Review Article

Journal of Journalism and Media Management

The Role of the Jordanian Public Security in Collecting Digital Evidences and its Impact on the Detection of Crime

Omar Alakayleh

Independent Researcher, Jordan

Corresponding author
Omar Alakayleh, Independent Researcher, Jordan

Received: July 30, 2025; **Accepted:** August 11, 2025; **Published:** August 16, 2025

ABSTRACT

The study aimed at identifying the role of the Jordanian public security in collecting digital evidences and its impact on the detection of crime. The study also used some analytical and descriptive statistical approaches to achieve its objectives the researcher used a questionnaire consisted of two parts to collect field data the population study composed of the workers in the department of laboratories and criminal evidence.

The study sample consisted of 277 workers were chosen randomly. The study concluded that the level of the (technical expertise, administrative and logistical experience, the level of effectiveness of technical security measures in detecting cybercrime) and the high-average and the means of the samples answers was (4.48), technical expertise was (4.48), administrative and logistical experience was (4.45), the level of effectiveness of technical security measures in detecting cybercrime was (4.52). Finally, the study suggested the following recommendations: Providing all the necessary support and training with the technological development of the security services so that they can detect electronic crime with ease, raise the Jordanian society awareness about the dimensions of the dangers of cybercrime.

Keywords: Public Security, Collecting, Evidence, Digital Evidences, Crime

Introduction

The significant technological advancements of our era have led to the emergence of modern technological tools such as computers and the Internet. These tools have profoundly altered individuals' personal habits and social relationships, to the extent that they have become deeply integrated into all aspects of life. It can even be said that humans have become enslaved by technology.

The technological revolution has had positive impacts and brought about a qualitative leap in the lives of individuals and nations, given its speed and accuracy in gathering and storing information. However, it is undeniable that technology has also produced negative effects, most notably the emergence of new types of crimes that did not exist before. These new crimes now pose local, regional, and international threats that endanger the interests of individuals and states across all fields. Accompanying these modern crimes is a new criminal mindset that differs significantly from that associated with traditional crimes [1].

These emerging crimes have posed a major challenge to public security personnel in Jordan, placing a heavy burden on them and requiring efforts that exceed the capabilities offered by traditional investigative procedures and forensic evidence-gathering methods. This is due to the inadequacy of classical systems in proving crimes committed through electronic means, including computers. Traditional investigative techniques are no longer effective in addressing these new types of crimes. As everything around us evolves, Jordan's Public Security Directorate has responded by establishing specialized departments for cybercrime, staffed with highly skilled technical experts. These experts are tasked with extracting and securing digital evidence generated by criminals during the commission of a crime. The process of securing and proving digital evidence requires advanced skills and rapid response at the crime scene.

Citation: Omar Alakayleh. The Role of the Jordanian Public Security in Collecting Digital Evidences and its Impact on the Detection of Crime. J Journalism Media Manag. 2025. 1(1): 1-9. DOI: doi.org/10.61440/JJMM.2025.v1.08

There is no doubt that the subject of forensic evidence in Jordan-particularly within the Directorate of Laboratories and Forensic Evidence-is continuously evolving. Evidence is no longer physical in the traditional sense but has become electronic or digital, appearing on computer devices and capable of being erased within fractions of a second without being noticed. This makes it critical to determine how and by whom such evidence was accessed. As a result, Jordanian courts handle digital evidence with extreme caution to ensure that judges can rule justly, after confirming its validity and imposing appropriate penalties on offenders. After all, there is no crime and no punishment without legal provision, and such provisions can only be applied with the presence of conclusive evidence proving the offender's guilt. Otherwise, the crime remains circumstantial.

Research Problem and Questions

One of the foundations of justice in courts is the imposition of a penalty on the accused only after guilt has been proven through conclusive evidence that convinces the judge, following the preparation of all supporting documents and evidence by the Public Prosecution, represented by the prosecutor and public security officers. Therefore, the issue of evidence is of utmost importance. However, with the rapid increase in crimes committed using computer technology and the Internet, several challenges have emerged regarding the difficulties in proving such newly developed crimes, which are characterized by the unique nature of digital evidence. These challenges include the absence of physical traces at the crime scene, difficulties in extracting digital evidence, issues related to searching and seizing electronic evidence, and how it is handled by investigative authorities.

Given the unique nature of the cybercrime scene and the complex steps a criminal investigator or forensic expert must take to conduct electronic examinations and obtain digital evidence—which is stored within electronic devices and therefore susceptible to manipulation—the task of gathering and extracting such evidence becomes extremely challenging. The difficulty also lies in the process of investigating cybercrimes and in the fast pace at which such crimes are committed, which makes them easier to perpetrate and erase before detection. A criminal can commit a crime through a computer without leaving any tangible trace.

Hence, the research problem can be summarized by addressing the following questions:

- **A.** What is the impact of technical expertise in securing and extracting digital evidence from the crime scene in uncovering crimes, from the perspective of the study sample?
- **B.** What is the role of administrative and logistical expertise in facilitating the work of the technical investigation team, from the perspective of the study sample?
- **C.** To what extent are technical security procedures effective in detecting cybercrimes, from the perspective of the study sample?

Significance of the Study

The theoretical and practical significance of this study lies in the following:

1. Shedding light on the process of securing digital evidence by public security personnel and its impact on crime detection in Jordan, particularly in relation to the rising prevalence of cybercrimes—especially during the COVID-19 pandemic.
2. Enriching the Arabic and Jordanian academic literature on this relatively rare topic.
3. This study is among the few that explore the cybercrime scene and the methods used by specialized investigators in Jordan to secure digital evidence, particularly within the field of criminology.
4. Opening the door for future researchers to conduct similar studies in other Arab countries.

Study Objectives

This study aims to:

1. Identify modern technical methods and the skills of technical investigators in collecting and extracting digital forensic evidence, and assess the impact of technical expertise on crime detection.
2. Determine the role of administrative and logistical expertise in facilitating the tasks of the technical investigation team.
3. Assess the effectiveness of technical security procedures in detecting cybercrimes in Jordan.

Operational Definitions and Key Concepts

- **Securing (Evidence):** According to Lisan al-Arab, securing means preserving, protecting, and safeguarding something from being taken.

Legally, it refers to the procedures carried out by the competent authority to preserve forensic evidence from the crime scene in an appropriate environment to present it before the judiciary [1].

- **Evidence:** Defined as the tool used by the judge to form judicial conviction and reach the truth based on sound evaluation [2].
- **Digital Evidence:** Refers to evidence extracted through scientific analysis of data found on computer systems, used as proof in court [3].
- **Operationally:** All evidence extracted from computers by qualified public security personnel, whether before or after the crime, in Jordan.
- **Crime:** Some define it as behavior or negative actions that violate laws, ethics, and societal values [4].

Al-Wraikat defines it as a deliberate act that violates criminal law, committed without justification, and punishable by the state [5].

Key Concepts Related to Securing Digital Evidence

- **Crime Scene:** Refers to the location where the crime was committed and includes both physical traces and intangible evidence. Every crime has a location, though not necessarily a defined "scene," especially for behavioral crimes [6].

- **Cybercrime Scene and Its Importance:**

Al-Sarhani defines it as a virtual space within a computer environment, consisting of digital data stored and transmitted through systems and hard drives. Unlike physical crime scenes, the cybercrime scene involves digital elements, which require handling by specialized technical experts in digital evidence [7].

According to Al-Ma'aytah, the crime scene consists of two main elements:

1. The place or area where the crime occurred and other related locations.
2. The traces left by the crime.

The crime scene is the cornerstone of investigations due to its critical role for investigators and prosecutors in preliminary inquiries. Its importance includes:

- o Allowing investigators or experts to identify facts about the crime and how it was committed.
- o Helping determine the number and identity of perpetrators.
- o Providing material traces that assist in unraveling the crime.
- o Offering insights into motives and methods behind the crime [8].

Cybercrime

Cybercrime has multiple definitions. The Jordanian Cybercrime Law No. 27 of 2015 defines it as unauthorized access to information networks or systems.

Legal scholar Don Parker provides a broader definition, describing it as any criminal act, regardless of its relation to information technology, that causes harm to the victim or profit to the perpetrator [9].

Tott & Ahradcatst define it as crimes in which some part of the criminal activity occurs through a computer.

Technical Expertise

Linguistically, expertise means knowledge, and a "khabeer" (expert) is one who understands something in depth.

Legally, Jordanian law does not explicitly define "expertise," but outlines procedural rules. Some define it as the opinion provided by a technical expert on a matter requiring scientific knowledge [10].

A technical expert is a specialized person with sufficient knowledge to extract any evidence that may help clarify a crime [11].

Theoretical Framework and Previous Studies

Theoretical Framework:

The Role of Technical Expertise in Securing Digital Evidence at the Crime Scene Undoubtedly, the extraction of digital evidence from crime scenes is a highly sensitive and complex task, particularly given the rapid development of technology and the evolution of cybercriminal methods. This necessitates the involvement of technical and forensic experts who assist judges or investigators in forming judgments on matters requiring scientific understanding. Digital evidence serves as a tool for uncovering truth with the help of qualified personnel [12].

Therefore, the role of the technical expert at the cybercrime scene is fundamental and indispensable. The importance of technical expertise increases with the growing need to extract and secure digital evidence in cybercrime cases.

Elements of Cybercrime

Legal scholars differ in their definitions of cybercrime and in determining its essential elements. Some argue that cybercrime consists of only two main elements: the material element (actus reus) and the moral element (mens rea). This school of thought excludes the legal element, asserting that the illegality of an act is determined based on the legal classification of the crime, which is a relational concept rather than a constitutive part of the offense itself [13].

Others maintain that cybercrime comprises three essential elements: the legal, material, and moral elements. According to this view, the legal element is indispensable, reflecting the unlawful nature of the act in relation to the provisions of criminal law.

a. The Legal Element:

This principle applies to defining crimes and determining the punishments and security measures imposed on individuals. A judge cannot criminalize an act unless it is defined as a crime by law, nor impose penalties that are not legally stipulated. Internationally, some organizations play a key role in promoting international cooperation to combat cybercrime. For example:

- The 1985 UN Congress on the Prevention of Crime in Milan commissioned a group of 20 experts to study the protection of information systems and offenses against computers, issuing recommendations to counter cybercrime.
- The 2001 Budapest Convention by the Council of Europe.
- Regionally, the Arab Council of Ministers of Justice adopted the Arab Model Penal Code under Resolution No. 229 of 1996. Chapter 9 of this code addresses cybercrime under the title "Offenses Against Individuals' Rights Arising from Data Processing." Article 461 outlines various forms of cybercrime and the penalties for incitement [14].

b. The Material Element of Cybercrime:

This refers to the unlawful misuse of electronic systems, or the tangible destruction, theft, or manipulation of computer-based information, such as credit card theft or data forgery. In traditional crimes, the material element typically involves observable behavior (e.g., physical acts of killing or stealing). However, in cybercrimes, it is often difficult to detect or apprehend the perpetrator physically, as these crimes are committed through digital data and virtual networks.

c. The Moral Element:

This relates to the mental and emotional state of the cybercriminal, as well as the relationship between the objective circumstances of the crime and the personality of the perpetrator.

Technical Expertise and Its Importance at the Cybercrime Scene

The significance of technical expertise becomes evident when securing and extracting digital evidence is necessary. As previously mentioned, rapid advancements in communication and technology have made technical expertise essential in investigating cybercrimes, given the complexity of their methods.

Administrative Skills and Attributes Required of the Technical Expert

The Code of Criminal Procedure emphasizes the importance of certain skills and attributes for those conducting investigations, due to the potential infringement on individuals' rights and freedoms. These individuals must be chosen with precision and possess substantial knowledge, as their role is critical in achieving justice and security. Key qualities include:

1. A consistent commitment to uncovering the truth, as truth is the foundation of justice [15].
2. The ability to act swiftly during investigations, preserving evidence before it is altered or lost. Delay may result in the loss of crucial evidence or the violation of rights [14].
3. A genuine passion for the work, which drives excellence and dedication.
4. Strong observation skills and quick comprehension.
5. Extensive general knowledge, familiarity with criminal laws and criminology, understanding the motives and causes of crime, and awareness of the societal context [16].
6. Self-confidence, especially when handling digital evidence, which requires precision and certainty.
7. Energy, agility, and responsiveness, such as quickly arriving at the cybercrime scene and securing digital evidence.
8. Neutrality and impartiality, which are among the most critical traits of a forensic expert.
9. Meticulousness, as working in virtual environments demands high precision; even small mistakes may compromise evidence.
10. Knowledge of criminal tactics, allowing the expert to deduce how the crime was committed based on the digital clues.

Collection of Digital Evidence at the Crime Scene

It is crucial to handle the cybercrime scene according to specific administrative and technical protocols to preserve the integrity and probative value of digital evidence. Investigators must adopt procedures tailored to the unique nature of cybercrimes. According to the Association of Chief Police Officers (ACPO) in the UK (2003), four guiding principles should be followed when collecting electronic evidence:

1. No changes should be made to data on the device.
2. If exceptional circumstances necessitate changes, the expert must provide a valid justification.
3. All steps taken in evidence collection and analysis must be fully documented, and preferably verified by a third party.
4. The investigator assumes full responsibility for adhering to these principles.

Effectiveness of Technical Security Measures in Uncovering Cybercrime

Modern Technical Methods for Collecting Digital Forensic Evidence

Obtaining digital forensic evidence is a challenging task requiring significant expertise in digital technologies. The diversity and evolving nature of cybercrimes necessitate the use of advanced tools and techniques, which are broadly categorized into two types:

1. Modern Physical Tools for Digital Forensic Collection

These are technical tools used in digital environments to perform investigative tasks and establish the occurrence of a crime and the identity of the perpetrator. These tools are used to gather evidence left behind by users online, such as IP addresses, cookies, and browser information.

Key methods include:

a. Use of IP/TCP Protocols

These protocols are foundational to internet communication. The IP protocol assigns addresses to data packets, while the TCP protocol breaks down information into packets and ensures their delivery [17].

b. Use of Cookies

When a user visits a website, a cookie is created on their device to store information such as login data, browsing history, and modification dates. This data can be crucial in investigations [18].

c. Use of Proxy Servers

Proxies act as firewalls and gateways, storing logs that may include user identities, access times, and usage restrictions. These logs are valuable in tracing criminal activity and proving user behavior [17].

d. Use of Tracking and Intrusion Detection Software

These programs detect hacking attempts, gather relevant data about the intruder, and notify the affected parties. One such tool is Hack Tracer v1.2.

Second: Modern Procedural Means for Extracting Digital Evidence

Methods of proof have not escaped the effects of technological development. The required harmony between the nature of the evidence and the nature of the crime from which it arises—and which it is suitable to prove—has resulted in procedural methods compatible with the technical nature of the crime and digital evidence. This enables investigation authorities to collect and extract digital evidence through advanced modern information technology. Among the modern procedural methods for extracting digital evidence are the following:

Infiltration: Infiltration refers to the process by which the judicial police officer penetrates criminal groups and deceives them into believing he is a partner, in order to catch them.

1. **Interception of Communications:** The process of intercepting communications is one of the newly developed procedures in collecting digital forensic evidence. It refers to intercepting, recording, or copying communications that take place via wired or wireless communication channels and means. These communications are data that can be produced, distributed, stored, received, and displayed [19].
2. **Electronic Surveillance:** This refers to a fundamental security operation involving electronic information systems, whereby the monitor (with a closed letter Qaf) surveils the monitored (with an open letter Qaf) using electronic devices and through the internet to determine a specific purpose, with the results saved in an electronic file and reports prepared accordingly [20].

Techniques and Software Used in Collecting Digital Evidence

When extracting digital evidence from the cybercrime scene, the expert and technical investigator must use tools that assist them in performing their duties, while taking into consideration the fundamentals and procedures that must be followed at the cybercrime scene. Among the techniques and software that assist in collecting digital evidence are the following:

Warrant Program (Warrant Program Computer Scorch):

A software containing a database that allows input of all important information required to number the evidence and record its details. It also issues receipts upon receiving evidence and searches through evidence lists to locate a particular piece or determine the conditions under which it was seized.

1. **Bootable Diskette:**

A disk that helps the investigator access the system if it is protected or encrypted. The disk should be equipped with a disk space doubling program, as the criminal may have used such a program to expand the hard disk space.

2. **File Processing Program (X Tree Pro Gold):**

A program that assists the expert and investigator in finding files over the internet or on the hard drive. It is used to evaluate the contents of the suspect's hard drive and also helps read computer programs in their original form [21].

3. **Imaging Techniques:**

This technique involves making a copy of the contents of the electronic device without modifying or damaging the data contained therein. Examples include:

- o **Encase Forensic:** One of the most famous and costly programs, a sophisticated device used for examining and analyzing digital evidence, placed at forensic stations. It is used by police, investigations, and intelligence to search and explore the suspect's computer and document any evidence against them [1].
- o **Lap Link Software:** Can be run from a floppy disk in a way that allows copying data from the suspect's computer and transferring it to another disk.

4. **Disk Viewing Programs (View Disk Amapisk):**

Used to obtain the contents of the hard drive regardless of disk formatting methods. This program has two versions: one for individuals and another for the police [19].

Theories Explaining the Study Topic

Opportunity Theory

The Opportunity Theory was formulated by Cloward and Ohlin in 1960 in their book Delinquency and Opportunity. The theory discusses the social construction of illegitimate opportunities. People from the working-class culture in American society generally want to achieve their goals successfully through legitimate means available in society. However, they face severe obstacles because society denies them chances to succeed. These obstacles include cultural and linguistic differences, access to vital means of upward mobility, inability to afford advanced education, and urban crowding, which makes class differences clearer (such as car ownership, housing, etc.). When legitimate means to achieve goals are blocked, severe frustration occurs, leading individuals to resort to illegitimate means. Juvenile gang crimes are examples of such illegal paths to achieve goals [5].

Regarding this theory and our study topic, modern technologies and the internet have created unprecedented opportunities for the spread of cybercrime. Opportunity leads to crime (Felson & Clark, 1998), and the environment and its arrangements play a significant role in creating crime, breaking social rules—for example, times of deviance (day or night), lack of supervision, all increase the chance of committing cybercrime. Information becomes an easy and profitable target with low risk and a small chance of the criminal being caught [20].

Information and communication technologies have created new opportunities for criminals through their increased internet use, facilitating the growth of cybercrime. Internet crimes represent a new and distinctive form of crime and pose challenges to predict developments and prevent such crimes [22].

Criminal Evidence Theory

This theory is one of the fundamental theories relied upon in this study. It revolves around the rules of criminal procedures from the moment the crime occurs until the issuance of the judicial verdict. The judicial ruling against criminals is based on the authority granted to the judiciary to assess forensic evidence, which may differ depending on the type of proof the court adopts. The theory is based on the principle of proving the occurrence of the crime and attributing it to the accused. The goal is to uncover the truth to achieve justice. Without evidence, the judge cannot impose a penalty on the deserving, and the trial procedures become invalid [23].

One of the main principles of the criminal evidence theory is the principle of judicial conviction (free evaluation of evidence), which grants the judge the right to act regarding the means of evidence, inference, and investigation, which are not strictly defined by criminal law. The principles of this theory agree with the logical approach to thinking in public life and with scientific research methods. The judge decides the case based on personal conviction about the evidence presented and can accept or reject it according to confidence in it. The judiciary's discretionary power in determining the importance of evidence is fully granted.

Regarding this theory and our study topic, the role of experts and technical investigators in uncovering cybercrime is limited to providing logical, objective, and conclusive evidence to form the judge's judicial conviction to fairly convict and sentence the accused.

The Jordanian legislator has enshrined the principle of judicial conviction in Article (147/2) of the Jordanian Code of Criminal Procedure, stipulating that evidence in felonies, misdemeanors, and violations can be established by all methods of proof, and the judge rules according to his personal conviction. The Court of Cassation ruled in 2004 that the trial judge in criminal matters has the discretion to take the evidence he trusts and may accept part of the evidence and exclude the rest [23].

Previous and Related Studies

Among the previous studies addressing digital evidence extraction and its impact on crime detection:

- Study titled The Effect of Modern Criminal Evidence on the Personal Conviction of the Criminal Judge in Algerian Legislation. The study concluded that technological advances were not accompanied by legal adaptations. Due to the mutual impact between using these technologies and the infringement on individual rights and freedoms—a matter not addressed by previous studies or laws—this formed a challenge for the state. The study recommended updating Algerian legal texts to bridge the gap between investigators and civilians.
- Study titled The Role and Impact of Digital Evidence in Cybercrime Investigations. The study found that agencies face difficulties in proving digital evidence against accused persons amid the growth of internet crimes, noting a shortage of training and personnel, which complicates investigations.

- Conducted a study titled Criminal Investigation Procedures in Information Technology Crimes according to UAE Legislation. The study concluded that IT crimes require judicial police officers to have sufficient IT culture to directly conduct evidence collection procedures.
- Study titled Modern Scientific Evidence and its Role in Criminal Proof concluded that modern evidence plays a significant role in achieving justice, whether to prove the accused's innocence or the victim's case. It recommended specialized technical training for judges and investigators in dealing with modern scientific evidence [24].
- Abdul Wahab study titled The Evidentiary Value of Electronic Evidence in Criminal Proof found clear shortcomings in many substantive and procedural criminal legislations facing crimes committed by or through electronic means, leading to many criminals escaping punishment.
- Al-Arroud study aimed to identify the impact level of security investigations on crime detection, the necessary skills and attributes for investigators, and the effectiveness of investigative methods in crime detection. The study included 269 police officers in Jordan and found high levels of impact, skills, and effectiveness but also noted significant obstacles [23].
- Shamut, Adwan, and Jabour study titled Evidence in Cybe0072crimes: A Comparative Study found that proving evidence in computer and internet crimes faces great difficulties, especially because electronic data storage makes evidence invisible and incomprehensible to the naked eye, and noted weak legal regulations regarding proof in cybercrimes.
- Al-Qahtani study titled Developing Criminal Investigation Skills to Face Information Crimes surveyed 156 investigators in Riyadh's Public Prosecution and found high agreement on the availability of investigation skills, obstacles to skill development, and ways to improve skills. The study recommended building training infrastructure, benefiting from advanced countries' experiences, and updating academic curricula [24].
- Al-Arroud study titled Use of Technical Means by Investigators and its Relation to Crime Detection in Jordan surveyed 157 participants and found moderate usage of technical means. The most detected crimes using technical means were theft, drug trafficking, murder, and robbery, respectively [23].

Commentary on Previous Studies

From the review of previous studies, it is noticeable that they varied in their objectives but all focused on modern techniques of evidence and the role of digital forensic evidence in crime detection, as well as methods of investigation and inquiry using modern technology. For example, the study by Al-Mazrouei and Suleiman aimed to identify criminal investigation procedures in information technology crimes according to Emirati legislation. The study by Hussein focused on modern scientific evidence and its role in criminal proof. Al-Arroud's study examined security investigations and their impact on crime detection from the perspective of personnel in the criminal investigation department [23]. Al-Balawi focused on modern techniques in criminal investigation and their role in crime control. Krishnan S. studied the role and impact of digital evidence in cybercrime investigations, among others. It is noted that the current study aligns and harmonizes with the objectives of these studies but differs primarily in its focus on the seizure of digital evidence by public security officers and its effect on crime detection in general. It also aims to explore methods of extracting evidence and the obstacles encountered by those working in this field. Some previous studies' results highlighted the importance of digital evidence and the necessity of adopting new methods to trace its source and developing security agencies to keep pace with emerging crimes. Additionally, some studies emphasized the importance of the expertise and role of the technical investigator in extracting evidence and handling the crime scene.

Methodology and Procedures

This section of the study describes the study methodology and procedures, identifies the study population and sample, and details the steps taken to achieve the study objectives, including the measurement tool and validity and reliability indicators.

Study Methodology:

The study employed a social survey method, appropriate for the subject of this research.

Study Population:

The population consists of personnel working in the Forensic Laboratories and Evidence Department, across various ranks and positions, totaling (940) officers and non-commissioned officers distributed across different divisions and sections.

Study Sample:

To select the sample members, the study used proportional stratified random sampling at 30% of the target statistical population. The number of personnel in the Forensic Laboratories and Evidence Department was enumerated, and the number of questionnaires to be distributed in workplaces was determined according to personnel counts. A total of (300) questionnaires were distributed, representing 30% of the study population. After implementation, (280) questionnaires were retrieved. Upon reviewing the returned questionnaires, (3) incomplete questionnaires were excluded. Thus, the final sample size consisted of (277) officers and non-commissioned officers, representing 92.33% of the distributed questionnaires and 29.4% of the total study population.

Study Instrument:

The researcher developed a questionnaire specifically for collecting field data after conducting a literature review and examining relevant previous studies. The questionnaire comprised the following main parts:

- **Part One:** Includes qualitative and functional data of the study sample individuals, including variables such as gender, educational level, age, military rank, nature of work, number of training courses attended, and years of experience.
- **Part Two:** Contains (31) items distributed across 3 domains:

1. **Domain One:** Includes (9 items) aiming to identify the role of technical expertise in seizing and extracting digital evidence from the cybercrime scene and its impact on crime detection.
2. **Domain Two:** Includes (9 items) aiming to identify the role of administrative and logistical expertise in facilitating the work of the technical investigation team.

3. **Domain Three:** Includes (13 items) aiming to assess the effectiveness of the following procedures in the field of cybercrime detection and seizure of digital evidence.

The third part was rated using a five-point Likert scale as follows: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree. The arithmetic mean was used to provide a clearer and more precise indication of the importance of the questionnaire items and study domains, according to the following scale:

High	Medium	Low
(3.50 and above)	(2.50 – 3.49)	(2.49 and below)

Validity of the Study Instrument:
The face validity of the study instrument was verified by presenting the initial draft of the questionnaire to seven faculty members from the College of Social Sciences, the College of Educational Sciences, and the College of Law at Mutah University and Al-Balqa Applied University. Their opinions were sought regarding the following:

1. Ensuring the content of the study instrument covers the elements of the study topic.
2. The sufficiency of the items within the domains, and whether any items need modification, deletion, or addition.
3. The extent to which the domains of the study instrument can answer the study questions.

Reliability of the Study Instrument:
Reliability coefficients were extracted using Cronbach's Alpha as an indicator of internal consistency. The overall reliability coefficient was (0.908), while the reliability coefficients for the questionnaire domains are shown in Table (1):

No.	Domain	Number of Items	Reliability Coefficient (Cronbach's Alpha)
1	Role of technical expertise in seizing digital evidence	9	0.841
2	Role of administrative and logistical expertise in facilitating the technical investigation team's work	9	0.828
3	Effectiveness of security procedures in seizing and extracting digital evidence in crime detection	13	0.851
4	Overall	31	0.908

Means, Standard Deviations, and Ranking of Study Sample Estimates Regarding the Impact of Technical Expertise in Seizing and Extracting Digital Evidence from the Crime Scene on Crime Detection (Ranked Descending) Table (2)

Level	Standard Deviation	Mean	Item Description	Item No.
High	0.602	4.74	Technical expertise contributes to preserving digital evidence in a special way different from physical evidence	1
High	0.608	4.70	Technical expertise contributes to identifying and scientifically analyzing types of digital evidence to detect crime	2
High	0.718	4.55	Technical expertise contributes to judicial conviction by the judge in digital evidence after it is admitted as proof in court	3
High	0.698	4.44	Technical expertise contributes to converting invisible evidence into visible and readable evidence to help solve the crime	4
High	0.725	4.41	Technical expertise contributes to isolating the information system without damaging or destroying digital evidence	8
High	0.638	4.40	Technical expertise contributes to determining the correlation between physical evidence and digital evidence	5
High	0.729	4.37	Technical expertise contributes to using modern and advanced methods to detect digital evidence at the crime scene	9
High	0.666	4.36	Technical expertise contributes to knowing locations of cybercrime, locally or internationally	7
High	0.668	4.34	Technical expertise contributes to understanding methods of committing cybercrime	6
—	0.408	4.48	**Overall Mean**	—

Means, Standard Deviations, and Ranking of Study Sample Estimates Regarding the Effectiveness of Technical Security Procedures in Detecting Cybercrime from the Perspective of the Study Sample (Ranked Descending)Table (3)

Level	Standard Deviation	Mean	Item Description	Item No.
High	0.574	4.62	Use of tracking and hacking programs	1
High	0.582	4.61	Validity of access to personal data for proving cybercrime	2
High	0.641	4.57	Use of Cookies information	4

Level	Standard Deviation	Mean	Item Description	Item No.
High	0.685	4.57	Use of Proxy information	3
High	0.661	4.54	Use of IP/TCP protocol	4
High	0.857	4.53	Digital signature technology, which helps prevent forgery of emails	6
High	0.709	4.53	Tracking communications and correspondence	7
High	0.938	4.50	Encryption	8
High	0.694	4.49	Use of intrusion detection systems and solutions for security gaps	**9**
High	0.689	4.49	Use of computer databases rules	11
High	0.725	4.47	Setting a network security policy and mobilizing all human and material resources to implement it	12
High	0.754	4.47	Keeping backup copies of all sensitive information on external disks not connected to the network	10
High	1.085	4.41	Use of firewall	13
—	0.427	4.52	**Overall Mean**	—

Recommendations:

In light of the results, the following recommendations are proposed:

1. Strive to exert more efforts to enhance the level of technical expertise among public security personnel and specialists by granting them the necessary legal and administrative authorities that would accelerate achieving more accurate results, saving time and effort in reaching the truth.
2. Organize training courses and workshops, and encourage employees in the laboratories and forensic departments to participate by increasing the financial incentives allocated for participants in these courses.
3. Increase the number of employees in laboratories and forensic departments, especially in the digital evidence sections, due to the increase and diversity of these crimes.
4. Benefit from the practical expertise of technical experts and those with long experience in their workplaces or after retirement, and avoid transferring them to other locations.
5. Develop the management of laboratories and forensic departments.
6. Equip the digital evidence department, in particular, with the latest devices and equipment, and increase the expertise of its staff.
7. Raise awareness among Jordanian society about the dangers of cybercrime, considering its impact on individuals, society, and national security.
8. Conduct a similar study to this one on other relevant departments within the public security involved in investigations and collection of digital evidence.

References

1. Al-Khashashneh, Tawfiq Abdullah. Crime Scene and Its Inspection via the International Information Network, First Edition, Dar Al-Thaqafa, Amman. 2020.
2. Al-Sarour, Ahmed Fathi. Al-Waseet in Criminal Procedures Law, Tenth Edition, Dar Al-Nahda Al-Arabiya, Cairo. 2016.
3. Eskhita, Radwan Hassan. Scientific Review of the Digital Forensic Investigation Book Forensik IT, Published Research, Scientific Generation Journal. 2018.
4. Al-Hassan, Ihsan Muhammad. Sociology of Crime, First Edition, Dar Wael, Amman. 2008.
5. Al-Warikats, Ayed Awad. Theories of Criminology, First Edition, Dar Wael, Jordan. 2013.
6. Atiyah, Tarek Ibrahim. Crime Scene in Light of Procedural Rules and Technical Methods, Dar Al-Jami'a Al-Jadida, Alexandria. 2012.
7. Al-Sarhani, Muhammad bin Nasir. Skills of Forensic Investigation in Computer and Internet Crimes: A Survey Study on a Sample of Police Officers in the Eastern Region, Unpublished Master's Thesis, Naif Arab University for Security Sciences, Riyadh. 2004.
8. Adas, Imad Awad. Investigations as a Procedure in the Search for Truth, Dar Al-Nahda Al-Arabiya, Cairo. 2007.
9. Youssef, Amir Faraj. Information Crimes on the Internet, University Publications House, Alexandria. 2008.
10. Al-Dhunaibat, Ghazi Mubarak. Role of Technical Expertise in Proving Forgery in Handwritten Documents in Jordanian Law: A Comparative Study, Published PhD Dissertation, Amman Arab University, Amman. 2003.
11. Hasan, Amal Abdulrahman. Modern Scientific Evidence and Its Role in Criminal Proof, Published Master's Thesis, Faculty of Law - Middle East University, Amman. 2012.
12. Al-Khashashneh, Tawfiq Abdullah. Seizure of Digital Evidence and Its Effect on Crime Detection, Published Research, Public Security Journal. 2019.
13. Bousqia, Ahsan. Brief in General Criminal Law, Dar Houma, Algeria. 2006.
14. Halabi, Khaled Ayad. Procedures of Investigation and Inquiry in Computer and Internet Crimes, Dar Al-Thaqafa, Jordan. 2011.
15. Ibrahim, Khaled Mamdouh. Forensic Investigation in Cyber Crimes: A Comparative Study, First Edition, Dar Al-Fikr Al-Arabi, Alexandria. 2018.
16. Al-Arud, Alaa Ali. Use of Technical Means by Investigators and Their Relation to Crime Detection, Published Master's Thesis, Mutah University, Jordan. 2013.
17. Debra, Shinder. "Scene of cybercrime", Computer Forensics Handbook. Book, publishing by syngress Inc. 2002.
18. Bunting Steve, Wei William. Encase computer forensic, wily publishing Inc. United States of America. 2006.
19. Abdelmuttalib, Tahiri. Criminal Proof with Digital Evidence, Master's Thesis, University of M'sila, Algeria. 2015.
20. Al-Badaineh, Thiab Mousa. Cybercrime: Concept and Causes, Scientific Paper at the Forum. 2014.

21. Capeh, Tracy. x tree mac makes the mac desktop more

    powerful, InfoWorld. 1989. 8.
22. UNODC. United Nations office on Drugs and crime, comprehensive study on cybercrime, United Nations. 1989.
23. Al-Arud, Alaa Ali. Security Investigation and Its Impact on Crime Detection from the Perspective of the Criminal Investigation Department Workers, PhD dissertation, Mutah University, Jordan. 2016.
24. Al-Qahtani, Abdullah bin Hussein. Developing Criminal Investigation Skills in Facing Information Crimes: An Applied Study on Investigators at the Bureau of Investigation and Public Prosecution in Riyadh, Master's Thesis, Naif Arab University for Security Sciences, Riyadh. 2014.
25. Ibn Manzur, Muhammad bin Makram. Lisan al-Arab, edited by Amer Haidar, Dar Al-Kutub Al-Ilmiyyah, Beirut, Lebanon. 2004.
26. Al-Jabara, Abdulfattah Abdullatif. Technical Inspection Procedures of Crime Scene, First Edition, Dar Al-Hamed for Publishing and Distribution, Amman. 2011.
27. Cybercrime Law. 2015.
28. Al-Arabi, Mustafa Ibrahim. Role of Digital Evidence in Criminal Proof, Published Research, Legal Research Journal, Misrata University, Faculty of Law. 2016. 4.
29. Al-Buqmi, Nasser bin Muhammad. Importance of Digital Evidence in Criminal Proof: A Study According to Saudi Regulations, Published Research, Police Thought Journal. 2012. 21.
30. Al-Jabali, Mansour bin Abdulaziz. Principles of Criminal Investigation, First Edition, King Fahd National Library. 2008.
31. Hijazi, Abdulfattah Bayoumi. Principles of Criminal Procedures in Computer and Internet Crimes, Dar Al-Fikr Al-Jami'i, Alexandria. 2006.
32. Al-Kasasbeh, Fahd Youssef, Al-Tarawneh, Mustafa. Legal Controls on Search without Permission in Jordanian and Egyptian Laws: A Comparative Study, Published Research, Journal of Sharia and Law Studies, University of Jordan. 2015. 42.
33. Al-Qahtani, Suleiman Ali. Digital Forensic Sciences (Concepts and Processing Methods in Light of Modern Technical Development), Research Center, King Fahd Security College, King Saud University. 2011.
34. Abdelmuttalib, Mamdouh Abdulhamid, Jassim, Zubaida Muhammad, Abdulaziz, et al. Proposed Model for Digital Evidence Admission Rules in Computer Crimes, Conference on Electronic Banking Business Between Sharia and Law. 2003. 5.
35. Al-Anzi, Suleiman Muhja. Investigation Methods in Information Systems Crimes, Master's Thesis, Naif Arab University for Security Sciences, Graduate Studies, Riyadh. 2003.
36. Blasma, Raed Mahmoud. Collection of Digital Evidence from the Cybercrime Scene, Unpublished Research, Department of Laboratories and Forensic Evidence Management. 2015.
37. Khalaf, Jassim Khuraibet. Difficulties of Criminal Evidence in Information Crimes, Law Journal for Legal Studies and Research, University of Thi-Qar, College of Law, Iraq. 2016.
38. Al-Bishri, Muhammad Al-Amin Al-Bishri. Investigation in Emerging Crimes, Center for Security Studies and Research, Naif Arab University for Security Sciences, Riyadh. 2004.
39. Eoghan Casey. Digital evidence and computer crime, third Edition, published by Elsevier, Inc. London. 2011.
40. Association of chief police. (UK), good practice guide for computer based electronic evidence, ACPO. 2003.