPERTS IN ELECTRONIC EVIDENCE

In the Jordanian legal system, IT forensic experts need to be approved by the public prosecutor to be able to conduct investigations and present evidence in a court of law. It is not clear what certification is required for an expert to be accepted by the public prosecutor, though it is possible that already having been appointed as an expert previously, or being registered as an expert with a government department such as the Ministry of Justice may be sufficient. The law states that an expert may be an employee of the government or of a private entity, which can include being self-employed. If a private entity is an internal department of another organization (e.g. an IT department), the expert may need to have an employee-employer relationship as if he were an employee of the larger organization to legally be considered as an employee of the private entity. An expert may also be a non-Jordanian as long as he has the necessary qualifications and is recognized by the public prosecutor. In some cases, this may be beneficial, such as if a company based in Jordan has global IT systems and the case involves analysis of IT at a foreign office. A requirement for the expert to have a record of good conduct and behavior indicates the desire to have honest and respectable persons as experts. This implies that a conviction for a crime involving dishonesty or possibly a conviction for any indictable offense could be grounds for the public prosecutor to de-approve an expert. This has both positive and negative implications, as some of the brightest and most experienced experts are ex-law enforcement or military personnel who have turned to IT after leaving their previous careers.

Competent forensic experts play a very important role in the collection, examination, evaluation, and preservation of electronic evidence. It is equally clear that the expert needs to have a solid foundation in the principles and practice of computing and telecommunications. It is not sufficient to have expertise in traditional evidence and simply learn about electronic evidence as an adjunct. Proficiency in IT is an essential qualification for a digital forensics expert.

6.1. Qualifications and responsibilities of forensic experts

Law no. (21) of 2001 on forensic examination Article 2 is probably the most direct legislation focusing on the utilization of forensic experts and is very inclusive to all types of forensic investigation. It states "Any matter subject to trial, for the need of evidence or verification, expert examination, whether specialized or not, may be utilized with the approval of the requested party or may be asked ex officio with the approval of the party involved." This article inclusively puts all matters subject to trial as eligible for expert examination in all scientific fields. The approval of the party involved could be vital as the requested examination could be costly and prolong the judiciary process and thus it may not be beneficial to all involved parties.

Forensic science in general and computer forensics in specific has become a significant and helpful entity of the investigation process. In light of utilizing computers as a base tool in information processing and communication, it is likely to assume that most criminal activities nowadays involve the use of computers. Thus, the increase in involvement of computer systems in criminal activities has also inflated the necessity for skilled forensic experts. However, it is a little unsettling to fathom that such reliable and documented evidence like computer data and electronic devices are still in need

of protection and prevention of tampering and alteration throughout the process of investigation and evidence procurement. It is for this reason that Jordanian lawmakers have realized the importance of involving experts in legal proceedings in order to ensure credibility of electronic evidence usage, thus various legislations were put into place to protect and regulate its usage.

6.2. Role of forensic experts in analyzing electronic evidence

To ensure that the process and results of evidence assessment are conducted in the correct manner and are effectively utilized for case requirements, Jordanian laws aim to mandate expert testimony in evidence assessment conducted by forensic experts. This concept is provided within Article of the Law on Civil Transactions and Article of the Law on Criminal Procedure. The testimony of the witness or affidavit with the attendance of the witness or an expert may be compelled at the discretion of the judge or president who has issued the subpoena of the witness concerned. Data this method of examination and presentation can be considered to lead evidence and is a requirement for any evidence which is to be weighed for preponderance on the balance of probabilities. Any evidence which is to be weighed for this sort of standard must actually help the party adducing it to meet the standard and it is imperative that the evidence is not inadvertently weighed for the higher standard of clear and convincing or beyond reasonable doubt.

Generally, the objective of the examination and assessment of evidence is to discover and present the true state of facts. Thus, if an expert or witness examined or assessed the digital evidence, it may be required to provide a report of the evidence assessment process and/or the results. These reports may then be utilized for purposes of further assessment, maintaining admittance of the evidence, weighing the reliability of the evidence or the report, and/or preparation for direct or cross-examination of the expert or witness.

Moving on from identification of the expert, there are numerous types of evidence which may be assessed by forensic experts. In the present information age, electronic evidence is stored in multitude of data types and formats. Digital forensic experts can handle this range of evidence, needing to develop and maintain a deep understanding of the modern technology and methods of storing data in order to effectively and efficiently extract and assess the evidence in accordance with case requirements.

Firstly, it is necessary to understand and identify the roles and functions of digital forensic experts as opposed to other IT professionals involved in the evidence assessment process. Jordan has evolved its regulations and laws in a way which mandates that evidence assessment in certain cases must be performed by qualified experts, specifically Articles and of the Law on Criminal Procedure. This concept has been upheld by various decisions of judicial councils and it is important that this trend is maintained and further detailed to provide a distinction in the roles and functions of the various IT professionals.

One of the most important aspects in the legal and justice system is the process of examining and evaluating evidence. Forensic experts play a critically essential role in analyzing electronic evidence and they need to uphold tight methodology which will enable to convince the court of law or tribunal on the issue of evidence assessments, digital or otherwise. Emirates will from here on be a focus of the process the conducting expert analysis of Electronic Evidence and the evolution in regulations and laws to accommodate the requirement for employing professionals in the field. This phase of Electronic Evidence is fundamentally the discussion and examination of the manner and method in which Forensic Experts can contribute, examine, and evaluate evidence in the context of civil or criminal procedures. Forensic experts may be appointed as court experts or tribunal assessors or may provide evidence in the capacity as fact or expert witnesses. As aforementioned in Part and this may often be an inaccurate area, evidence assessment, digital or otherwise, may be conducted by extremely diverse range of personnel or specifically trained professional, most of whom will not have an understanding as to the process and methodology required to effectively examine the evidence in accordance with the rules of evidence in civil and criminal proceedings.

6.3. Expert testimony in court

This does not mean, however, that the right conclusions are being made in regard to the evidence. Among the major concerns facing the possible introduction of the Anglo-American adversarial system to Jordan is the potential misleading of the fact finder. Inquisitorial judges in Jordan are more accustomed to just investigating cases themselves, and the possibility of an unswayed investigation could lead to a judge looking for evidence to confirm his beliefs, rather than the evidence itself. This, in turn, could lead to the increased potential of altering electronic evidence, which is already an issue in itself.

Expert testimony can fall under different categories, depending on the evidence being presented. The first is reporting on items such as printers or fax machines, where the explanation is general and basic. The second is explaining to the judge or jury the scope and the results of the analysis that was conducted. The final category is the explanation of technical terms, in situations where the witness needs to attribute his meaning with the use of the term, as it may not be the common interpretation. The current status of Jordanian law on the admissibility of expert testimony and the methods for which the judge or jury receives the explanation is based on Articles 60, 182, 183, and 184 of the Jordanian Code of Criminal Procedure. Expert testimony is allowed and is, in fact, encouraged. However, many electronic evidence cases are not reaching this phase because of the judges' or jurors' lack of understanding of the evidence. If the testimony is given, the expert must be very detailed and thorough in his explanation in order to convey to the fact finder the same meaning he derived from the analysis.

In Jordan, as in other legal systems, electronic evidence is fast becoming an important aspect of legal cases. This change is a result of the growing usage of the internet, computers, and mobile phones, and stems from the many advantages and shortcomings of digital evidence. To accurately present electronic evidence, a forensic expert is often required to explain complicated technology and its implications to a judge or jury. This expert testimony is a critical phase in the process of presenting electronic evidence and greatly affects the judge or jury's perception of evidence. Unfortunately, many traditional rules of evidence in most legal systems were designed for tangible objects and are sometimes out of place when used to determine the admissibility of electronic evidence. Jordan is not an exception to this reality.

7. CHALLENGES AND ISSUES IN ELECTRONIC EVIDENCE

7.3 Cross-border issues and international cooperation: Many internet-related cases involve evidence that is held in a different jurisdiction than where the case is being heard. This raises issues as to whether the evidence is attainable and even if it is, whether obtaining it would breach the laws of that jurisdiction. Furthermore, mutual legal assistance treaties and letters rogatory were designed to obtain evidence from foreign countries and hold no provision for the handling of electronic evidence. The current procedures and requirement to have evidence translated may be overly cumbersome for the handling of rapidly changing and transient data.

7.2 Technical challenges in handling electronic evidence: The technical process of actually gathering, handling, and presenting electronic evidence gives rise to a myriad of issues. The complex nature of digital evidence and the requirements to recover, analyze, and present the evidence will often require the involvement of a computer forensics expert. Failure to handle the evidence correctly can lead to it being disallowed. There are also technical differences between digital evidence and traditional evidence, which may require amendment of laws and legal procedure. Up until this point, the Jordanian judiciary and legal profession have not had adequate training on managing electronic evidence, which will pose a problem should a case arise that is heavily reliant on digital evidence.

7.1 Privacy concerns and data protection: A fundamental issue is that the retrieval and revelation of electronic evidence is often in direct conflict with privacy and data protection laws. As most systems contain vast amounts of personal data, any search and seizure activity is likely to include a large amount of irrelevant personal data of third parties. Jordan is yet to enact specific legislation dealing with data protection and privacy, meaning that this potential conflict between private rights and the need to secure evidence is yet to be addressed.

Challenges and issues in electronic evidence: Protecting the evidentiary material comes under serious threat due to the constant movement and processing of data. Each phase of movement and processing may alter or damage the data, thereby rendering it useless as evidence. Ensuring the reliability and integrity of the evidence is a major concern. The factors discussed below identify the problems when attempting to use electronic evidence in legal disputes.

7.1. Privacy concerns and data protection

To prevent abuse and misuse, privacy concerns and data protection should be the main consideration for implementing electronic evidence in Jordan. The concepts concerning privacy and data protection are very subjective and vary from one culture or society to another. In general, privacy can be understood as a human right that, upon its violation, will cause mental injury or suffering. These mental injuries and sufferings are caused by fear of surveillance, the feeling of being watched, loss of control over personal information, and potential embarrassment or damage to reputation. Generally, fear comes from the potential misuse of information. Meanwhile, the derogation on data protection is the biggest concern

because electronic data, just like any other form of information, can be easily duplicated and misused. This, of course, will make it very difficult to prevent direct or indirect injury to the data owner. Data misuses can occur during evidence identification and collection, while some people even attempt to plant fake evidence in litigation opponent's electronic data. This event will make it very difficult to ensure that the evidence is real and authentic. Data misuses can happen again during the evidence storage, processing, and transmission. An unauthorized access by certain parties may change or destroy the data. Transmission via the internet has a higher risk due to its packet-based nature, which makes the data can be reconstructed or captured during its transmission. The more complex the internet route, the higher the risk of captured data before it reaches its destination. All these risks, of course, will lead to data owners' direct or indirect injury. The last data misuse may occur during the evidence retrieval. Any loss of evidence accessibility and availability due to data change or destruction will directly affect the evidence usability in trial. All aforementioned events will have the same result: injury to the data owner and evidence itself, and in the end, will affect the truth-seeking process in litigation.

7.2. Technical challenges in handling electronic evidence

There are countless technical challenges in collecting, securing, and ultimately presenting electronic evidence in court. Many of these issues stem from the abstract nature of ESI and the fluid manner in which it is created and stored. Perhaps the biggest problem facing lawyers and judges is the ephemeral nature of electronic data. Unlike paper records, which can be preserved and taped to a defendant or attorney, electronic evidence can easily be erased or altered, either accidentally or intentionally. This problem is compounded by the fact that many people (defendants, third-party witnesses) do not understand the way in which their computer creates and stores data. This often leads to situations in which potentially valuable evidence is erased or overwritten because a witness did not understand how to properly preserve it. An interesting aspect of this issue with erased evidence is that an adverse inference can often be drawn from the fact that evidence was destroyed. This is in contrast to traditional evidence law, under which the loss or destruction of evidence would often have no effect on the case due to the absence of proof regarding the relevance of the evidence. Step number one in understanding and combating the problems associated with electronic evidence is for attorneys and judges to come to terms with the foundational manner in which computers create, store, and display data. This is best done through practical experience, and there are various classes and programs which provide instruction on computer and forensics basics for legal professionals.

7.3. Cross-border issues and international cooperation

Although the global nature of the internet presents significant difficulties in identifying the location of the computer, the data, and the parties involved in a particular electronic evidence matter, the issue of whether data located in one country can be compelled to be produced for use in a foreign proceeding is clear. The 1980 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters was not drafted with digital evidence in mind and as a result, there is a lack of clarity on whether obtaining computer data for use in a foreign proceeding qualifies as 'evidence taking'. In an attempt to modernize the convention, an expert working group met in The Hague in 2003 and agreed upon a first draft of a new convention with the specific intention to include electronic evidence. However, future ratification and 'buy-in' to a revised convention is uncertain and its implementation would not have the effect of changing procedural laws and evidence rules in the varied legal systems of the world that also have an impact on whether electronic evidence located in another country can be accessed. An example of this is Australia where data located in a foreign country can be compelled to be brought into Australia for the purposes of its use in a court proceeding. The issue of whether evidence can be taken overseas can have significant cost implications for litigants. The retrieval and transportation of computer data and associated electronic evidence from a foreign jurisdiction can incur substantial costs. These costs can be further exacerbated by the need for expert witnesses to explain the data and evidence in a foreign court or for the translation of data and evidence into the language of the foreign proceeding.

8. CASE STUDIES ON ELECTRONIC EVIDENCE IN JORDANIAN LAW

An identical reproduction of electronic evidence, which can be shown to be of the same content as when it was first obtained, is referred to as best evidence. Electronic messages on email and mobile phones are prime examples of best evidence as they can be easily altered, deleted, and denied. A case involving the suspected bribery of a Jordanian Minister showed that some judges have a good understanding of this concept. One lawyer defending in this case explains how he "had to present evidence of an email sent to my client in which he was offered a bribe. The judge simply said that the email must be brought to court from the recipient's 'inbox' and asked me to explain it to the technical guys at court so they could get it right". This

statement shows a good understanding from the judge and a critical consideration of whether the evidence was of best evidence and therefore admissible.

An example of how this process works in Jordanian courts can be seen in a case involving a medical malpractice in which electronic evidence was crucial in the court's decision. In reference to this case, one lawyer states "the evidence had to be translated into paper copies before they were accepted to be submitted to court. This demonstrates the general mistrust and unfamiliarity with electronic evidence". This case was not successful in a retrial; however, the fact that the evidence was not accepted was not due to the judgment on its admissibility. The evidence was not reproducible and therefore was deemed inadmissible based on this fact. This does show, however, that electronic evidence is closer to being fully accepted in Jordanian courts.

The fact that electronic evidence is a product of a new technological era means that it is a relatively unexplored area of law. Guidance on the admissibility of such evidence and the procedures for its proper presentation is essential. At present, there is no legislature in Jordan specifically pertaining to electronic evidence. In the absence of a set of criteria for assessment, judges frequently have to make decisions on a case as to whether the evidence in question should be deemed admissible. Similar to the US, judges will make this decision by determining whether the evidence is deemed relevant, authentic, altered, and reliable.

Over the past few years, several cases involving the use of electronic evidence in Jordanian courts have contributed to the understanding of this concept and its acceptance as a legal tool for both prosecution and defense. Study of these cases provides insight into the judicial acceptance and understanding of electronic evidence in Jordan.

8.1. Landmark cases involving electronic evidence

The first Jordanian case which reached an appeal court and dealt with digital evidence was in 1999. In this criminal case, the appeal court justice refused to accept the evidence of a so-called 'sound expert' who had produced a cassette recording allegedly from a wiretapped phone call. He refused to accept the digital evidential medium on the grounds that the witness and his qualifications were suspicious; the witness was an employee of a party in the case. This is strong evidence of judicial hesitation and lack of recognition of digital evidence as a credible medium. This is supported by the fact that a verbal statement by the same 'sound expert', which was in the form of translation/interpretation of a conversation between Swiss and Arab defendants, was accepted by the same judge who discarded the cassette evidence due to the fact that it was the judge's opinion that the verbal statement was in the interests of the defendant receiving a fair trial. This is again significant and points to the need for general training in the theory and valid methods of electronic evidence gathering and analysis for legal practitioners in Jordan.

Electronic evidence first appeared in Jordanian courts in 1994, during a trial that was concerned with an electronic banking transfer. Here, two conflicting parties presented different printouts to the judge, each from their own floppy disk. The judge extracted the data to his hard drive, though after doing so one floppy disk was accidentally formatted. The judge then ordered an analysis of the bank's computers to determine if the printouts were genuine, but it was inconclusive due to lack of technician awareness. However, the court made a conviction based on other evidence. The issue of the printouts was not worked out on appeal and the case was settled out of court. This case is significant as the evidence was hearsay because the judge had to take the data from the floppy disks; this point was held on appeal. This requires special attention from the evidence law section of this study.

8.2. Court decisions and precedents related to electronic evidence

It is widely known that precedents in common law systems and court decisions in civil law systems are a significant guiding factor for future cases. The development of the law of evidence in Jordan, as discussed, a mixture of both systems, has been greatly influenced by past cases, in particular those in the higher courts. Unfortunately, alongside the lack of primary legislation in the field, there are few reported decisions specifically concerning electronic evidence. This is, however, a growing area and based on the rapid development of electronic communication, it is likely that the number of cases will increase in the future. Traditionally, in evidential matters, the Jordanian courts have been somewhat cautious in accepting new forms of evidence or using new methods for fear of tampering or modification. This is evident in the fact that, unlike some common law jurisdictions, there has been no attempt to alter the burden of proof or presumption of evidence in civil cases to accommodate the new internet age. (Should probably mention these articles and get translations). This trend has

also been reflected in the judiciary's treatment of electronic evidence. In the case of First National Bank v Odeh, a case involving the transfer of funds out of a frozen account, the plaintiff had obtained an order to seize the defendant's computer after showing evidence that he had made transfers from it. However, the plaintiff was unable to produce the computer or the date of the alleged transaction, and the request for a copy of the hard drive was denied. This case was in 2005, and somewhat unfortunately, that situation that caused it has changed little. The most important factor in accepting electronic evidence, as with any evidence, is the establishment of its relevance to the case and its admissibility. An example of this can be seen in an employment dispute between Jordan Telecom and some of its former employees. The employees, in a case of wrongful termination, claimed that the telephone company had been using software to monitor their chat logs and thus gain evidence against them. In the defendant's submission, a printout of one such chat log was produced as evidence to show that the relationship the chat logs had to their termination was relevant and direct. This printout was challenged by the plaintiff's counsel and was later deemed inadmissible due to the inability to connect the printout with a specific person and the inability to prove that it had indeed been part of a monitored chat log. Writing this judgment is a moot point in public interest, the current state of law would indicate that such evidence would be inadmissible, but recent rulings such as these show that the judiciary will measure each case on the individual circumstances and the method is a process.

8.3. Lessons learned from past cases

During the case, OKC provided evidence in the form of SMSs taken from the opponent's mobile phone. The court found in favor of OKC and awarded them a large sum in damages. Adnan Masha'l subsequently appealed the case. Annulling the original verdict, the appellate court concluded that the evidentiary material did not actually belong to the defendant and the plaintiff failed to show how it violated his rights. OKC was ordered to repay the damages. This case is significant in that it initially resulted in a hasty and costly judgment based on incorrect assumptions of the nature of electronic evidence and how it is attributed to an individual. The subsequent verdict, albeit a costly one, demonstrates a much more precise evaluation of the evidence and used it in making a decision that was well reasoned and did not infringe the rights of either party.

The case of OKC vs Adnan Masha'l is further testament to the fact that the judiciary has learned from past mistakes in dealing with electronic evidence. This was a civil case between two mobile phone companies, and it was filed by OKC in response to a series of false accusations from Adnan Masha'l.

An example is the Al Bashabsheh case, where the appellant's lawyer succeeded in pointing out procedural errors in how the evidence was taken and presented, and the case was subsequently dismissed. This case clearly showed that lawyers are becoming more aware of the nature and associated issues of electronic evidence and are thus better equipped to defend their clients from void or unsound convictions.

The impact of these cases and others relating to electronic evidence has been momentous. Jordan's judiciary has developed a learning curve in dealing with electronic evidence. Whereas earlier cases failed to address the specifics attributed with such evidence and resulted in incorrect or vacuous decisions, later cases have shown a marked improvement in the understanding of the nature of electronic evidence and the proper procedures required in handling and scrutinizing it.

9. BEST PRACTICES FOR HANDLING ELECTRONIC EVIDENCE

Guidelines for collecting and preserving electronic evidence normally come in the form of best practices manuals or court rules. One example is the best practices manual on seizing electronic evidence put forth by the US Department of Justice. It should be noted that different forms of electronic evidence have different lifespans and rules with regards to how long the evidence must be kept. Static evidence, evidence stored in a static form like a word document, is easier to preserve compared to dynamic evidence such as an internet conversation or data stored in a database. The best way to secure data, assuming it is not in danger of being destroyed, is to make an image of the media or relevant files. This ensures the original evidence is not changed while searching through it and the copy will have the same evidentiary quality as the original. A printout of data, despite not being an exact copy of the original, will often suffice as a copy of data stored in a dynamic form. After data is secured, the next step is to prove the integrity and authenticity of the evidence. Section 9.2 focuses on integrity and authenticity.

Grasping the collection devices and sources of electronic evidence in modern technology is a job within itself. Electronic evidence emanates from personal computers, laptops, PDAs, cell phones, servers, printers, networks, internet service

providers, websites, and numerous types of software such as databases and email writers. This evidence is collected in forms such as magnetic and optical media, live memory (RAM), and various printouts. With the ever-changing face of technology and the multitude of places electronic data can hide, this type of evidence can be very difficult to track and there is a greater risk of missing something. Devices and software are frequently replaced, updated, and discarded at a fast rate. Thus, courts and parties must implement guidelines and systems with the flexibility to adapt to new technology and capture evidence in different locations.

By implementing a system that will control the collection and preservation of electronic evidence, the CJLE organizes the evidence so the fact finder can easily navigate, comprehend, and weigh the evidence. Before evidence can be preserved, it must be collected. The collection of electronic evidence is a crucial phase in the litigation process because evidence that is not collected cannot be preserved. Evidence that is not preserved will likely be altered or destroyed. Alteration or destruction of evidence can lead to disputes about the evidence's authenticity and admissibility and can even result in the evidence becoming inadmissible. Evidence that is destroyed can lead to the imposition of serious sanctions on the spoliating party. Thus, any best practice for handling electronic evidence must address the proper collection and preservation of the evidence.

9.1. Guidelines for collecting and preserving electronic evidence

The first step in preserving digital evidence is to make a copy of the evidence so that the original evidence is not altered. This is called creating a forensic image. SWGDE explains that a forensic image is an exact duplicate of the original storage medium, bit for bit, and documented to the extent necessary to show that the duplicate exactly represents the original storage medium. This relates to Jordanian law in that an identical representation of the original evidence must be presented to the court so that there is no question on the integrity and authenticity of the evidence. The court has no tolerance for ambiguity, and variations in the presentation of evidence might render it inadmissible in court. This would be the case if the evidence was not a true representation of the original and it could be altered. For example, if the evidence was a file from a computer and the file contained graphics and text, then a forensic image of the file would show exactly how it was, but if the file was opened and viewed in the program that it was created then the file would only show how it was opened and not how it was in its original form.

Preserving digital evidence has become an essential part of criminal investigations. The challenge for law enforcement officers and computer forensic experts is to preserve digital evidence in a way which is forensically sound, so that it can be admitted as evidence in court. Most computer forensic examiners use the guidelines mentioned in SWGDE (Scientific Working Group on Digital Evidence) Best practices for computer forensic which is very helpful to understand how to go about preserving digital evidence. This paper looks at the guidelines stated by SWGDE and how it relates to the handling of evidence in Jordan.

9.2. Ensuring the integrity and authenticity of electronic evidence

The importance of how evidence is collected in determining its integrity is discussed by Ritter (2006), who makes a distinction between system data and application data. Ritter proposes that when an event occurs that is likely to result in litigation, system data should be collected as near to the time of the event as possible and should be preserved in the long term for later examination of its probative value. Ritter describes 'system data' as that which "describes the state of the system at the time the event being investigated occurred" and asserts that effective preservation of this information can provide an accurate representation of the incident in question, thus increasing the probative value of the evidence (Nuisance Lawsuit Alleges Computer System Implemented to Remove Competing Software). This can be contrasted with application data, such as internet history or word processing files, which is more volatile and subject to change. For this reason, Ritter suggests that it is often more practical to collect application data closer to the time it will be used in litigation, as it is less permanent and can incur higher collection costs. Ritter suggests that a professional "cost/benefit analysis" of preserving application data over the long term should be conducted to ensure that undue costs are not incurred for insignificant evidence (Electronic Discovery and Evidence Collection). Although Ritter's proclamations are not specific to Jordanian law, they are useful guidelines for determining the influence of events on the collection of electronic evidence and what methods are best used to ensure the long term preservation and subsequent probative value of information.

Ensuring the integrity and authenticity of electronic evidence is vital to its admissibility in court. Hoda and Rogerson (2008) articulately propose the necessity of preserving the three attributes of evidence: reliability, believability, and trustworthiness. The authors also provide certain points to ensure the aforementioned, such as assessing the probative value

of the evidence, removing any doubt as to the authenticity and correctness of the evidence, and minimizing hearsay. All of this is aimed at producing evidence that is free of tampering or alteration, the hallmark of integrity in electronic evidence.

9.3. Adapting to advancements in technology

In the Jordanian legal system, as well as other systems of law that have been based on traditional documentation, the introduction of electronic evidence with modern technology has created many instances where the judicial system is ill-equipped to handle the challenges of authenticating evidence in digital form. Currently, the doctrine of precedent requires decisions to be based on previous like cases. This principle is difficult when a judge can rely on retrieval of information that with a few keystrokes may adapt the results. Proof provides a major challenge. Information that must be printed or saved as a file is easily adaptable or changeable. This turns an innocent act of information gathering into potential tampering. There are significant application barriers which have prevented the legal system adopting traditional methods of authenticating electronic data, e.g. through test the reliability of the source of evidence and the evidence itself. Encryption and proprietary code of many software companies create a bar among others. The discrepancy between the speed of technological change and the speed at which law evolves necessitates an anticipation of future issues. With globalization, the challenges regarding electronic evidence in court are those faced in countries all over the world. A general set of global standards should be reached enabling a defined set of procedures to be followed.

10. CONCLUSION

The aim of this article was to examine the regime of proof and the methods of evidence in Jordan with an eye on their adequacy to meet the challenges posed by the use of modern technology. It emerged early that the potential problems are enormous, particularly in the context of an inquisitorial system which places great reliance on documentary evidence. A substantial body of primary and secondary legislation has been unearthed in the course of this project which relates to the admissibility and evidential weight of electronic records. However, as elsewhere in the world, the law has struggled to keep pace with technological change. Subject to some modernisation in commercial law statutes, the current regime essentially reflects the era of the typewriter and carbon paper. Although the common law of evidence was received from England, few modern developments are evident save for those which pertain to the practice of the judicial process such as the establishment of the Jordan Institute for Judicial Studies. Thus, to the extent that the law of evidence in the electronic age is a law of evidence in a new key, there is much to be done. A fundamental principle of justice in any system must be the resolution of disputes according to the truth. If modern technology can alter or obscure the truth when it enters the arena of fact-finding, then an important part of access to justice may be lost. This implies the necessity of legal reforms which will facilitate the effective representation of electronic records and the clarification of the effect of their destruction or alteration. This study has identified numerous lacunae in the current law along with some changes that are liable to do more harm than good. The search for appropriate solutions will require an understanding of what electronic records can and will do, and their implications for the fact-finding process. This involves a mastering of the technology itself, an area where lawyers and judges have generally feared to tread. The subjective incompetence of decision makers in this aspect was identified as a problem in the ABA report on electronic records and remains so today. If the law is to harness technology, it will require not only training for legal professionals, but consultation with experts on the capabilities and limitations of information systems.

10.1. Summary of key findings

However, a more comprehensive statement on what constitutes electronic evidence is necessary. Specific provisions on evidentiary presumptions pertaining to electronic documents should also be included. This is an area in which many common law jurisdictions have been developing, such as section 69 of the UK's Criminal Justice and Immigration Act 2008 which creates a presumption that certain documents are authentic and have not been altered.

Establishing a comprehensive framework for the admission and weight of electronic evidence. The first step in achieving this would be to develop clear and consistent definitions of "electronic evidence" and "electronic document" to be incorporated into the relevant legislation. The Royal Decree on e-Transactions and Communications Concerning Commercial and Non-Commercial Transactions and Signature no. 85 of 2001 contains some relevant definitions of electronic records and e-signatures which could serve as a useful starting point.

The comparative approach demonstrated in this study clearly shows that Jordan has made significant strides in the regulation of electronic evidence. Nevertheless, compared to other jurisdictions such as the United States and the United Kingdom, Jordan is still at an early stage of development and has much to learn. Therefore, it will be beneficial for Jordan to learn from the experience of other jurisdictions in developing its own electronic evidence laws. The following list of recommendations has been drawn up with specific reference to the comparative findings in this study and are designed to assist in the refinement and further development of electronic evidence laws in Jordan.

10.2. Implications for the future

In many cases, the law has failed to keep pace with technology, particularly in common law legal systems, and it has been necessary for rulings in case law to effectively set precedent and create law or amend the interpretation of statute to account for the changes. This presents a potential issue in Jordan, the mixed legal system. Should statutory law fail to keep pace with technological progress, there may be pressure to change systems and depend more on case law and the doctrine of stare decisis, which is not well established in the present legal system. This could lead to problems of uncertainty and inconsistency in law. Case law and amendments to interpretation can result in a body of law becoming complex and unwieldy. This has happened in the United States with the formation of an Electronic Communications Privacy Act of 1986 and a plethora of complex case law interpreting its application to new technologies, suggesting a law which lacks simplicity and clarity.

In many ways, the research suggests that the capability and admissibility of electronic evidence in the Jordanian legal system is quite advanced. The fact that the law in many areas, in particular the Evidence Law, is not only able to cope with most eventualities, but also in certain areas pre-empt the advances witnessed in electronic communications, suggests a legal system that is both flexible and robust. That said, however, computer and communications technology advances at a truly remarkable rate, and should history repeat itself in any form, it is likely that law will once again fail to keep pace with technological advancement.

10.3. Recommendations for improving electronic evidence procedures

The law is well-advanced in Jordan and Jordanian judges have a good understanding of the Anglo-Saxon system of justice. It would be fair to say that Jordan is keeping pace with legal developments in developed nations. The requirement of a typed statement for evidence is an important procedural move. Without this, evidence will not be clear, easy to read, and easily accessible in electronic form. It is suggested that the procedures in Part 27 of the Civil Procedure rules regarding 'evidence' are scrutinised with the view to be incorporated into the Jordanian system. These procedures make an attempt to account for the potential use of all forms of electronic evidence, and suggest that parties give advance notice of the intention to rely on it. This will help to increase awareness of electronic evidence among judges and lawyers, as well as providing the evidence giver more certainty as to the admissibility of the method. However, the UK provisions only are sufficient for an internet document in exceptional cases, and do not yet account for the diversity of modern technology. It is clear that Jordan is in need of guidelines on the admissibility of electronic evidence. As demonstrated throughout this study, the laws of evidence were designed for written evidence and electronic evidence is forced into an unsuitable framework. Before the rules of evidence can be modified, repealed or rewritten to account for the changes in technology, the judiciary and lawyers must have a sufficient understanding of the evidence, how it was obtained, and what it represents. This requirement for understanding coincides with the definition of weight in Article 38 of the Evidence Law. The Evidence Law does not provide any guidance on how to assess the weight of electronic evidence compared to similar written evidence. Weight is currently assessed by judges who have the authority to disregard evidence they feel is unconvincing. A provision should be made to state that electronic evidence under Article 32 is admissible to the same extent as other evidence, thereby repealing Articles 33-37 which create presumptions about documentation execution method.

REFERENCES

[1] MA KAMASE - 2023 - dspace.uii.ac.id. The Action Of Sharing Consumer Reviews On Social Media From The Perspective Of The Electronic Information And Transactions Act. uii.ac.id

[2] J Sitompul - 2020 - torrossa.com. Cross-border Access to Electronic Evidence: Improving Indonesian Law and Practice in Investigating Cybercrime. [HTML]

[3] NK Wardani, A Afriansyah - 3rd International Conference on Law …, 2020 - atlantis-press.com. Indonesian legal challenges regarding electronic contracts in international trade. atlantis-press.com Cited by 7

[4] E Makarim - Data Protection Around the World: Privacy Laws in …, 2021 - Springer. Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach. [HTML] Cited by **4**

[5] AY Alfred, NMAA Putri - … On Religion, Culture, Law, Education …, 2022 - prosiding.iahntp.ac.id. The Use Of Electronic Evidence In Civil Jurisdiction Processes In Indonesian Law Courts. iahntp.ac.id

[6] N Fatmawati Octarina, T Effendi… - International Journal of … - repository.narotama.ac.id. The Urgency of Personal Data Protection Laws in Indonesia. narotama.ac.id

[7] N Fatmawatia, T Effendib, A Ulfac - ijicc.net. The Urgency of Personal Data Protection Laws in Indonesia. ijicc.net

[8] MAA Dari, NM Oktarina - Rechtenstudent, 2023 - rechtenstudent.uinkhas.ac.id. Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims. uinkhas.ac.id Cited by **1**

[9] AB Riswandi, M SH - 2020 - dspace.uii.ac.id. Legal Protection For User Data In Fintech Peer To Peer Lending Rupiah Cepat. uii.ac.id Cited by **1**

[10] SR Tsary - ijmra.in. Consumer Legal Protection on Electronic Transactions through the Platform without the Collective Account Features by Trusted Third Parties. ijmra.in

[11] MIA El-Haija - Global Journal of Politics and Law Research, 2024 - tudr.org. The Role of Proof of Written Vice Electronic Documents: A Study of the Laws of Jordan and the United Arab Emirates. tudr.org

[12] IAM Thunibat - Russian Law Journal, 2023 - cyberleninka.ru. MODERN MEANS OF PROOF IN ADMINISTRATIVE CASES: A COMPARATIVE STUDY (FRANCE EGYPT–JORDAN). cyberleninka.ru

[13] MMM Airout, SIAA Azam - Migration Letters, 2023 - migrationletters.com. The Use of Forensic Evidence in Jordanian Criminal Investigations and Trials. migrationletters.com

[14] II Al Saleh - Pt. 2 J. Legal Ethical & Regul. Isses, 2021 - HeinOnline. The Procedural Framework for the Electronic Blackmail Crime in the Jordanian Criminal Legislation. [HTML]

[15] IF Rayyan, NA Al-Dabbas… - Journal of Namibian …, 2023 - namibian-studies.com. The authority of the electronic document in case of conflict with the paper document according to the Jordanian legislation and the comparative legislation" …. namibian-studies.com Cited by **1**

[16] F Shawabkeh, T Shiyab - The Lawyer Quarterly, 2023 - tlq.ilaw.cas.cz. … and analytical study of the compatibility of witness testimony through videoconferences with good governance in criminal proceedings in the UAE and Jordan. cas.cz

[17] MAQ Nayel Al Omran - Journal of Southwest Jiaotong University, 2021 - jsju.org. Authenticating electronic administrative contract and its legal force before the Jordanian judiciary. jsju.org Cited by **1**

[18] SM Awaisheh - International Journal of Cyber Criminology, 2023 - cybercrimejournal.com. Digital Justice in Jordan: The Role of Virtual Arbitration Sessions in Modernizing the Legal System. cybercrimejournal.com Cited by **1**

[19] WMB Al-Wazzan, AKA Al-Sufani - … Electronic Comprehensive Journal For …, 2021 - mecsj.com. Approval In The Evidence Act And Its Amendments.. mecsj.com

[20] RM El-Kady - journals.nauss.edu.sa. Accepted Manuscript Provisional PDF. nauss.edu.sa

[21] S Porsdam Mann, BD Earp, N Møller… - The American Journal …, 2023 - Taylor & Francis. AUTOGEN: A personalized large language model for academic enhancement—Ethics and proof of principle. tandfonline.com Cited by **29**

[22] J Lasky-Fink, E Linos - Journal of Public Administration …, 2024 - academic.oup.com. Improving delivery of the social safety net: The role of stigma. harvard.edu Cited by **2**

[23] PA Homan, TH Brown - Health Affairs, 2022 - healthaffairs.org. … Of Being Excluded: Structural Racism In Disenfranchisement As A Threat To Population Health Equity: Study examines structural racism in disenfranchisement as a …. healthaffairs.org Cited by **38**

[24] P Sankaridurg, N Tahhan, H Kandel… - … & visual science, 2021 - iovs.arvojournals.org. IMI impact of myopia. arvojournals.org Cited by **207**

[25] A Advani, H Tarrant - Fiscal Studies, 2021 - Wiley Online Library. Behavioural responses to a wealth tax. wiley.com Cited by **58**

[26] M Viecca, D Radovanovic, GB Forleo… - Pharmacological research, 2020 - Elsevier. Enhanced platelet inhibition treatment improves hypoxemia in patients with severe Covid-19 and hypercoagulability. A case control, proof of concept study. nih.gov Cited by **138**

[27] R Yearby, B Clark, JF Figueroa - Health Affairs, 2022 - healthaffairs.org. Structural Racism In Historical And Modern US Health Care Policy: Study examines structural racism in historical and modern US health care policy.. healthaffairs.org Cited by **208**

[28] AYL Chan, VKY Chan, S Olsson, M Fan, M Jit, M Gong… - Value in Health, 2020 - Elsevier. Access and unmet needs of orphan drugs in 194 countries and 6 areas: a global policy review with content analysis. sciencedirect.com Cited by **58**

[29] YM Rodgers, E Coast, SR Lattof, C Poss, B Moore - PloS one, 2021 - journals.plos.org. The macroeconomics of abortion: A scoping review and analysis of the costs and outcomes. plos.org Cited by **26**

[30] …, C Calvert, A Crampin, T Dadirai, A Dube… - The Lancet …, 2021 - thelancet.com. Age patterns of HIV incidence in eastern and southern Africa: a modelling analysis of observational population-based cohort studies.

[31] D Chalmers, C Fisch, R Matthews, W Quinn… - Journal of Business …, 2022 - Elsevier. Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs?. sciencedirect.com Cited by **170**

[32] K Smith, E Ostinelli, O Macdonald, A Cipriani - JMIR mental health, 2020 - mental.jmir.org. COVID-19 and telepsychiatry: development of evidence-based guidance for clinicians. jmir.org Cited by **142**

[33] …, S Panagiotakis, E Pallis… - … Surveys & Tutorials, 2020 - ieeexplore.ieee.org. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. ieee.org Cited by **756**

[34] R Auer, G Cornelli, J Frost - 2020 - papers.ssrn.com. Rise of the central bank digital currencies: drivers, approaches and technologies. econstor.eu Cited by **462**

[35] S Bose, EKY Lim, K Minnick… - … : An International Review, 2024 - Wiley Online Library. Do foreign institutional investors influence corporate climate change disclosure quality? International evidence. wiley.com Cited by **7**

[36] SQ Meng, JL Cheng, YY Li, XQ Yang, JW Zheng… - Clinical psychology …, 2022 - Elsevier. Global prevalence of digital addiction in general population: A systematic review and meta-analysis. google.com Cited by **205**

[37] S Nazah, S Huda, J Abawajy, MM Hassan - Ieee Access, 2020 - ieeexplore.ieee.org. Evolution of dark web threat analysis and detection: A systematic approach. ieee.org Cited by **68**

[38] S Omboni, RS Padwal, T Alessa, B Benczúr… - Connected …, 2022 - ncbi.nlm.nih.gov. The worldwide impact of telemedicine during COVID-19: current evidence and recommendations for the future. nih.gov Cited by **196**

[39] AMA Ausat, S Suherlan - BASKARA: Journal of Business and …, 2021 - jurnal.umj.ac.id. Obstacles and solutions of MSMEs in electronic commerce during covid-19 pandemic: evidence from Indonesia. umj.ac.id Cited by **100**

[40] K Parajuly, C Fitzpatrick, O Muldoon, R Kuehr - Resources, Conservation & …, 2020 - Elsevier. Behavioral change for the circular economy: A review with focus on electronic waste management in the EU. sciencedirect.com Cited by **215**

[41] MMM Airout, SIAA Azam - Migration Letters, 2023 - migrationletters.com. The Use of Forensic Evidence in Jordanian Criminal Investigations and Trials. migrationletters.com

[42] A Abuanzeh, E Søndergaard - Arab Law Quarterly, 2023 - brill.com. International Perspectives on Jordan's Legislation on Deprivation of Liberty Prior to Trial. [HTML]

[43] A Aldmour - 2021 - researchgate.net. Jordanian case law on recognition and enforcement of foreign judgments and foreign arbitral awards. researchgate.net Cited by **1**

[44] BMAR Tubishat - International Journal of Religion, 2024 - ijor.co.uk. Electronic Commerce and Consumer Protection in Jordan: The Emerging Trend. ijor.co.uk

[45] V Shapovalov - SSP Modern Law and Practice, 2023 - ssp.ee. Interdisciplinary legal, forensic and pharmaceutical, forensic and chemical, forensic and narcological, forensic and toxicological, criminal and legal study of the illegal …. ssp.ee Cited by **5**

[46] A Amoako - J. Legal Ethical & Regul. Isses, 2023 - HeinOnline. Legal Issues and Challenges of Searching and Seizing Hardware and Software as Evidence for Prosecution in Ghana. [HTML]

[47] M Wasek-Wiaderek - Rev. Brasileira de Direito Processual Penal, 2021 - HeinOnline. Admissibility of Statements Obtained as a Result of" Private Torture" or" Private" Inhuman Treatment as Evidence in Criminal Proceedings: Emergence of a New …. redalyc.org

[48] B Malkawi - Research Handbook on Digital Trade, 2023 - elgaronline.com. Legal approaches to the regulation of digital trade by Middle Eastern countries. [HTML]

[49] L Jordan-Philbert - 2023 - search.proquest.com. A Retrospective Investigation of Intimate Partner Violence's Impact on Well-Being and Relationships: A Phenomenological Study. [HTML]

[50] W Zhang, D Eike, L Pasquero, A Mahieu… - Global Journal of …, 2023 - irep.ntu.ac.uk. … -based violence in humanitarian settings: A qualitative analysis of international guidelines for humanitarian practitioners and scoping review of existing evidence. ntu.ac.uk

[51] MMM Airout - Russian Law Journal, 2023 - cyberleninka.ru. Criminal Evidence With Modern Technology And Its Impact On Basic Freedoms In Jordanian Legislation. cyberleninka.ru Cited by **1**

[52] MIA El-Haija - Global Journal of Politics and Law Research, 2024 - tudr.org. The Role of Proof of Written Vice Electronic Documents: A Study of the Laws of Jordan and the United Arab Emirates. tudr.org

[53] IAM Thunibat - Russian Law Journal, 2023 - cyberleninka.ru. MODERN MEANS OF PROOF IN ADMINISTRATIVE CASES: A COMPARATIVE STUDY (FRANCE EGYPT–JORDAN). cyberleninka.ru

[54] MMM Airout, SIAA Azam - Migration Letters, 2023 - migrationletters.com. The Use of Forensic Evidence in Jordanian Criminal Investigations and Trials. migrationletters.com

[55] II Al Saleh - Pt. 2 J. Legal Ethical & Regul. Isses, 2021 - HeinOnline. The Procedural Framework for the Electronic Blackmail Crime in the Jordanian Criminal Legislation. [HTML]

[56] MAQ Nayel Al Omran - Journal of Southwest Jiaotong University, 2021 - jsju.org. Authenticating electronic administrative contract and its legal force before the Jordanian judiciary. jsju.org Cited by **1**

[57] IF Rayyan, NA Al-Dabbas… - Journal of Namibian …, 2023 - namibian-studies.com. The authority of the electronic document in case of conflict with the paper document according to the Jordanian legislation and the comparative legislation" …. namibian-studies.com Cited by **1**

[58] WMB Al-Wazzan, AKA Al-Sufani - … Electronic Comprehensive Journal For …, 2021 - mecsj.com. Approval In The Evidence Act And Its Amendments.. mecsj.com

[59] SM Awaisheh - International Journal of Cyber Criminology, 2023 - cybercrimejournal.com. Digital Justice in Jordan: The Role of Virtual Arbitration Sessions in Modernizing the Legal System. cybercrimejournal.com Cited by **1**

[60] RM El-Kady - journals.nauss.edu.sa. Accepted Manuscript Provisional PDF. nauss.edu.sa