Educational Administration: Theory and Practice
2024, 30(4), 6902-6909
ISSN: 2148-2403
https://kuey.net/

Research Article

The Role Of Cybercrime Scene Investigation In Enhancing Digital Evidence And Its Admissibility

Fathi Al Fauri*

*Department of Law, Faculty of Law, Petra University, Amman-Jordan
fathifaouri@yahoo.com

Citation: Fathi Al Fauri (2024 The Role Of Cybercrime Scene Investigation In Enhancing Digital Evidence And Its Admissibility , *Educational Administration: Theory and Practice*, *3*(4), 6902-6909
Doi: 10.53555/kuey.v30i4.2490

ARTICLE INFO **ABSTRACT**

This study aims to examine the role of cybercrime scene investigation in enhancing digital evidence. The descriptive and analytical approach was used by describing the problems related to digital evidence's privacy and the obstacles it creates in extracting digital evidence from the electronic crime scene. The findings reflected that the authority in digital evidence is not solely related to its content as evidence, but rather to independent factors related to its credibility. The credibility of digital evidence is of utmost importance and depends on the proper functioning of the electronic crime scene. The most important recommendations imply enabling judges and prosecution members to pursue and prosecute offenders of information technology crimes.

Keywords: Cybercrime, Digital Evidence, Electronic Crime Scene, Digital Evidence Credibility, Criminal Proof, Procedural Challenges.

Introduction

Investigating cybercrimes is one of the most complex and challenging processes, demanding the use of sophisticated and evolving technologies, especially due to the unique nature of these crimes. While they may share traditional crime labels such as theft, extortion, fraud, forgery, defamation, and libel, they are fundamentally different from conventional crimes. Hence, the importance of the role of the electronic crime scene cannot be overstated.

This research holds great importance, particularly since many studies have neglected to define and clarify the electronic crime scene's significance, despite it being the environment where these cybercrimes are committed. Without it, extracting the cornerstone of criminal proof, i.e., digital evidence, becomes impossible. The digital evidence must meet all requirements to convince a criminal judge and constitute the main basis for imposing penalties on the perpetrators.

Therefore, this study is an endeavor to answer the main question: What is the role of cybercrime scene investigation in enhancing digital evidence? It was seeks to answer the sub-questions: What is the nature of the electronic crime scene?,How does digital evidence differ from traditional physical evidence? Does the electronic crime scene play a role in enhancing digital evidence? Are there procedural challenges faced by the electronic crime scene in extracting digital evidence and ways to overcome them?

Furthermore, this study seeks to achieve the main objective represented in identifying the role of cybercrime scene investigation in enhancing digital evidence. Besides, it ventures to define the electronic crime scene, describe the unique nature of the electronic crime scene, address difficulties and obstacles related to investigating cybercrimes, highlight the role of the electronic crime scene in extracting digital evidence, and explore how the electronic crime scene enhances digital evidence's credibility before the criminal justice system.

Literature Review

The importance of crime scene investigation is evident in traditional crimes, where a physical crime scene exists, containing tangible physical traces. The purpose of crime scene investigation is to preserve and examine these traces to determine their validity as evidence. However, the situation seems different in the field of cyber crimes, where physical traces are rare. Moreover, the period between the commission and discovery of cyber crimes can be prolonged, exposing the remnants of the crime to damage and erasure.

The cyber crime scene faces various technical obstacles that hinder law enforcement agencies during the investigation process. Digital evidence, like other physical evidence, requires proper preservation, documentation, and protection to ensure its credibility and prevent any flaws.

Some define the electronic crime scene as "the spatial location where the criminal incident occurred, encompassing all its specific details, particularly the criminal event. It refers to any changes made to the physical stability of the place where the crime occurred" (Attia, 2012). Additionally, it can be defined as "the location where all evidence originates, guiding the police officer to initiate the search for the perpetrator and uncover the evidence supporting the accusation. It also serves in reconstructing the crime." (Al-Hawqal, 1999) Furthermore, the electronic crime scene can be described as "any place or unit, whether a facility or a piece of land, that contains the core of the crime and its center (Al-Habashi, 1995). It serves as a field for the original perpetrators to engage in criminal activities or attempt to commit them." In our opinion, the cyber crime scene refers to the place or places where the crime was committed, either above, on, or inside it. It contains and reveals the secrets of the crime, (Mamdouh, 2009) leading to the identification of its perpetrators.

In this respect, we should refer to the cyber forensics laboratory which deals with the scientific utilization of knowledge to collect, preserve, analyze, and evaluate evidence obtained from electronic devices like computers, CDs, printers, scanners, etc., which are used for unlawful purposes. The derived evidence must be reliable and stand up to scrutiny. Digital forensics is one of the fastest-growing professions in combating digital crimes (Huang & Yin).

There are different classifications of cyber forensics laboratories (Gershtegn, et al). These include Hardware Forensic Laboratory which deals with analyzing hardware devices to extract relevant data, Software Forensic Laborator, which focuses on analyzing software and applications to extract information. They also include Network Forensic Laboratory: Involves the analysis of data traffic over networks, tracing cyber-attacks and illegal activities.

Here, it is urging to discuss the digital evidence that encompasses all data that can prove the occurrence of a crime, establish a connection between the crime and the perpetrator, or establish a connection between the crime and the victim. It includes a wide range of digital data, such as written texts, graphics, maps, audio, images, and more (Brown, 2015).

Digital evidence is a legitimate evidential means that helps the judge achieve certainty through scientific examination or interpretation of data, presented in the form of written texts, graphics, or audio, to prove or disprove a specific matter in the case (Al-Maghaita & Al-Muqadhali) It must be legally obtained through proper procedures, analyzed scientifically, and presented in a credible form before the court to reach a verdict of innocence or guilt (Salibia, 1993).

Linguistically, the evidence is the guide, what is guided by, and what is inferred by it, and the indicative evidence and the plural are evidence, and it also means confirming the truth with evidence, which is the evidence or argument, (Zaki, 1987) and legally the evidence is the means that the judge uses to reach the truth that he seeks, and what is meant by truth in this regard is everything that Relates to the procedures and facts before it to apply the rule of law to it (Diaa El-Din, 1983).

What is meant by evidence or procedural work: every manifestation of activity, whether public or private, within or for the sake of the dispute that directly leads to influencing the development of the dispute, or in other words, it is every action that takes place in the dispute or aims to prepare it (Abed, 1989) and it is the legitimate evidential means that contributes to achieving the case. The judge has certainty in a way that is acceptable and reassuring (Saif, 2004) and evidence is the means obtained by legitimate means to present it to the judge to achieve his state of certainty and rule accordingly, (Me Graw Hill, 2000) and Swanson defines it as “anything that is useful in proving or denying a specific issue in the case or everything that is directly related To convict or acquit the accused based on logic, and the focus must be on the word “anything” in the broad sense that can be evidence. (Casey, 2000) Digital forensic evidence can be defined as a type of forensic evidence, and its definitions have varied. “Ferry Casey” defined it as including all data. Digital data that can prove that a crime has been committed, or that there is a relationship between the crime and the perpetrator, or that there is a relationship between the crime affected by it, and digital data is a group of numbers that represent various information, including written texts, drawings, maps, sound and images.

There are those who see digital evidence as “evidence taken from computers and in the form of magnetic or electrical fields or pulses that can be collected and analyzed using special programs, applications and technology, and presented in the form of evidence that can be relied upon before the judiciary” (Abdel Muttalib, 2007). Some have defined it as “evidence that finds Mainly in the virtual world and leads to crime (Bin Younis, 2006).

Our digital evidence is the evidence derived from or by means of computer information software systems, computer devices, equipment, tools and accessories, or communications networks through precise legal procedures to be presented to the judiciary after scientifically analyzing or interpreting it in the form of written texts, drawings, or it is shapes and sounds to prove the occurrence of the crime. To decide acquittal or conviction therein.

Research Methods

Our study adopts a descriptive and analytical approach by describing the problems related to digital evidence's privacy and the obstacles it creates in extracting digital evidence from the electronic crime scene. We also analyze essential procedures to enhance digital evidence.

Results and Discussion

Most jurists and analysts agree that the crime scene, in general, is the silent witness, which has no suspicion of falsification or distortion in its testimony whenever the handler is able to interrogate it. If this is done, we can, without any dispute, reveal the secrets that its containers hold, and therefore extract sufficient evidence to expose its perpetrators and establish the overwhelming proof against them, ensure their punishment, and achieve the desired goal of punitive legislation, and guarantee the realization of general and specific deterrence. For this reason, it was of utmost importance to address the role of the electronic crime scene in preserving and enhancing digital evidence so that it has legal validity before the judiciary. This is the matter that prompted us to devote the second part to this pivotal issue in our research study, in which we chose to address the means through which the electronic crime scene plays this crucial role, until we move our study to its final part related to the validity of digital evidence in proving.

The Mechanisms of Digital Crime Scene in Enhancing Digital Evidence Electronic evidence refers to valuable information and data obtained, stored, and transmitted through any electronic device. It is acquired when physical items are collected for examination purposes (Farag, 2007).

Electronic evidence is valuable information and data in the investigation and is stored and transmitted by any electronic device with the ability to obtain it when the physical elements contained within it are collected for the purposes of the examination. The precautions that must be taken in harvesting, preserving and examining digital evidence by the person who inspects the digital crime scene is to follow the following steps: identifying and identifying the evidence, documenting the crime scene, collecting and preserving the evidence, packaging and documenting the evidence (Al-Bishri, 2002).

This documented information assumes that this is done by a legal authority competent to collect and possess evidence, and that measures are taken to secure and document the crime scene, including photographing, drawing, and taking notes through the use of protective equipment used when necessary, such as gloves.

With regard to preparing the entity to deal with electronic evidence, the person dealing with a digital crime recorder is supposed to have experience in dealing with digital evidence, and the dealing must also take place within the limits of the laws of the country, especially the law protecting the right to privacy (Al-Maamari, 2019).

The digital crime scene equipment consists of the computer, including the processing unit (CPU) and stored data (DATA), as well as the devices attached to it (the keyboard, mouse, and monitor), and these devices may be connected to the Internet. Also, the files created by the user may contain important evidence that could indicate the crime, such as Database files, still and moving images may be evidence of the crime of child prostitution. Likewise, communications between the accused, e-mail, messages, e-mail files, audio and video files, graphic files, Internet bookmarks, documents, and text files may be considered evidence of the commission of the act (Youssef, 2016).

Files protected by the user are considered a way to hide evidence in various ways, such as encrypting data and protecting it with a password, hiding files on a storage disk, hiding them inside other files, or hiding important evidence under unobtrusive names such as compressed files, encrypted data with password protection, or the SLEGANOGRAPHY method, which is a science. The art of writing hidden messages in such a way that no one other than the sender and the intended recipient can suspect the existence of messages. Data, files, etc. can also be hidden in computer operating systems, as well as back-up file systems. These things are useful in the digital criminal scene in collecting evidence (Abdel Muttalib, 2006).

Computer backup files are also considered BACK UP FLLES - LOG FILES - which record all movements and actions that take place on a specific program or script, and CONFIGRATION FILES - COOKIES files - which are text files that are not programs or codes from which passwords can be discovered, and HISTORY FILES. SWAP FLES Swap files to optimize RAM and temporary files (Dawoud, 2013).

Other data areas can be used to create the directory, which include the damaged sector (BAD CLUSTER), computer date & time, passwords (PASSWORDS), deleted files (LOST CLUSTER), free spaces (FREE SPACE), hidden spaces (HIDDEN PARTITION), lost groups and reserved areas, SLACK SPACE, which are storage areas within Storage disk (Abdel Muttalib, 2015).

Computer components include the central processing unit (CENTRAL PROCESSING UNITS), which contains a MICRO PROCESSOR that performs all the logical arithmetic functions of the computer, controls its operation, and is useful in theft and forgery. They also include access control devices which include SMART CARDS, the DONGLOS Internet communication device, and the automatic answering machine that records calls and voice messages and determines the time and date, but they are easy to lose when the batteries run out or the power goes out. DIGITAL CAMERA records photos and video and displays Save them and transfer photos and videos to your computer or display screens. Moreover, they include portable personal assistance devices such as computers, telephones, faxes, and pagers that are useful in (text messages, voice messages, documents, and e-mail), hard drives, storage disks for files, MEMORY CARDS, and modems, which are used to connect to the Internet, or connect computers to each other on the Internet, Local LAN card, LOCAL AREA NETWORK, ROUTERS, HUB devices, SWITCH devices, Sir VR which provide some services for other computers not connected to the network, Internet connection cables.

Computer components also include removable storage devices, CDs, DVDs, recording tapes, and scanner devices which are useful in child prostitution and counterfeiting of telephones, along with various other electronic devices such as credit cards, cell phones, audio recording devices, credit card skimmers, and DIGITAL WATCHES. They also include investigation tools to collect digital evidence. In this respect, we have the TOOL KIT that contains crime scene examination supplies such as a notebook camera, drawing board, and marking tape (Abdel Baqi, 2018). Moreover, there are other tools and equipments like connecting devices such as connecting cables and non-removable marking tape, disassembly tools, which are a variety of screwdrivers that fit all of the above and transportation supplies: such as static bags for packing, plastic bags, evidence collection bags, evidence tape, adhesive tapes, cardboard boxes of different sizes, and shock-absorbent packaging tools. Other tools are represented in gloves, a wheel for transporting and carrying tools with tires, rubber bands, a list of phone numbers, a magnifying glass, printing paper, a storage disk, and a small flashlight.

The necessary precautions in collecting, preserving, and examining digital evidence require the digital crime scene investigator to identify and define the evidence, document the crime scene, collect and preserve the evidence, package, seal and label the evidence.

On the other hand, the documentation process implies that it should be carried out by a legally authorized authority to collect and possess evidence. In this respect, the crime scene is secured and documented (photographs, sketches, notes, wearing protective gear when necessary, such as gloves). Here, the question "Is the entity prepared to deal with electronic evidence?" is raised. In this respect, the individual handling the digital crime scene is expected to have expertise in dealing with digital evidence and must adhere to the laws of the country, especially privacy protection laws.

The types of digital crime scene equipment include the computer with its Central Processing Unit (CPU), Stored Data(DATA), associated devices like keyboard, mouse, and screen, which may also be connected to the internet, files created by the user may contain crucial evidence of the crime, such as database file static and animated images, which may indicate crimes like child prostitution, communications between suspects, Email content, messages, audio files, video files, graphic files, Internet bookmark, and text documents and files.

Users may hide evidence in various ways, such as encrypting data, protecting it with a password, hiding files on storage disks, concealing files within other files, or hiding essential evidence under inconspicuous names, like compressed files. Data can also be concealed using steganography, which is the art of writing hidden messages in a way that no one other than the intended recipient can suspect the presence of messages. Data and files can be hidden in computer operating systems. Also, backup files are beneficial in the digital crime scene for collecting evidence.

Files created by the computer include backup files, log files (record all actions and operations performed on a specific program or script), configuration files, cookies (text files that do not reveal passwords), history files, swap files (used to optimize RAM), and temporary files.

Other data areas include bad clusters (damaged sectors), computer date and time, passwords, deleted files (lost clusters), free space, hidden partitions, lost groups, reserved areas, slack space (storage areas within the storage disk)

Computer components include Central Processing Units (CPUs) which are microprocessors that perform all the computational and logical functions of the computer. They can be used for theft and forgery, Access Control Devices, which are Smart cards, internet dongles, answering machines (records calls and voice messages with timestamps but can be easily lost due to battery depletion or power outage), and digital cameras (record images and videos and store them for transfer to computers or display screens). They also include Personal Digital Assistants (PDAs), which are handheld devices like calculators, phones, fax machines, and pagers that facilitate tasks such as text messaging, voice messages, document handling, and email.

Computer components also included hard drives, which are storage disks for files, memory cards, which are used for data storage, modem devices, which are used for internet connection or connecting computers to the internet, Local Area Network (LAN) cards, which are used for connecting computers within a local network, routers, hubs, switches, which are networking devices that provide services to computers not directly connected to the network, internet communication cables. They also include removable storage devices: CDs, DVDs, recording tapes, and scanners, other electronic devices: Credit cards, mobile phones, voice recorders, credit card skimmers, digital watches, etc., Investigation tools and equipment: Toolkits containing examination necessities like cameras, notepads, drawing boards, securing tapes, and markers, connecting tools like cables and non-removable securing tapes, disassembly tools: Various screwdrivers suitable for different tasks, and transport supplies: Static packing bags, plastic bags, evidence collection bags, evidence tapes, adhesive tapes, various-sized cardboard boxes, shock-absorbing packaging materials. Other tools include gloves, a trolley for transporting and carrying tools with wheels, elastic ties, a phone number list, a magnifying lens, printing paper, storage disks, a small flashlight.

Securing the digital crime scene involves protecting physically and electronically vulnerable data, which may exist in devices like pagers, and documenting, photographing, and securing it. It also involves identifying and documenting the connected phone lines to the modem, categorizing and disconnecting them, securing the keyboard, mouse, CDs, or any component that may contain fingerprints or physical evidence. Care should be taken as some chemicals used by forensic investigators may damage electronic devices. Furthermore, it involves conducting preliminary interviews to separate all individuals, identify witnesses, record their statements upon arrival at the crime scene, and gather information in accordance with legal regulations, determining the owner and user of electronic devices present at the crime scene, including network credentials, passwords for operating systems or data, encryption keys, email, access codes, tables, contact lists, any bypass or destruction software, hidden data, and documentation of the devices and software installed on the computer.

On the other hand, preliminary documentation of the crime scene involves documenting the physical scene, such as the placement of computer peripherals like the mouse, CPU, etc., documenting the condition and location of the computer system, indicating whether it was in an operational or standby mode, as indicated by the cooling fan sound or if it was warm, indicating recent power-off, identifying and documenting the connected peripheral components to be collected, photographing the interior scene to retain a physical image of the crime scene, photographing the computer, screen, and other components and making written notes such as serial numbers, brand names, and any relevant documents or videos, collecting evidence should be done carefully to preserve the associated devices.

In this respect, inspecting the laptop involves checking whether it is connected to the internet or not, observing the screen status, whether it is turned on, off, or in standby, and following appropriate procedures for each state, if in a relaxed state, moving the mouse without pressing any keys and noting changes in the screen display and the last state of programs. It also photographing the screen and recording the displayed information, removing the laptop battery, verifying external connections such as the modem, phone, ISDN, DSL, and identifying the phone number when it was in connection with the network. To avoid potential evidence damage, it involves removing any storage media like CDs, floppy disks, CD drives, and avoiding touching any disks to prevent damage and leaving them in the drives. It also involves placing a tape over all disk drive slots and power connectors, recording the country of origin, model, and serial number of the device, labeling all links and cable ends for precise reassembly later, labeling used and unused ports, recording procedures according to instructions and guidelines followed Transport in breakable packaging labeled appropriately: In complex environments, this type of crime scene involves multiple interconnected devices through a central server ("host"). Securing and preparing the crime scene, especially when the devices are connected, can present various challenges. Improper shutdown of these devices could result in data loss and the disappearance of evidence crucial to identifying criminal activity.

Therefore, careful planning is necessary when examining the crime scene, seeking the assistance of experts knowledgeable about these devices and complex operating systems that require different shutdown procedures. Indicators that may be present include the presence of multiple computer systems (Al-Ghaferi, 2005), the presence of connecting cables such as HUBs and SWITCHES, and information provided by guides and individuals present at the crime scene.

Packaging and handling procedures include ensuring that all electronically packed evidence is properly documented, labeled, preserved, and cared for, storing magnetic media in static-free plastic containers, avoiding storing materials that can generate static electricity in plastic bags, avoiding folding, scratching, or bending computer media such as CDs and disks, and confirm that all evidence containers are correctly labeled. On the other hand, transport procedures include keeping electronic evidence away from any magnetic fields, radios, heated seats, or any heat sources to avoid damage. It also avoiding long-term storage of electronic evidence in vehicles under extreme hot, cold, or humid conditions, and ensuring that all electronic components are securely transported in vehicles, avoiding placing them on the floor to prevent violent vibrations (Al-Jabbara, 2010).

In this respect, storage procedures include ensuring that all evidence is stored according to management instructions, away from high temperatures, humidity, and any adverse conditions that could cause damage. It also includes storing evidence away from any magnetic fields (Sammes & Jenkinson, 2000). Significantly, different legal systems have different positions regarding criminal evidence. In this respect, according to The Legal Evidence System, the legislator specifies the evidence that the judge can rely on for proof. The legislator also determines the probative value of each piece of evidence. The role of the judge is limited to examining the evidence to ensure that it meets the conditions defined by the law. This system is known as the legal scope of evidence (Al-Jabour, 1984). Furthermore, the Free Proof System is followed in Latin legal systems. According to this system, the criminal judge has absolute freedom in evaluating the facts presented to them. The judge is not bound by specific evidence that needs to be presented; they have the discretion to consider any evidence they find relevant in forming their conviction. The legislator does not specify the types of evidence that the judge should rely on, giving them wide discretion in assessing the evidence and forming their conviction (Farag, 1982). In such a system, evidence is not prioritized based on its textual content; all evidence is considered equal in probative value in the eyes of the legislator. The judge has the discretion to choose among the presented evidence what he deems relevant to reach the truth. The judge enjoys absolute freedom to accept what he finds convincing and reject what he does not find convincing, even if the evidence is valid. According to this system, the presumption is that all evidence exists legitimately, making digital evidence admissible as a presumption of its existence (Al-Hijjawi, 2014).

The mixed system of evidence combines both the restricted and free systems of evidence. It is prevalent in many legal systems that generally follow the principles of the free system of evidence, with exceptions in specific crimes where the restricted system is applied. Some argue that the mixed system emerged as a result of the evolution of the free system of evidence and due to specific exceptions that were introduced. Secondly, the probative value of digital evidence in criminal justice involves merely obtaining digital evidence and presenting it to the court is not sufficient to rely on it as evidence for conviction. This type of evidence can be manipulated, altering its true content, and only experts can detect such tampering. Thus, the mere possession of digital evidence does not guarantee its credibility in criminal trials. The possibility of errors in obtaining accurate digital evidence seems high, which raises doubts about its reliability as criminal evidence. Does this mean that digital evidence should be excluded from criminal evidence due to its conflict and potential for exculpatory evidence According to the Latin system of evidence, the judge has broad discretion in evaluating the evidence and determining its admissibility. The judge has the authority to accept or reject evidence based on his conviction, including scientific evidence. However, the judge must be knowledgeable about technical aspects related to digital evidence and the laws and standards regarding its admissibility in criminal cases. Additionally, specialized experts should be involved in verifying the authenticity and reliability of digital evidence, analyzing it, and assisting the judge in making decisions (Al-Bishri, 2000). In conclusion, robust and reliable procedures should be in place to handle digital evidence in criminal justice. It should be treated with caution and care to ensure its strength and validity as evidence in legal proceedings. In such a system, when the conditions of certainty are met, the judge cannot exercise his authority to verify the establishment of the facts presented by the digital evidence. However, it does not contradict the fact that digital evidence remains subject to doubt regarding its integrity and the validity of the procedures used to obtain it. There are two aspects of doubt in digital evidence. The first aspect involves that digital evidence can be tampered with to present a certain incident in a way that contradicts the truth. This tampering may not be detectable by anyone other than an expert, making it a prevalent concern when evaluating all digital evidence presented to the court. Modern technology allows for easy manipulation of digital evidence, making it appear as an authentic version. The second aspect implies that although the technical error rate in obtaining digital evidence is extremely rare, it remains possible. Technical errors in obtaining digital evidence can be attributed to two reasons: a) Errors in using the appropriate tool to obtain digital evidence, resulting from defects in the code used or incorrect specifications. b) Errors in extracting the evidence due to decisions made using tools with less than 100% accuracy, often occurring in data reduction methods or data processing in ways different from the original application.

In conclusion, the authority in digital evidence is not solely related to its content as evidence, but rather to independent factors related to its credibility. The credibility of digital evidence is of utmost importance and depends on the proper functioning of the electronic crime scene.

This study examined the role of the electronic crime scene in enhancing digital evidence in cybercrimes through thorough research, addressing the significance of the electronic crime scene and the evidence presented therein.

Conclusion

This study has examined the role of the electronic crime scene in enhancing digital evidence's credibility for its admissibility in front of the judiciary. The importance of the electronic crime scene in presenting reliable digital evidence has been highlighted throughout the study.

Recommendations

Based on the findings, this study recommends strengthening international cooperation in combating cybercrimes to bridge the gap between national criminal laws, collect evidence, and apprehend criminals, and exchange expertise and information, particularly in the field of electronic forensic investigation. It also stresses the importance of enabling judges and prosecution members to pursue and prosecute offenders of information technology crimes and effectively utilize technical evidence through proper training and preparation, enacting a criminal procedural law specific to digital evidence to avoid applying traditional procedural rules that may create loopholes allowing criminals to evade punishment. Furthermore, it recommends establishing specialized forensic laboratories for cybercrimes and regularly update their capabilities. Additionally, create dedicated criminal courts to handle cybercrimes, equipped with well-trained personnel to effectively deal with this type of crime. By implementing these recommendations, the credibility of digital evidence can be strengthened, ensuring its proper use in the judicial process and promoting effective prosecution of cybercriminals.

References

1. AbdelFattah, A. L. (1989). Technical Inspection Procedures for a Crime Scene, first edition, Dar Al-Hamid for Publishing and Distribution, Amman.

2. AbdelHafeez, A. H. (1989). Criminal Proof by Evidence, PhD thesis, Cairo University.
3. AbdelMuttalib, M. (2007). Digital Forensic Research and Investigation into Computer Crimes, Dar Al-Kutub Al-Qanuni, Al-Mahalla Al-Kubar, Egypt.
4. Abdullah, H. A. (2003). Procedures for collecting evidence in the field of information theft, research for the first conference on the security legal aspects of electronic operations, the Emirate of Dubai, (1).
5. Ahmed, F. S. (1981). Mediator in the Code of Criminal Procedure, Dar Al-Nahda Al-Arabiya, Cairo, 2nd edition.
6. Amir, F. Y. (2016). Criminal Proof of Cybercrime and Jurisdiction therein, 1st edition, Al-Wafa Legal Office, Cairo, 290.
7. Cameron, S. D. (2015). Investigating and prosecuting Cyber crimes: Forensic Dependencies and Barriers to justice, International Journal of Cyber Criminology, 1 (1).
8. Charles R., Neil, C. & Leonard (2000). Criminal investigation ,7th Ed., London , Me Graw Hill.
9. DiaaEl-Din, A. (1983). The Legitimacy of Evidence in Criminal Matters, PhD thesis, Faculty of Law, Ain Shams University.
10. Electronic Crime SceneInvestigation: A Guide for First Responders, Technical Working Group for Electronic Crime Scene Investigation , U.S. Department of Justice Office of Justice Programs Washington, DC 20531.
11. Eoghan, C. (2000). Digital evidence and a computer crime, London; Academic press, 260.
12. Fadi, A. (1995). Technical Inspection of the Crime Scene, Arab Center for Studies and Training Publishing House, Riyadh.
13. Harith, A. D. (2013). Security Risks in Internet Protocol Version 6 (IPv), Arab International Journal of Informatics, Volume Two, Issue Four, Naif Arab University for Security Sciences, Saudi Arabia.
14. Hilali, A. A. Inspection of Computer Systems and Guarantees for the Accused and the Two Known Persons, Dar Al-Nahda Al-Arabiya, 1st edition, Cairo.
15. Hisham, A. H. (2007). Crime Scene Inspection, Without Publishing House, Cairo.
16. Hussein, S. S. (2005). Criminal Policy in Confronting Internet Crimes, a dissertation to obtain a doctorate in law, Faculty of Law, Ain Al-Shams University, Cairo.
17. Ihab, F. A. (2014). The Authority of Digital Evidence in Criminal Proof, Journal of Legal and Economic Sciences, First Issue, Year 56, p. 117.
18. Jamil, S. (1993). The Palestinian Dictionary, Beirut, Dar Al-Kitab Al-Lubani, 1st edition.
19. Jeremy, L. J. (2012). Digital forensic and preservation, the Digital Preservation Coalition England.
20. Jouola, P. (2008). Authorship arribution foundation and trend in information, retrieval now publishers.
21. Junwei, H. ,Yinje, C. & Kyungseok, C. Y. Crime scene investigation, University of Massachusetts Lowell, USA.
22. Khaled, M. (2009). The Art of Criminal Investigation in Cybercrimes, Dar Al-Fikr Al-Jami'i.
23. Mamoun, S. (1977). Criminal Procedure in Egyptian Legislation, Dar Al-Fikr Al-Arabi, Cairo.
24. Mansour, O. A., AbdulMohsen, A. (1423AH). Criminal Evidence, Security Research Journal, King Fahd Security College, Issue 22, Shaaban.
25. Masoud, H. A. (2019). Electronic Guide to Proving Cybercrime, International Kuwaiti Law Journal, (6) 203.
26. Mohamed, O. S. (2004). His projects in the criminal and disciplinary fields, “a comparative study”, with application in the legislation of the United Arab Emirates, doctoral dissertation in police sciences, Mubarak Security Academy, College of Graduate Studies, Egypt.
27. Muhammad, A. A. (2000). Investigation into Computer Crimes, research presented to the Conference on Law, Computers and the Internet, College of Sharia and Law, UAE, 3.
28. Muhammad, A. A. (2003). Investigation and collection of evidence in the field of electronic crimes, research for the first conference on the security legal aspects of electronic operations, the Emirate of Dubai, 1.
29. Muhammad, F. R. (1992). Penal Code and Information Technology Risks, Machinery Library in Assiut.
30. Muhammad, M. A. (1971). The Code of Criminal Procedure in Sudan, Commenting on it, International Press, Cairo.
31. Muhammad, N. A. (2004). Technical Criminal Investigation Skills in Computer and Internet Crimes, “A Survey Study” on Police Officers in the Eastern Province, Master's Thesis in Police Sciences, College of Graduate Studies, Naif Arab University for Security Sciences.
32. Muhammad, O. A. (2012). An in-depth study in the principles of criminal trials, at Al-Sharq University 1 (Middle East University for Postgraduate Studies, for the first semester of the year 2010/2011.
33. Mujab, M. A. (1999). The Role of Physical Trace in Criminal Proof, Naif Arab Academy for Security Sciences, Riyadh.
34. Mustafa, A. (2018). Investigating and Proving Cybercrime in Palestine, Studies, Sharia and Law Sciences, 5.
35. Nasser, I. M. (1987). The Authority of the Criminal Judge in Evaluating Evidence, “A Comparative Study,” PhD dissertation, Faculty of Sharia and Law, Al-Azhar University.
36. Omar, M. Y. (2006). Notes on online criminal proof, Digital Evidence Symposium at the headquarters of the League of Arab States, Cairo, 8-5.

37. Pavel, G., Mark, D. & Sajeet (2006). Forensic analysis of bios chip in advanced digital forensic, Boston Springer, 301-314.
38. Richard, S. (1995). Criminlistics, An introduction to forensic science ,5th ed., Englewood Cliffs, prentice hall.
39. Sammes, T. & Jenkinson, B. (2000). Forensic computer, Apartitioner,s , Guide.
40. Shindre, Debra, Scene of the cybercrime: computer forensic, Handbook, Rockland, MA, sungress publishing.
41. Suadad, S. Introduction to Computer Components Al-Mustaqbal University College, Department of Medical Laboratory Techniques, Computer Principles.
42. Sultan, A. (1984). Rules of Evidence in Civil and Commercial Matters, A Study in Egyptian and Lebanese Law, University House, Beirut.
43. Sultan, A. (1984). Rules of Evidence in Civil and Commercial Matters, A Study in Egyptian and Lebanese Law, University House, Beirut.
44. Taher, A. (2015). Criminal with Digital Evidence, Master's Thesis, Specialization in Criminal Law, Faculty of Law and Political Science, University of M'sila.
45. Tariq, I. A. (2012). The Crime Scene in Light of the Procedural Rules, "Technical Methods", New University House, Alexandria.
46. Tawfiq, H. F. (1982). Rules of Evidence in Civil and Commercial Rules, University Culture Foundation, Alexandria.
47. Vassilaki, I. (1993). Computer crimes and other crimes against information technology in Greece.