AN INTRODUCTION TO DIGITAL CRIMES

Safiia Mohammed

B.Sc (honours) of Computer Science, University of Khartoum, Khartoum, Sudan

ABSTRACT

Because the technology is used largely in the last decades; cybercrimes have become a significant international issue as a result of the huge damage that it causes to the business and even to the ordinary users of technology. The main aims of this paper is to shed light on digital crimes and gives overview about what a person who is related to computer science has to know about this new type of crimes. The paper has three sections: Introduction to Digital Crime which gives fundamental information about digital crimes, Digital Crime Investigation which presents different investigation models and the third section is about Cybercrime Law.

KEYWORDS


1. INTRODUCTION

Digital crimes or cybercrimes is not a secret particularly during the last ten years. People are depend on computers or mobiles devices to do their work every day, they also use them in social networks to communicate with their friends and families, all these activities produce a massive amounts of data and information on computers/ mobile devices or pass through different kinds of computer networks. If these data and information did not have enough security and protection then it will be exposed to theft and destruction. Digital crime begins when there is illegal activity done to data or information on computers or networks. In the early days of cybercrimes, the crime was committed usually in the financial field, but Cybercrime now has evolved to include other forms, for example information systems for one reason or another can be stolen or damaged -by some one- in companies, also computer or mobile devices can used as a tool to committee the crime and in general the rate of digital crime is increased clearly after the advent of the Internet. Networks also play a significant role in increasing the rate of cybercrimes. The high cost of cybercrimes and the damages resulting from it called the international community and law specialists to enact cybercrime laws ,some countries started to enact national cybercrime law and other have not enact it yet.

2. INTRODUCTION TO DIGITAL CRIMES

2.1 What Is Digital Crime?

Digital crime has many synonymies for example: cybercrime, electronic crime and computer crime are changeable words. Firstly computer crime term was used to denote to any criminal activity that done against computers and networks or using computer as tool to do that activity. But in the last few years these crimes extend to encompass other digital devices like cell phone, so the term was extend to digital crime. There is no one definition for digital crime until now and it’s difficult to form standard one, however what can be said is that: digital crime is focused on
2.2 Characteristics of Digital Crime:

Unlike traditional crime digital crime has unique Characteristics. For example it has no geographic boundaries, so digital crime can be committed in one country or region against other country or region, furthermore in digital crimes Offenders usually don’t leave physical trace instead of that they leave digital trace.

2.3 Digital Crime Environment:

In usual the environment of digital crime is described as virtual environment because the crime is done on computer data, digital systems or networks.

2.4 Brief History of Digital Crimes:

Digital crimes were differed and varied since 1960 (in that time the telecommunications systems were affected by attacks) to now. In the early era of information systems, computer crimes were committed by some employees, also physical attacks on computer system was common in the time between 1960 and 1980. In 1980 malicious software was begun to appear against personal computers.

In the beginning of 1990s the internet had been a significant factor of increasing digital crimes; criminals were access to poorly protected systems using unauthorized way usually for financial gain, credit-card fraud for example was grown rapidly in the middle of 1990s. By the end of 20th century and the beginning of 21st credit-card fraud was involved into broader category called identity theft. Criminals were thieving identities of other people to do illegal activities. In 2008 it was being the fastest growing form of fraud.

Cell phone crimes are being increasing these last few years, beside these, nowadays a new type of criminal activities is being done on cloud computing. [2]

2.4.1. Roles of Computer in the Crimes:

According to Donn Parker (a computer crime researcher) Computer has four different rules in crimes (this is taken from an investigative point of view):

- A computer as an object of a crime (e.g. computer can be stolen as itself).
- A computer as a subject of a crime, that is computer is an environment of a crime.
- A computer may be used as a tool for conducting a crime (e.g. to access to another computer and commit a crime there).
- Using a symbol of the computer to doing illegal activities. [3]

2.5. Types of Digital Crimes:

Offenders committed different kinds of digital crimes or cybercrimes such as:

- Assault by Threat: Threat the lives of others or Attempt to vilify other people by using computers, networks or phones.
Cyber laundering: electronic transfer of illegal money to hide its source or destination. Cyber theft is using a computer to steal: use a computer in Criminal activities, for example: DNS cache poisoning, espionage, identity theft, fraud, malicious hacking and plagiarism. [4]

2.6. Digital Evidence:

There is no complete crime; the offenders have to leave traces behind them. Since these crimes are digital crimes, these traces will be mostly digital evidences. These evidences will help significantly to find out the identity of the offender.

What is Digital Evidence?

“Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi”. Data here refers to different types of information like text, number audio or video [3].

These different types of digital data are useful in the process of investigation. Sources of digital data can be divided into three categories:

- Open computer systems: are computer systems that known to the majority of people such as laptops, desktops, and servers. The increasing of storage space in these computer systems guarantees that we can obtain a large amount of digital evidences (e.g. one file could contain a significant amount of digital data).
- Communication systems: Traditional and advance telephone systems, wireless telecommunication systems (SMS/MMS messages,) and the internet (e-mail) are rich sources of digital evidences. The content of messages transferring between these communications systems is important in the investigation.
- Embedded computer systems: many embedded computer systems like Mobile Devices, Navigation systems, Microwave ovens and others systems can contain many valuable digital evidences. [3]

2.7. Challenging Aspects of Digital Evidence:

Like physical evidence, digital evidence has several challenges:

- Digital evidence is a kind of evidence that is very difficult to handle. For example a hard drive has many platters each of them consists of many amount of messy and disorderly data it’s very difficult to extract available data from it.
- Digital evidence is an abstraction of some digital object or event. For instance, if computer is used to perform some tasks not all aspects of these tasks will be remaining, only a few of them give us partial view of what is occurred.
- Digital evidence is usually circumstantial. If a case only depends on single digital evidence usually it will be unacceptable and additional information is needed to support that case, otherwise it will be considered as a case with weak evidences.
- One problem that is faced by Investigators is that digital evidence can be altered, obscured or deleted by offenders or even unintended during the investigation process.[3]

2.8. Impacts of Digital Crimes:

As the number of the internet and computer users is increased, this leads the digital crimes to grow up fastly, and subsequently, there will be many impacts of them. Digital crime or
cybercrime is becoming now one of the challengeable issues for governments, Legal institutions, organizations, companies - which their work depend directly on computers and the Internet - and even the public opinion; because it is in a steady increase and Caused heavy losses. In United States and other countries digital crimes have become on the national level, they created groups and regional centres to investigate this type of crimes, but the intensive requests had led it to become unsustainable as the result of the pressure of the work.

2.8.1. Economic Impact:

Economic impact consider as one of the significant impact of digital crimes. Cybercrime has direct and indirect financial cost impacts, for instance Theft of user accounts-direct impact- and reset back these accounts -indirect impact-. [5] the report of the global council on organized crime (2012) said that the economic impact of cybercrimes in business reached multibillions dollars. If we return back one year (2011) the cost of global cybercrime activities was estimated between 300 billion to 1 trillion dollars. Just in America it was estimated at about $24 billion to $120 billion [6]. In 2011, a report made by United Kingdom government reveals that the overall economic effect of cybercrime in UK was £27bn a year [7]. In 2013 the cost of cybercrime and cyber espionage done by the McAfee security firm in the US was estimated by $100 billion per year, while global impact was around $300 billion annually [8]. In South Africa according to Symantec’s report that was done between July and August (2013) there are over 1 million victims in South Africans. Cybercrime costing the country about $337 million or $233 per victim. [9]

In United Arab Emirates the statistic data shows that in 2011 the economic cost of cybercrime reached over $600 million per year [10]. In Saudi Arabia the overall cost of cybercrime in 2013 exceeded $6 billion [11]. In 2014 cyber crime In Arab region is considered as the second type of economic crime (according to PwC Middle East Economic Crime Survey 2014).[12]

3. DIGITAL CRIME INVESTIGATION

3.1. Why Digital Crime Investigation?

The new terms in crime language like digital crime create new type of crime investigations that related directly to cybercrimes [3]. Digital crime investigation like other type of investigations tries to answer common questions like: who, what, when, where, why and how [13]. Investigator firstly asks these questions and tries to solve them; in the end the ultimate goal behind the investigation is to discover the truth and the real criminals by tracing back what they leave behind them. But here the crime scene which will be investigated is not a traditional one it is a digital scene.

3.2. What is the Role of the Digital Crime Investigator?

A cybercrime investigator has to be able to collect the significant evidences from crime scene; evidences mean in particular digital evidences which criminal can leave them behind in computers, networks or any digital device. An investigator has to be able to discover these evidences and deal with them in a proper way because digital evidences are sensitive to any changes; also he/she has to well understand the legal issues that related to digital crimes investigation and be ready to any risks through his/her work. [14]

3.3. Investigation Process (General Glances)

Investigation process begins when someone report that there is a criminal activity takes place, when investigator arrived to crime scene there are many steps have to be done: firstly investigator
should has clear plan to start the investigation including where and how to search, collect evidences (digital evidences and sometimes physical evidences) and seize them, also he has to take pictures - for documenting purpose - for crime scene and evidences. Investigator may require a warrant to seize evidences if a suspect has essential evidence. After investigation process has been finished there must be a report including details describing what happen in the crime and Note down all his observations, after that all these information will be analyzed. [13]

There are many models and frameworks used to conduct digital crime investigation process. The main purpose of these models or frameworks is to carry on a successful forensic investigation, although there is no a clear restrict on choosing which model, but the obvious rule is to use the most suitable and efficient one depending on crime case. This part will discuss different investigation models:

3.3.1. Computer Forensic Investigative Process (1984)\textsuperscript{[15]}

This process was proposed by M. M. Pollitt which consists of four phrases as shown in figure 1 below.

![Computer Forensic Investigative Process](image)

**Figure 1: Computer Forensic Investigative Process**

- Acquisition: Accepted evidence was acquired authoritatively
- Identification: after acquiring the evidence, digital components was identified and transformed to human format.
- Evaluation: digital components were evaluated to check if they are relevant to case that is been investigated and if they legitimately acceptable.
- Admission: after all these phases the evidences will be presented at court.

3.3.2. DFRWS Investigative Model (2001)\textsuperscript{[15]}

It’s a proposal for an investigation process which presented by the first Digital Forensics Research Workshop (DFRWS), this model has 6 phrases as shown in figure 2.
Identification: identified tasks like profile detection and system monitoring are accomplished.
Preservation: the purpose of this phase is to ascertain that the collected data is not a foul data, e.g. to guarantee that there is an acceptable chain of custody.
Collection: data that related to the case are collected using recovery techniques.
Examination and Analysis: after those phases evidences were examined to ensure that these evidences are validated and related to the case that is focused on also encrypted data is recovered.
Presentation: the last phase in which the investigation is documented and expert testimony is taken.

3.3.3. Abstract Digital Forensics Model (ADFM) (2002) \(^{[15]}\)

This model is an enhanced model for previous one (DFRWS Investigative Model). The authors (Reith, Carr & Gunsch) presented three additional phases (Preparation, Approach Strategy and Returning Evidence) now it will be nine phases. (See figure 3)
These new phases are mentioned briefly here:

- In preparation phases investigation tools and techniques are perpetrated.
- Approach Strategy phase is aim to ensure that the evidences is free from contamination and the negative effects for the victims are the least that can be.
- Returning Evidence: this phases check out that if evidences are returned back safely to their original owners.

3.3.4. Integrated Digital Investigation Process (IDIP) (2003) \(^{15}\)

It’s introduced by Carrier & Spafford, their aim is to integrate several investigation processes into one model. In this model the digital crime scene was included to present a virtual environment where digital evidences of a crime are exist. (See figure 4)

- Readiness phase: in this phase the investigation equipments have to be ready and staff must be trained. Everything must be ready to begin the investigation process.
- Deployment phase: here the crime or accident is detected and then investigator knows that there is a crime that has been committed.
Physical Crime Scene Investigation phase: this phase is concerned with collecting and analyzing physical evidences.

Digital Crime Scene Investigation phase: like the previous phase but here the digital evidences are collected and analyzed.

Review phase: all previous steps of the investigation process are reviewed to make any addition or enhancement to the investigation procedures if necessary.

Note: It is worth mentioning that readiness and deployment phases have a number of sub-phases.

3.3.5. Enhanced Digital Investigation Process Model (EDIP) (2004) \(^{15}\)

In this investigation model Carrier & Spafford intended to enhance the previous model, two new phases were added: Traceback and Dynamite. We will explain briefly these new phases:

- **Traceback**: To track down the trails that left by offenders
- **Dynamite**: here the investigation process focuses on the crime scene and works hard to discover any information about criminals.

![Enhanced Digital Investigation Process Model](image)

Figure 5: Enhanced Digital Investigation Process Model

3.3.6. Computer Forensics Field Triage Process Model (CFFTPM) (2006) \(^{15}\)

In this process the phrases: identification, analysis and interpretation are provided in short time on-the-scene. This model has six main phrases and another 6 sub-phrases as shown in figure 6:

- **Planning phase**: Good planning ensures the success of the investigation process.
- **Triage phase**: here the evidences have been ordered according to their importance, the most important of them has to process first.
- **User Usage Profile phase**: in this phase the users’ activities are analyzed in order to associate evidence to the Suspect.
- **Chronology Timeline phase**: the purpose of this phrase is to arrange the probable crime activities in time.
- **Internet phase**: in this phase the internet related services are examined.
- **Case Specific Evidence phase**: here the investigator has to adapt the examination to focus on specific case.
3.4. Digital Crime Scene investigation:

After an investigator reach the crime scene the real investigation process is began, the important part of investigation process and next steps are depended on it. An investigator should recognize significant evidences in the crime scene; he/she also has to identify these evidences and their sources. As done in traditional -physical-crime scene evidences must be preserved and documented. The thing that should be kept in mind is the importance of integration between physical and digital crime scenes, the scene of the crime has physical part and digital part and they cannot be separated.[3] (See figure 7)
3.4.1. Guidelines for Handling Digital Crime Scenes:

There are many guidelines that can be followed by investigators to help them to accomplish the investigation of digital crime scene. One of the best guidelines is called “The Good Practice Guide for Computer Based Evidence”, ACPO Guide has four fundamental principles:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to Computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. [16]

3.4.2. Authorization issues:

Before beginning to search the crime scene for finding out the evidences, there are some authorizations issues must be bear in mind:

- The investigation or search process must not go against law.
- Computer security professionals have to hold authorization before any investigation process inside their organization.
- Sometimes a search warrant is required when evidence is needed to seized. [3]
4. CYBERCRIME LAW

There are many laws to control different kinds of crimes and digital crimes or cybercrimes are not exception. Cybercrime has no Geographical boundaries and the entire world will be affected.

The world and on the united nation level recommended to make effective laws against cybercrimes, it want to establish “an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime”. There are also collaborative works between countries (e.g. United States and the European Union in 2010) and works groups from institutions to fight cybercrimes and discus security and legal issues (for instance Cybercrime Legal Working Group established by The East West Institute in 2010 (EWI)).[17]

This section briefly introduces some about cybercrimes laws in developed countries (as example here U.S and Europe) and in developing countries (African and Arabic countries as example)

4.1. U.S Cybercrime Law

In the United States and because of its federal nature it has two levels of cybercrime law, one on the level of whole country and the other on the level of each state. In general Federal Cybercrime Law concentrates on cybercrimes like: Computer Fraud and Abuse Act, Identity Theft, Child Pornography, Copyright Infringement, and Trademarks and Trade Secrets but, states may differ in their legislations.[3]

4.2. European Cybercrime Law

European Cybercrime Law Falls under two legal frameworks: European Union (EU) and the Council of Europe (CoF), the last one has Cybercrime Convention on cybercrime side, where as the EU is apolitical union and each country in it has its own implementation for criminal legislation. [3]

4.3. Cyber Legislation in African countries

African countries start to concentrate with cybercrimes, in the beginning of second millennium some of countries began to set some laws that control the cyberspace, but in that time these laws were not took the form of cybercrime law yet. In the middle and end of first decade of the second millennium some countries were legislated laws for cybercrimes (Sudan is the one of these countries; in 2007 the cybercrime law was adopted). In general these laws work against cybercrime like: damage or illegal access to computers, misuse of information systems or electronic communication service, Computer-related forgery or fraud, child pornography and other cybercrimes. The penalties range from fines to imprisonment for months or years.

4.4 Cyber Legislation in Arabic Region

Although the cybercrimes rate is not low in Arabic countries but there are still slow procedures for activating a cybercrime law. Few Arabic countries have particular law for cybercrime (e.g. Sudan, UAE, Saudi Arabia, and Oman) while some other countries do not enact their cybercrime law yet.
5. CONCLUSION

There is no doubt that computer crime is not like ordinary crime, it has its own aspects that makes it different, for instance the digital evidence is more fragile than traditional evidence in other words it can be altered or damaged easily and this firstly caused many problems in particular in businesses where many people and business man lost their money by direct or indirect way. This means that digital crime has been a challengeable type of crimes and need big efforts to combat. Experts and specialists never give up they do their best to fight these crimes that is clear with many researches about computers crimes, investigation process with different investigation models and the most important, the cybercrime laws. This is not the end, like any crime digital crime will continue to be a great threat as the technology continues to be more advanced.

REFERENCES


Author

Safiia Mohammed is a computer science graduate who has B.Sc (honors) in computer science from university of Khartoum - faculty of mathematical science – computer department (2012). Now she has a big interest in digital forensic and information security field and this will be a field of her researches in the future.