State of Palestine

State of Palestine
دَوْلة فِلسْطِيْن

Palestinian Civil Police
Criminal investigation department
Cyber-crime Unit

Research Title :
"Collecting Digital Evidence"

Collecting Digital Evidence

- **The Abstract:**

This paper deals with digital evidences as a modern method of criminal proof and how it differs from the conventional evidence, whether it is in the acceptance of the criminal judge or it is in his discretion; and this evidence is an information accepted by logic and by human-mind and it is adopted by science, where it is obtained and analysed by legal procedures, using special scientific programs and applications through the translation of computational data that stored in computers, its accessories and in the networks; which can be used at any stage of the investigation and trial to prove an act, a thing or a person connected to the crime, to the offender or to the victim.

The research also discussed the legal value of the digital evidence and the extent of its validity in criminal evidence.

- **The introduction:**

1. introduction to the research topic:

Since the middle of last century the world has seen a new revolution which was termed the revolution of information, as a reference to the prominent role that has become played by information currently because it has become a considerable power in the hands of both countries and individuals. The tremendous development of the ICT sectors and the amazing integration that took place between them later has been the centerpiece of this revolution.

The information revolution highlighted a new system called the information system, which in his turn created the information society that relies on all kinds of communication technology, especially the processing of information; so the recipient deals with a huge amount of data and information, which exceeded the limits of space and reduced the element of time.

The world is now talking about a global network, that not only transmits the sent material and receive it, but it transmits the human being with all of his senses; so without moving he is from one end of the earth to the other to connect and interact with its counterpart from that extreme end.

It became the "cry of the age" and the language of the new world, and as a natural result of the logic development it will be the language of communication in our coming days; it is a new society by all standards imposed itself on all aspects of our social, economic and cultural life with it began the emergence of a new age which is the information age.

This information explosion, which we see today, is only the fruit of the combination between ICT technologies. This information and data are managed by governmental or personal sites that deal with all aspects of life, and it manages business and achieves communication. This is the positive side of the information revolution and communication technology. It is natural that this useful side in the information revolution is accompanied by another negative side, which is the exploitation of information in the commission crimes that was unknown previously which are the computer-related crimes or the cybercrime that has become a threat to individuals and States in all areas.

With the appearance of such crimes and its considerably increased danger and ineffectiveness of existing laws in facing these crimes that is different from the traditional crimes which have a specific nature and clear dimensions; so it was a necessary for States to search for how to face it legally. Some countries have begun to enact laws and treaties designed to combat these crimes, including Palestine where the cyber-crimes Law was passed in 2017 and amended at the beginning of 2018.

By issued a substantive nature laws but the practical application of these laws collides with legal procedural challenges due to the nature of the crime, the crime scene and the difficulty in applying certain criminal proceedings such as inspection, search, seizure, etc., which is a major impediment in keeping abreast to the use of digital evidence that are connected to computers and the World Wide Web.

The digital evidence is forensic evidence that has emerged with the appearance of cybercrime and has become an urgent necessity imposed by the need for evidence belonging to the same environment in which these crimes are committed or through.

Therefor there is a legal recognition of this evidence and an actual practice to get benefit from it, but there is some fear and hesitation in proving the cyber-crime, in get the digital evidence in addition to the existence of certain procedural and technical that are controlling the process of evidence deducing and submitting it to the judicial authorities, and these controls may delay the proof and to take advantage of the digital evidence.

And because of the importance of this topic, it will be discussed this research-paper in its three interlocutors.

2. The importance of this research:

The importance of this research comes from the fact that society has become an information society based on the power of knowledge and information, and the increasing reliance on the information technology system in various fields of life, which accompanied the cybercrime growing so a need to combat it and to punish its offender by acceptable procedures based on collecting digital evidence In a way that helps to prove the crime according to the law and commensurate with the change in traditional criminal evidence and the need to keep up with the technical progress that highlighted the need to collect digital evidence from a complex digital environment characterized by change and continuous evolution.

The digital evidence is a very important subject that is indispensable in criminal law in particular. The issue becomes more important because it is a serious and a modern one, which imposed itself on the law enforcement, especially the men of criminal jurisprudence and the judiciary.

3. The Searching Difficulty:

The past few years have witnessed a tremendous information revolution, which has included most of the human activities that overcome the barriers of time and place, through the rapid transfer of information that overcome the geographical restrictions and control restrictions that control the traditional means of information transmission; which is created a new environment that is developing rapidly and is changing constantly, accompanied by the emergence of crimes related to this environment, which is the cyber-crimes that have imposed a new challenge to the criminal justice system; with regard to the control procedures, characterization of the crime and the appropriate legal description of the facts that shape cyber-crime.

Those challenges are because of the specific nature of these crimes, which take place in a virtual environment and an open electronic space characterized by change, regeneration and geographical wild-spread. The change in the type of crime and the change in its environment necessitates the need for unconventional means to collect unconventional evidence that requires the response of procedural rules for continuous changes, Which accompanied the change in the method of committing crimes, the means of committing them, the environment which it committed in and legal ramifications. It also requires combined efforts of the investigator and the IT expert in order to collect the appropriate evidence, technically and legally, that evidence called digital evidence.

The digital evidence in terms of acceptance and determination in the criminal evidence is one of the modern topics; that is different from the traditional evidence and its role in the proof where the traditional evidence has been searched while the recent scientific evidences, including the digital evidence are new topics that have not been searched a lot in which there is a lot of difficulty because of its modernity and the scarcity of references.

The importance of combating cybercrime and the need to collect digital evidence in accordance with legal and process controls and technical assets is highlighting the research problem from the following question: What are the proper ways to collect digital evidence and its importance in criminal evidence?

4. Research Questions:

- What is the cyber-crime?

- What is the digital evidence?
- What is the difference between the digital evidence and the traditional evidence?
- What are the characteristics and the features of the Digital Evidence?
- What are the methods used to collect the digital evidence?
- What is the legal value of the digital evidence and its authority in criminal evidence?
- What is the judge's power to evaluate the digital evidence?

5. Research Methodology:

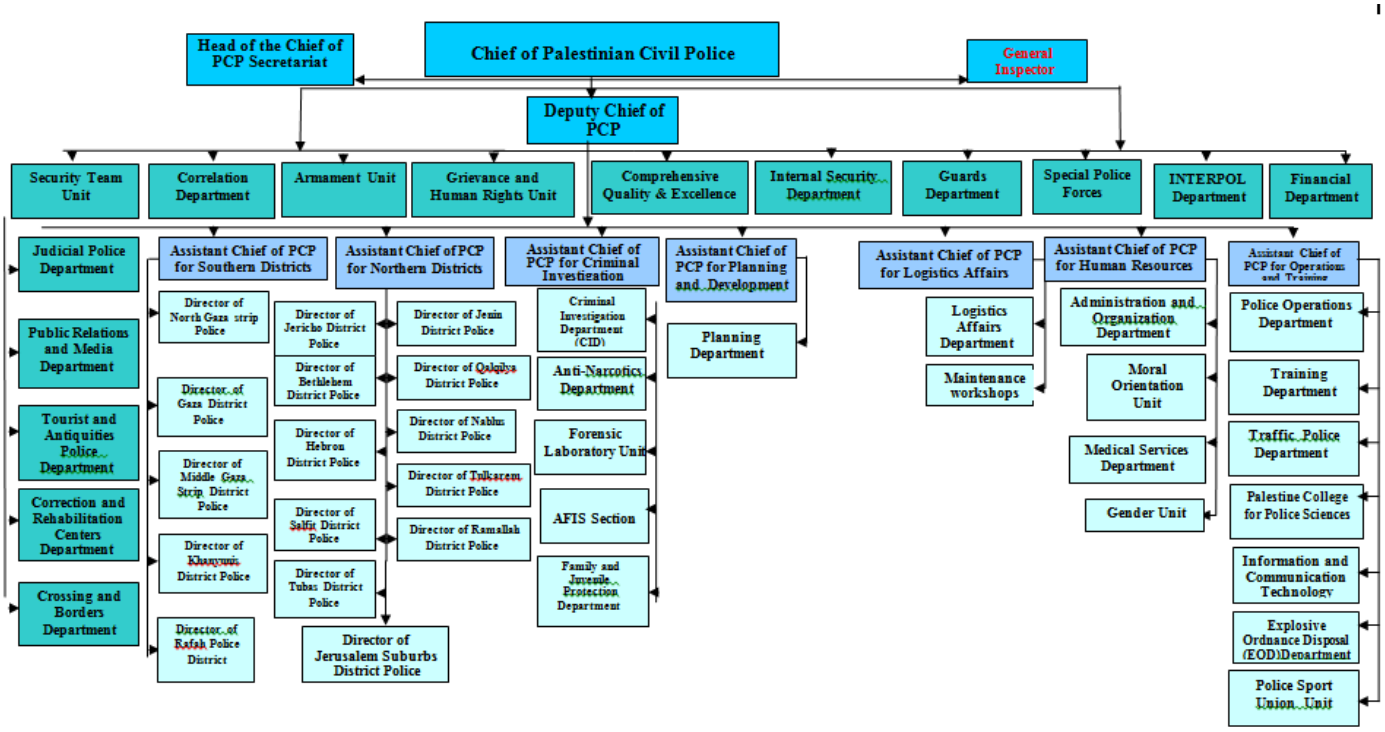
Due to the theoretical dependence on this research, the descriptive inductive approach will be used by relying on studies related to the digital evidence, the general penal procedural rules and the use of Palestinian law to reach the extent of the digital evidence authority and the importance of using it in the proofing.

6. research plan:

We will discuss the collection of digital evidence through three topics, respectively:

- What is the digital evidence?
- Methods of collecting digital evidence.
- The legal value of the digital evidence and its authority in the criminal evidence.

Structure of Palestinian Civil Police



The first topic
The Essence of Digital Evidence

The digital evidence is the natural and logical consequence of the emergence of cybercrime as an important proof means in criminal matters related to cybercrime, which came as a result of the scientific revolution in the IT system. Therefore, the digital evidence has a great importance in proving the cyber-crime and in identifying the perpetrators.

The digital evidence raises many questions in the field of criminal evidence, because of the difficulty of proving it and how to obtain it. Therefore in this research, we will discuss the definition of cyber-crime and the digital evidence, its characteristics and the difference between it and the traditional evidence.

The definition of the Digital Evidence

- **Firstly: The cyber-crime:**

Before going to study the essence of the digital evidence, we must study the essence of cybercrime. The definitions of cybercrime are varied according to the multiple angles we look at it from. So in one hand we have a technical definition and on the other hand, the legal definition as following:

Technical definition of cybercrime:

Some have defined cyber-crime technically as: "any criminal activity that uses computer technology directly or indirectly as a mean or as an object to carry out the intended criminal act."

From the point of view of this aspect, the definition of cyber-crime and the classification of its images require the definition of vocabularies related to the elements of cybercrime:

1. The computer: is a device that accepts or processes or stores or retrieves data or program.

2. A computer program: is an encrypted series of instructions or texts that are acceptable to the computer so that the data can be processed and get the results out of it.

3. Data: is a representation of information or texts in a manner acceptable to the computer, including documentation of programs prepared in an organized, stored, processed or transferred by computer.

4. Property: is an electronic payments, private information, copyrighted or registered copyright, electronically processed data, special identification codes, computer access numbers, systems that can be read by human or machine, and any other tangible or intangible computer related materials.

5. Entry: the use of communication or direct it.

6. Services: is processing data or storage functions.

7. Vital processes: Are the processes or the services required to operate, save, repair or connect computer transportation and distribution networks, to ensure the protection of public safety.

Legal definition of cybercrime:

Another aspect of jurisprudence defined cyber-crime as: "An illegal behavior, punishable by law, derived from criminal will and it takes place in related to computer data."

Criminal behaviour includes action and omission. This behaviour is unlawful, since legality denies the criminal act; it is punished by law, because criminalization is not achieved in criminal justice legislation but by the legislator's will and through the provision even if this behaviour was contrary to morality.

In fact, this aspect of jurisprudence holds that the place of computer crime - always - is the data in its Wide sense, which means the entered, produced, stored data and the programs of all kinds.

- **Secondly: The Digital Evidence:**

The emergence and the wild-spread of cybercrime - as a result of the electronic development in the information society - led to the ineffectiveness of procedural laws in general and the traditional criminal evidence in particular to combat this modern crime. Therefore, there was a need to find another way to prove this crime and bring their perpetrators to justice; this method was the digital evidence, because of the great importance of this evidence in proving the crime and attributed to the perpetrator.

The digital evidence is the crux of the research, does not depart from this approach because the questions that revolve around the criminal investigations in cyberspace are: How do the evidence and the electronic impact arise? How to find and recognize it? And how is it kept and presented to the court?

- **The evidence legal terminology**: The means used by the judge to reach the truth he seeks; the meaning of the truth in this context is about all the facts placed before the judge to implement law over them.

- **Also the digital evidence define:** The data that can be Prepared, transmitted or stored in digitized way so that it could help the computer to perform a task; or it is the evidence that has a place in the virtual world and leads to the illegal act and its perpetrator.

  Digital criminal evidence has been defined by some as the evidence that includes all digital data that can prove that a crime has been committed, a relationship between the crime and the offender or a relationship between the crime and the victim; and what is meant by the digital data in this definition is a set of numbers Which represent various information including written texts, graphics, maps, sounds or images.

Therefore, it can be said that digital forensics is information accepted by logic and reason and adopted by science. It is obtained by legal and scientific procedures by translating the computational data stored in computers, in its accessories and in

communication networks; and can be used at any stage of investigation or trial to prove an act, a thing, a person involved in crime, an offender or a victim.

- **Thirdly: The nature of the digital evidence:**

The issue of essence of the digital evidence raises three points in the discussion:

- Digital evidence and virtual incident.
- Digital evidence and physical incident.
- Digital evidence and dual incident.

Each of these points raises a wide discussion in this research. These three questions are the crux of the search in the essence of the digital evidence, the tool of communication between the authority of law enforcement and the investigation and the trial, and between the trial and what is a crime in law. In law, the relationship should be clear between the digital evidence and the nature of the incident whether it is virtual, physical or double.

1. **Digital evidence and virtual incident:**

The virtual incident is defined as: The incident that begins and ends within the virtual world; this incident constitutes the real structure of virtual crime in its ideal form.

The relationship between the digital evidence and virtual incident represented in idea that both are an image of each other since the digital evidence is the virtual incident itself, even if the technology is a mean to control this evidence; that does not mean that the technology itself determines the criminalization of the incident. What determines the decriminalizing and the virtual incident is the Penal Code only and this traditional determination apply to criminalization over the Internet.

In this case, the hacking crime, for example, it is committed and detected by using the same technique which the IT, where the hacker uses the same technique that the law enforcement and investigation agencies must use to detect the hacking incident.

2. **Digital evidence and physical incident:**

Sometimes a physical incident (crime) occurs, and computerization and digitization are used to detect it; in this case the digital incident effectively contributes in the

detection of the physical incident, so that the digital evidence becomes an evidence to detect the physical incident.

Here is the importance of digital evidence's detection procedures in physical incident, where the detection procedures begin with the authorization of the inspection. So we have to note the significant difference between the inclusion of an item that allows the search in computers in the search warrant and between the reservation of computer and digital materials in order to be transferred to the room concerned in conducting the inspection and extraction the digital evidence reserve it, in order to be submitted to the judicial authorities. Because such a matter is subject to judicial action if it is not been complied, and the argue on it is one of the substantive defenses which the judiciary must be subjected to it, otherwise the verdict lose it validity and has become subject to veto.

3. **Digital evidence and dual incident:**

The double incident revealed by the digital evidence, in the ability to use computers to commit physical crimes mixed with a digital character, and here the evidence will be a partnership between physical and digital.

In any case, it is not easy to get an integrated classification of the relationship between the digital evidence and the double incident; But it depends on taking in consideration its nature in terms of combating crime and reporting crimes and its perpetrators.

 Fourthly: the characteristics of the digital evidence:

The evidence in the physical world is a set of effects left by the criminal during committing the crime, and it is revealed by various proof means; while the digital evidence is completely different because it is within the digital environment. For example, the picture on the computer and on the Internet does not exist in the physical world unless it is printed.

The characteristics of the digital evidence are related to the environment in which it is in; which is the virtual environment that is reflected in the nature of this evidence.
So the digital evidence has several characteristics that made it distinguished from traditional criminal evidence:

1. Scientific evidence:

The digital evidence is an incident that tells about the commission of a crime or an illegal act. This incident substance is scientific because the digital or virtual world building is a scientific fact built by scientists and technologists.

According to this characteristic, the digital evidence can only be obtained or accessed through scientific methods. It also states that when law enforcement officers, investigating authorities, or prosecuting deal with the digital evidence in an effort to prove the truth, the search process must be based on a scientific facts because the scientific evidence is subject to the fact that it must be responsive to the whole truth.

So if the scientific evidence has its logic which it should not come out of it, thus the scientific evidence never get contradicted with the scientific facts, therefore the digital evidence has the same nature, this type of evidence never get contradicted with the digital science otherwise it loses its meaning.

2. Technical evidence:

The technique is defined as an equipment, devices and technical equations that can be employed in the performance of a task or function; thus the technique means, the forensic evidence-proofing devices, which helps to performer works and important results criminal evidence. We can say that the digital evidence is not like the traditional evidence, the technology does not produce a machine (such as a knife) in which the murderer is discovered, written recognition or money in the crime of bribery, etc. What

is produced by the technology are digital pulses, its value is in the possibility of dealing with the computer Hardwar.

This makes us decide that the digital evidence does not exist outside the technical or digital environment, but that a digital evidence must be inspired, derived, or even imported from the environment in which it come from "the digital environment". It is in the framework of cybercrime represented in the digital world called the virtual world, which is the world in the computer, the servers, the files and the networks, and the movement, handling and circulation are within this environment.

As a result of the technical nature of the digital evidence, it has gained several advantages over the physical evidence in terms of copy-ability, so that many replica copies of the digital forensic evidence can be extracted and have the same scientific value. This feature is not available in other types of evidence, which is a very effective guarantee to maintain the evidence against loss, damage and change, as well as the possibility of determining whether the digital evidence has been tampered with or modified by comparing it to the original copy using the right software and applications.

3. Concept contains diversity and evolution:

This concept means that even though the digital evidence is fundamentally unified in the composition with computer and digitalization; even though it may take several forms. The concept of digital evidence includes all forms and types of digital data that can be digitally exchanged; so that between them and the crime there is some kind of association related to the victim, which Achieve this bond between them and between the offender.

The characteristic of continuous development of the digital evidence is reflected in the developments in technology. It was not possible to obtain pictures or video through the Internet, the services were limited to text messages without pictures. But now, it is possible to connect to the network, not via fixed lines, but rather via mobile self-phone, satellite and optical fiber.

As for the term of diversity, the digital evidence can appear in different formats, such as unreadable data by controlling the source directory, as in the case of monitoring across Networks, Proxy, or Servers. It may be a human readable evidence, as if it were a document prepared by the word processing system in any system, and it

can be, also, fixed, animated, prepared by the audio-visual system or stored in the email system.

4. Hard to get rid of:

In this context, it should be said that whenever an IT connection occurs in the sense of entering data into that world, it is difficult to dispose it, even by using the tools of cancellation and deletion. It has ruled that when a computer file is deleted, the content of the file can be retrieved, as the space occupied by the file remains available as it is unless it is filled by another file, otherwise the deleted file can be retrieved using a recovery tool for deleted files. We can identify the date the file was created in, last modified and the last time it was opened.

- **Fifthly: The difference between the digital evidence and the traditional evidence:**

The difference between the digital evidence and the traditional evidence which come from the crime scene is as follows:

1. The method of copying the digital evidence from a computer reduces or almost eliminates the risk of damaging the origin evidence, where the copy method corresponds to the cerate method using the right applications and software. It is easy to determine whether the digital evidence had been tampered with or modified because it is could be comparable to the original one.

2. The relative difficulty of breaking or erasing the evidence, even if an order is issued by the offender to remove it from the computers; so the digital evidence can be reconfigured through the computer's storage units.

3. The activity of the offender to erase the evidence, also recorded as evidence, since a copy of this act (the offender's act) To erase the evidence is recorded in the computer and can be extracted later to be used as an evidence against the offender.

4. The global wide-spread of the digital evidence scene could help users to share digital knowledge at high speed and in different parts of the world, which contributes in identifying the perpetrators or their actions fast.

5. A high-capacity, the digital video machine can store hundreds of images, a small storage unit that can store a small library, and so on.

6. The digital evidence can monitor and analyse information about the perpetrator. The digital evidence can record the individual movements, also it can record his habits, his behaviour and some of his personal matters, so the criminal investigation may find its purpose easier than in the traditional evidence.

The Second Topic
Ways to collect Digital Evidence

After recognizing the digital evidence concept previously, we should talk about ways of extracting and documenting the criminal digital evidence by understanding ways used in this regard, where procedures of dealing with digital evidence is a unified process include identifying digital evidence, collecting, transferring, storing, analyzing them and prepare report about them and getting rid of them; we are going to talk about the recourses of the digital evidence.

First: the resources of the digital evidence:

Digital sets are found everywhere in our today world that could help people to communicate easily locally and globally, most people think that computers, cell-phone and internet are the only recourse of digital evidence; but the fact is any piece of technology that process data could be used in a criminal way; for example, hand-held game could hold an encrypted letter between criminals; even modern home equipment such as refrigerator an TV sets could be used to store, display and exchange illegal photos; it's important that expert are to be able and keen to identify and use the digital evidence in correct proper way.

Resource of obtaining digital evidence are found at the digital environment where the crime been committed, it's the computer of the offender or the victim, also, the equipment of the service provider. In fact, digital evidence recourses have a strong relation according to the digital evidence types according to the location we got it from.

Where the digital evidence can be obtained so as to track down the criminal and bring him to trail. So digital evidence can be divided into:

1. Computers and networks digital evidence.
2. Internet digital evidence.
3. World wide web Protocols for information exchange digital evidence.
4. World wide web digital evidence.

It should be said that, the diversity of the digital evidence means that there are several ways to get it because internet is a complex network; in spite of this the communication is easy especially with two types of internet access services (wire and wireless). Getting to the digital evidence require checking of the internet communication system, computer components, accessories and each device that could be used to access internet.

- **First: network communication system:**

It is represented in the system of checking the internet and the internet IP; the identifying of the computer used to commit the crime has become an easy thing which is called the (IP). It is normal, especially if the crime was reported or there was surveillances done by internet police; (IP) could be obtained through certain software. In case the crime was revealed, it becomes easier if the crime was committed by a (PC) this could enable the police authorities to track the offender, also, they could check the server and software security system to obtain more digital evidence.

- **Secondly: checking computers components:**

The most important digital evidence is the computer and all its components either it is hardware or software; in addition to the all means that it could be used to access network such as smart phones. Checking the offender's computer could enable and show the way he committed the crime in. Doubtless, the victim is the exposer and the result of the crime the offender committed, so checking the victim PC could enable the investigator to follow the access sources.

The digital evidence related to cybercrime could be reached through victim's or offender's computers by checking the computer system and its accessories, where computers are considered a rich source of digital evidence specially those PCs filled in

the individual archived behaviour; since those PCs have too much information related to individual activities and desires.

The process of seizing the computer to check it is the initial point in reveling the cyber-crime for the computer is the crime tool. The computer itself has two main components the hardware and the software and one more component which is in between the previous mentioned component which the information component; that why the checking is supposed to be in hardware and in the software.

1. Checking the hard disc:

The hard disc is the place where inside it a dual digital data, the hard disc is to be checked completely or partially according to the crime and its traces (its damages).

Partially checking of the hard disc is done by getting back the available information or the one that been deleted; to identify the component of the hard disc we should know the way to seize the computer, the efficiency of the person who extracting data without messing its contents. What we find after checking any hard disc for any computer is the data the offender used, saved photo and the hidden internet pages; out of which we could check the internet sites and pages addresses, also, the E-mails in addition to the outboxes and inboxes, the programs used by the suspect so we can identify his friends and what they were talking about.

2. Checking the Software:

Which is the computer Software

3. Checking the information system: the information system contains data in an exchanged digital form, also, the storing memory could be checked. The storing memory is the computer ability to save a full copy of what the internet user do while using this virtual world.

The main task of each information system is to achieve a hypothesis which is executing PC users orders. The process of checking information system is to seize all the information inside the computer that could be recovered and saved in files in any form as long as it related to crime and it could be recovered.

4. The accessories:

Development has been seen and noticed in part linked to computer such as the printer which is able to store computer outputs. There are advanced programs that could recover printers' outputs, such programs could help to know whether the person had printed pages including pornography context via internet in accurate day and time of doing it, estimating if the PC owner is one of the cyber-crime committers, so the determination of what has been recovered in printing if its belong to him (the offender) is completely according to legal authority. Also, the keyboard could be checked where the cyber-crime offender could control the keyboard so it could be a reliable evidence.

Thirdly: mobile smart devices:

Previously cell-phones used to be used for audio-calls only, today they are used, also, to take digital photos, movies, sending SMS, browsing internet, executing multitasks as same as a computer. Smart mobile phones allow and enable offender to sign in in different groups and doing more activities and it enables to track each step in internet, so the tracking features convert the cell-phone to a major evidence in many cases.

The digital evidence in cyber-crime could be obtained through mobile smart devices either for the offender or the victim by searching all data inside it such as applications, SMS, voice messages, photos, video or phone calls.

Fourth: internet users:

Committing both internet crime or cyber-crime has in general more than two sides, the offender, the victim and the internet service provider. So the first step to be done by the concerned authorities to search at:

1. The suspect:

To check the computer and smart phones he has especially if the crime committed by using these devises. Computers are to be checked completely including: the permanents storage unit and the sub-accessories unit that include: the floppy disk, CDROM and other storage unit that could be used such as removable disk.

2. The victim:

He could be a normal person; the concerned authorities could investigate the remained traces that could be left by the suspect. That's done by checking both: the systems and the virtual crime scene taking all the required measures to preserve the digital evidence.

3. Internet service provider:

We could ask his help to find out the available evidence he has whether it is an international provider, such as: (Facebook, YouTube and Google) or a local service provider, where the internet users' private data were recorded and saved, also, how do those users use these service.

Secondly: seizing digital devices:

The seizing is the process of transferring the potential digital evidence from its original location to other environment in order to be analysed later; the aimed devices in the following position that fixed the used way in seizing the require tools:

- A device contains the potential digital evidence in operating mode.
- A device contains the potential digital evidence in shut dawn mode.

The seizing process includes the following general steps:

- The documentation of the used method in the seizure process and in the chain of custody/ preserving evidences by using forms.
- Naming devices to clearly distinguish them.
- Seizing the potential digital evidence up to the priority that was set in during identification process.
- Identify if we could collect the potential digital evidence via the internet service provider or via mobile company by asking that.

- Pay attention to the special requirement for the seizing process depending on the set mood.
- Packaging the set before transportation.
- Gathering the non-digital evidence or tools that have nothing to do with potential digital evidence, such as: password, encrypted keys, etc...
- Meeting people at crime scene or at searching places to get information that could be related to the case.
- Seizing the potential digital evidence according to the procedures by asking for a searching warrant.

We should know the status of the amid device during the seizing process so as to lessen the damage on a potential digital evidences.

- **How to collect the digital devices:**

The stored digital information inside the digital devices are so sensitive and easily to be lost, that's why certain procedures to be identified and followed to seize those devices in a correct way. As soon as the crime scene is secured and police expert are allowed to use the evidences; devices could be gathered and passwords and codes are to be taken form certain individuals if possible, in addition to, chargers, cables and any other guiding evidences.

The first user needs to take care of digital device in particular, in addition to the normal used procedures in collecting evidences so as to prevent exposing these devices to heat, humidity and static electricity.

- **Collecting mobile phone:**

Immediately turn off the device and remove the battery if possible; turning off the mobile preserves the location information for the mobile phone calls files, it stops the possibility of exploiting the mobile that could change its data. In addition, if the mobile is set on the remote destruction which could be used without the knowledge of the police experts; some mobiles have the auto-mode to start getting the updating so that could harm data so that removing the battery is the best solution.

If cant switch off the device it should be isolated from the transmitting tower by putting it into bag faraday or any other isolating modes, using air plane modes, switch of Wi-Fi, Bluetooth or any other communication system. Digital devices are to be preserved in an anti-static electricity bags, we should avoid using plastic bags because they could transfer static electricity and humidity.

In emergency situation or life risk cases mobile information could be removed and kept at accident place, but we should be cautious to preserve data.

- **Collecting computer devices and the equipment:**

To prevent changing digital evidence during collecting process the responding teams should document any activity on the computer device or the components through taking photos and recording any information on the screen; the expert could move the Mouse without pressing the buttons to check if there is something on the screen. If the

computer is in the operating mode we strongly advice to call for Cybercrime expert because if the computer is turned off we could lose the contact with the criminal activity, if the computer is on the operation mode but starts a destructive operation, we should unplug it immediately to preserve the left data on it.

Office environment makes collecting data more difficult, because of the networks and the probability of losing required data. For example, if the server is turned off the clients will not be able to get their services which are harmful for them. Office equipment that could have evidence is to be collected such as photocopying machines, scanners, cameras, etc. Also, turned off computers could be collected as a digital evidence.

- **During collecting digital evidence we suggest the following so as to secure the safety of gathering and documenting:**

- Be committed to laws, regulation and guidance related to crime scene security.
- Plans should be put to the must be taken procedures and make sure you are authorized.
- The location of electronic devices including PC and mobiles should be known because data or digital evidence in such devices (smart phone or mobiles phone) could be erased or destroyed if there is an active connections in the devices.
- Avoid touching the devices at crime scene by unauthorized people including rejecting any technical help by unauthorized people. - Restrict accessibility to the devices places.
- Don’t change the mode and status of electronic devices.
- Make sure to keep the digital evidence in a secure controlled environment, or in a place of no-high heat or humidity and not to be exposed to magnetic, dust, vibration, etc...

- Don't turn on the shut dawn computer and vice versa.
- At crime scene the written passwords, papers, calendars, diaries, printed papers, etc. are to be looked for.
- Suspect people are to be separated, identified and registered (suspect, witnesses and etc...) at crime scene.
- For primary interview the following information should be noticed up to laws and regulations:

• personal information:

  - Owner and/or devices' users / system at crime scene, passwords, users name and internet providers
  - All passwords are to be looked for
  - Multiple passwords are might be in need such as (input and output system) so as to access the system, networks, internet providers, applications file, PGP passwords, other encrypting program, E-mail and etc.. ○ Accounts such as: My Space, Facebook, Twitter and etc..
  - Data remote control devices (that couldn't be found at crime scene).
  - Documentation that interprets the hardware and the software on it.

• Gloves and special clothes are to be used if necessary to preserve finger prints, DNA and other samples that could be used as an evidence such as: keyboard, Mouse and mobile devices to preserve information.

• If the computer is switched on or if that wasn't confirmed the following steps should be taken: ○ Look for indicators that the computer is on such as ventilation sound and dick movement sound, and etc.. ○ Check the screen to see if is any signal shows if the digital evidence are destroyed such as these words: "delete, remove, copy, move, cut, scan and etc."
  - Looking for evidences that show the possibility of any remote connection situation.
  - Looking for any possibility for active liaison such as: windows messages in internet chat rooms.
  - Check all cameras if they are on operating mode.

- The person in charge of preserving evidences and criminal digital evidence should be informed if the electronic devices provided with battery to guarantee preserving data.

- **The three type of reconstruction digital evidence:**

1. The correct digital evidence
2. The digital evidence that were erased or messed up.
3. The marginal digital evidence.

It is very important to use these three types to reconstruct the digital evidence; because by using them we extract information related to crime and criminal by checking them. The digital evidence that was messed or erased could be reconstructed by using special programs for this issue; the marginal digital evidence plays a decisive role in reconstructing the erased ant the messed evidences, also, it completes the shortages in the extracted digital evidence from the correct digital evidence related to relationship between the criminal and the crime.

- **Thirdly: the difficulty in collecting digital evidence:**

There might be a problem in extracting digital evidence for difficulties related to the size and quantity of data related to this crime, its big size and the easiest way to destruct it, one person is enough to press one button to erase huge quantity of data related to a cyber-crime or to a non-cybercrime. But it facilitates in proving the crime and who committed the crime.

Fourthly: documenting and securing electronic evidences:

Documenting is considered an important accurate and important phase in each step of collecting and analyzing evidence; there are many ways for documentation, the most important is the traditional one by using pens and papers which is hard to forge as in E-files. There are special software that help in documentation but it’s important to

document the usage of theses software. Photography and video recordings are used in documentation too.

We could gather between the previous methods but each page and file must be signed and a serial number must be given during documentation for credibility; some stipulate the presence of witness with their signature on all documents during the documentation.

The importance of documentation in each phase is to show others what was done during collecting evidences and processing them in addition to display how to produce those extractions again. Generally a protocol must be set so as to enable experts checking the result to follow up the written steps and the expected result of each step.

The preparation phase for collecting process begins, goals are set to what is expected to collect and study, the collecting process is described in an accurate way where no element of the evidence is to be lost or neglected. We focus on the privacy of the collected data so laws and procedures are to be taken into consideration which are related to the privacy of the individuals specially those who has no relevant with crime in the investigation.

Not following those criteria in this stage make the evidence questionable, after that, the evidence is preserve by a serial standard steps which assuring that the evidence is unchangeable, also, the evidence environment must be preserved to not allow any one to entry or contact with the evidence by using physical protection (the safe); also, using networks protection tools that prevent reaching these equipment and evidences. Special forms are to be filled with each evidence and its place. Also evidences to be separated whether it is switched on or off.

Fifthly: extracting digital evidence phases:

The technical development in the field of the digital treatment systems and the special nature of the digital evidence will certainly cause a big change in the nowadays concepts about the procedures and the ways of obtaining them. Which is certainly require a reevaluation for the traditional procedures in the Code of Criminal

Procedures; in addition, to create other sanction norms fit the nature of the technical environment.

The process of the investigation in the digital evidence starts by law authorities through the movement of the specialized team to crime scene, the collecting and preserving evidences and sending the evidences to the forensic lab to translate the analyses in order to prepare the file and offer experiences. Those authority follows preserve procedures through:

- Preserving it by using copies during the lab analyzing.
- Prepare a report about each completed process till the end of the analyses.
- Set an order, which register the contents in all phases.

Certain rules are followed related to the right used procedures in committing the crime through:

- Checking if this technique been used before, is it possible to try it again?.
- Checking if this technique been published or evaluated by a special lab.
- Checking error rate it could include also different types of needed supervision.

It is important to develop ways for police and experts work so as to follow up the new techniques and methods and prevent using traditional ways in dealing with crime; crimes need a big knowledge of modern techniques to prove the crime also we could consult experts in this field when needed.

Sixthly: analyzing digital evidence:

It is important in this stage to start working on a digital evidence replica but not the original copy which is used as a reference later. This phase starts by separating unnecessary data from inspection process that is because of the numerous numbers of data in the seized devices which needs tens of years to be studied one after the others.

First, we separate what is useful out of what is not useful for the case, also we separate according to the evidence location; for example, if the search is for prohibited context the focus should be only on the photo files and excluding the other content.

Seventhly: displaying the digital evidence:

Displaying phase is the last one in proving or denying the processed digital evidence during the investigation; the success of this phase depends on the credibility of the expert who took over this case, how he displays evidences and his belief of what he is displaying, no contradiction or ambiguity in his testimony, his commitment and accuracy to his job are checked also.

The documentation file that been prepared by him plays a major role in the detailed procedures; also, when displaying the evidences we have to focus on accuracy and addressing others up to their technical knowledge, for example, a completed detailed report is to be displayed in front of technical evidences experts on the other hand the result, the abstract and the procedures are to be shown in front of the judges and prosecutions.

So we noticed that the difficulties face the expert witness are the public nontechnical experiences inside the court, unlike to what been documented of detailed technical evidences, also, the possibility of technical experts intervention to examine the expert work, they could find errors in some expert's procedures.

Eighthly: terms of accepting digital evidence tools and programs:

The feature available in tool of getting and analyzing digital evidence so as to be accepted by court should have:

1. It could be accurately clarified and identified in any criminal investigation process; the use tool is to be identified and determined the way it works on, in addition to the aimed goal, that's why the problem should be displayed in a clear way, to detailed the expected out puts then declare tool's working steps. In the end, criteria should be built to measure and evaluate the sued procedures; that's how to make sure that the used tool in processing evidence dose clear specified work.

2. It's outputs are predictable, the used tool's tasks are to be known, if previous prediction and knowledge of the output failed then the tool is unaccepted; in order to look for certain text inside the files, the previous knowledge is needed

to know whether this tool is able to display the file having the text in addition to the place of the text. But if the tool collects files and changing it the tool is unacceptable.

3. It could be repeated, the used tools with same condition is giving the same result in case of repeating the process again and with acceptable allowed error.

4. Its validity could be checked, of the most important terms used in investigation so as to make sure of the validity and credibility of the achieved results; not only in the checking environment but by comparing results using others tools used for the same purpose. For example, if an investigator uses investigation tools (ENCASE), and other investigator uses (FORENSIC TOOL KIT), is it expected to get the same result? If not, a question is to be asked, was their error by the used program or by the investigator. In general errors are made by investigators in interpreting the evidence because the tools are internationally trusted and used.

❖ Conclusion: -

Palestinian Experience in the Collection of Digital Evidence

One on the important features of the information age is the wide spread of personal computers and the worldwide internet (web). These days, most of the elements of the economy and society rely on the digital information and on digital communication in un-precedented way.

The recent years reveal the appearance of new behavior and criminal act through the internet which was not known before. These aspects have started to threaten the security and safety of individuals and institutions. And in the light of the spread of the use of the internet in the electronic trade, it is believed that forms of cyber-attacks and threats will increase, and therefore we need to acknowledge the existence of such crime and to highlight its dangers. In addition, we need to take very firm and strong stand in order to fight such crime and to find the necessary solutions. Therefore and in the beginning of 2013, Mr. Hazem Atta-Allah, the head of the police force, issued the

necessary instruction to establish a specialized unit to deal with these kinds of crime as part of the general investigation department.

As a result, the structure of the unit was formulated, which was based on the existence of a centralized unit specialized in the resolution of complaint through technical ways after being referred by the first respondent team which was formed during the establishment phases of the unit. These respondent teams were distributed in the various provinces. The teams' responsibility is to receive the complaints from the public and to refer them to the centralized unit, and to complete the complaint process after receiving the technical outcome from the central unit, and then to collect the electronic devices used in committing the electronic crime(s). The confiscated devices are then transferred to the lab of the digital evidence. The digital evidence lab consists of three stations: the central unit tasked with the … and analysis of the digital evidence from the smart devices, the second is tasked with testing computer devices and storage units, and the third deals with surveillance systems where the digital evidence is collected, stored and, analyzed, before the evidence is presented to the investigation department in main unit and provinces in order to draw lessons from the outcome, and to provide the legal team with the report of the experienced technical unit.

The working manner of the investigation unit was specified by the central unit through the various training sessions provided to the members of the investigation team regarding how to deal with the crime and the proper process of collecting and safe keeping of the electronic equipment to warrant the protection of the digital evidence until it is delivered to the legal department.

It has been observed that throughout the work of the specialized unit that the collected digital evidence that has been stored in the laboratory of the has been increasing since the laboratory it was established until now in spite of the limited tools and program available in the lab. It was necessary therefore to build and to develop a way to deal with the gathering of the digital evidence and its protection, starting from the scene of the crime until the evidence is presented to the legal department, in the shortest possible time, although the available resources are very limited. The following highlights the percentage increase in the number of acquired evidence during the last three years:

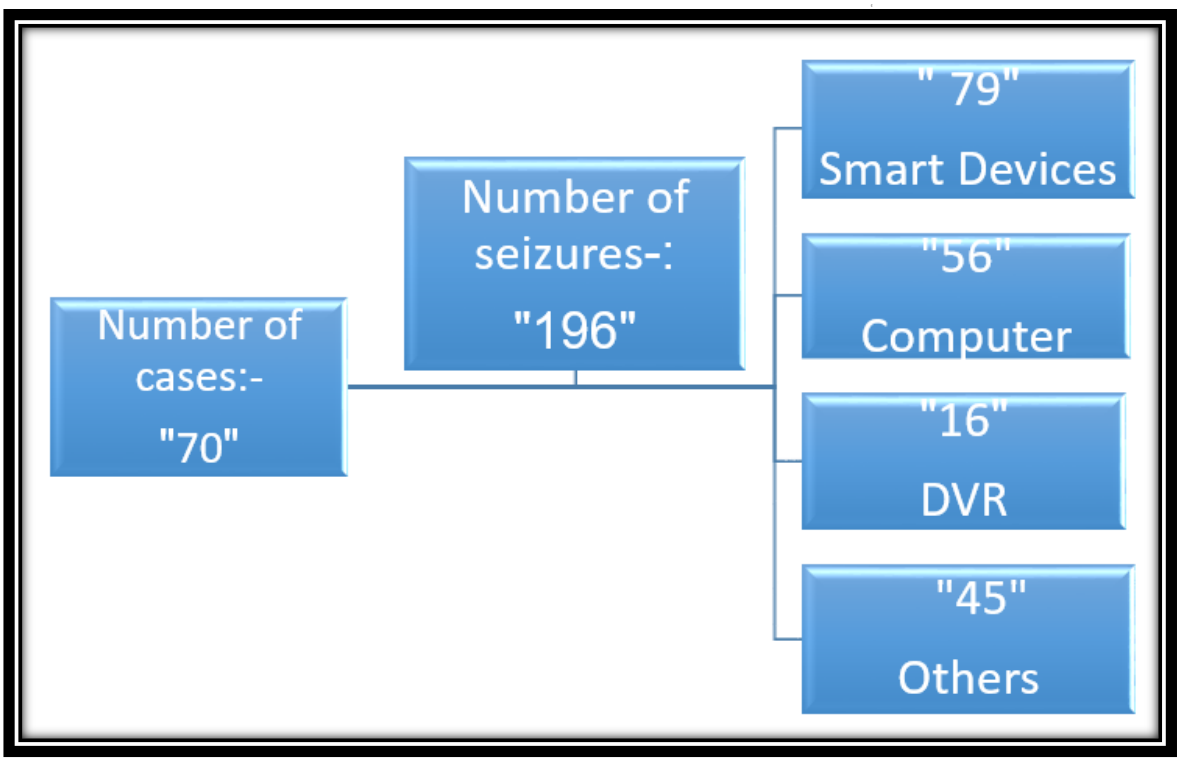


Figure I - Summary of seizures over 2016

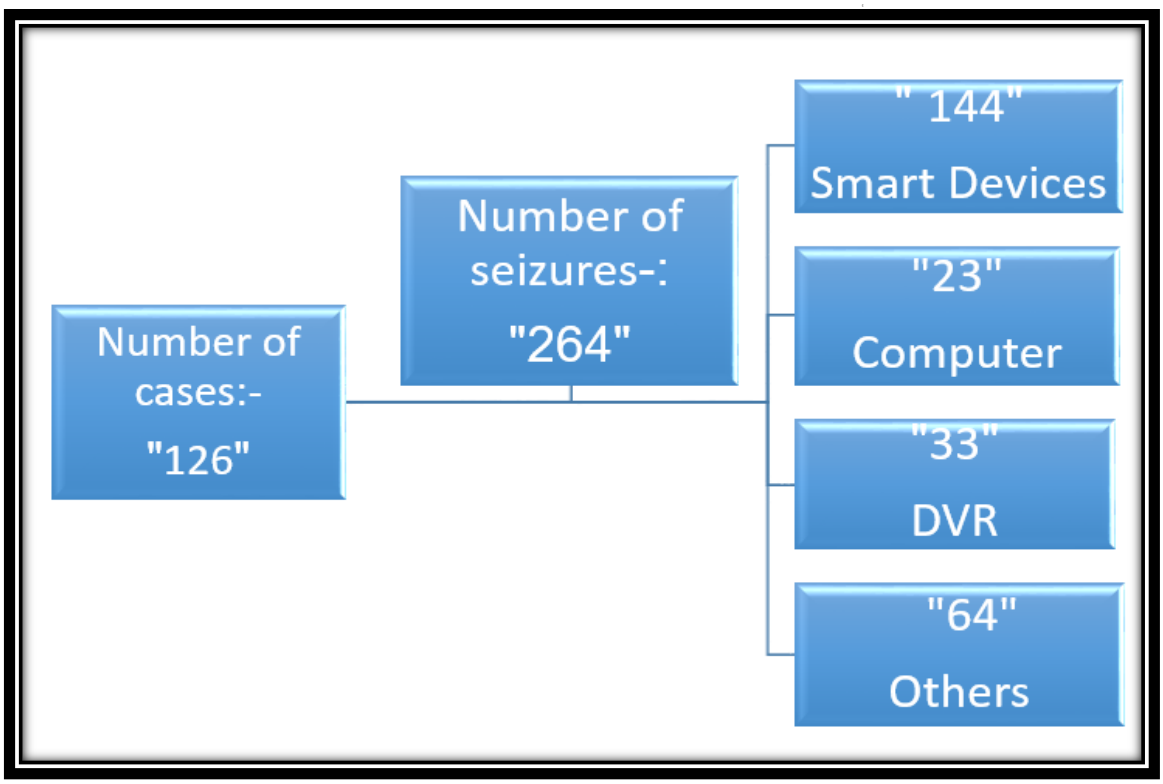


Figure II - Summary of seizures over 2017

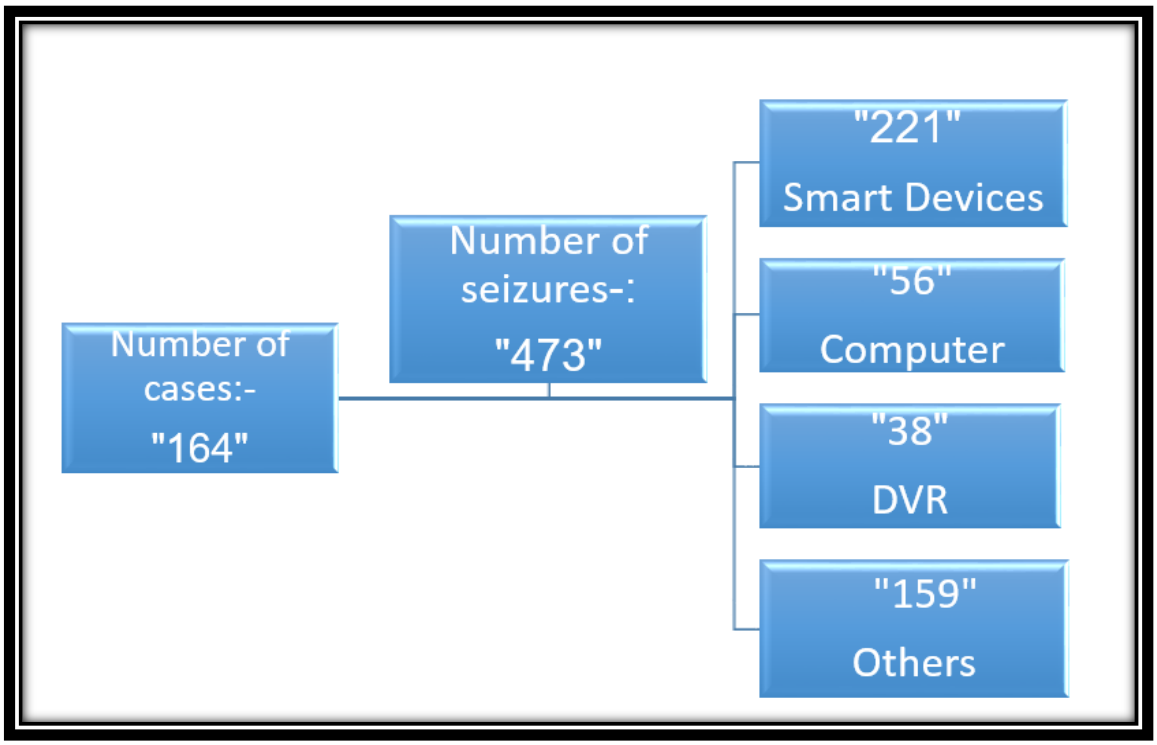


Figure III - Summary of seizures over 2018