SUST Journal of Engineering and Computer Science (JECS), Vol. 19, No. 2, 2018

# Digital Evidence and Best Evidence Rule

## Legal-Technological Approach headed for Digital Evidence Admissibility Review

Azhari Abdelrhman Mohammed
Bayan College of science and Technology
Email: azmoh65@gmail.com-Tel: 0919790165

Received : 22/11/2017
Accepted : 28/02/2018

**ABSTRACT-** Computer forensic whizzes do their utmost to employ effective tools and methodologies to extract and analyze data from storage devices used at the digital crime scene to acquire and be able to present admissible evidence in court. This paper is an attempt and a trial to highlight the areas of discussions and critical review of the available guidelines used to achieve successful computer crime investigation that is compatible with best evidence rule. The enforcement of information laws is a step in the right direction towards a knowledge-based well established cyber security, however having laws alone isn't enough for carrying out valid and effective confrontation against cyber criminals. Consequently this paper studies the common factors and elements in the computer crime case with focus on best evidence rule and suitable road map process of Digital Forensic Investigation Framework (DFIF) to maintain a close cooperation between parties through effective use of legal concepts and technology. The paper discusses the main challenges and basics needed to be handled, and observed closely to grasp a successful prosecution of a cybercriminal. Basically, the paper deliberates and reviews deferent investigation frameworks of cybercrime with emphasis on the most prominent frameworks, legal requirements, technological, and technical practices needed over and done with studying cybercrime categories, rules of evidence in court, employing historical critical literature review and the study of restrictions imposed over admissibility of digital evidence.

***Key Words:** Cybercrime, investigation framework, digital forensic, evidence, Storage Device, Data Recovery*

***المستخلص - أخصائيي الادلة الشرعية المتعلقة بالكمبيوتر يسعون لاستخدام أدوات ومنهجيات فعالة لاستخراج وتحليل البيانات من أجهزة التخزين المستخدمة في مسرح الجريمة للحصول على الادلة المقبول تقديمها امام المحكمة. هذه الورقة محاولة لتوفير مبادئ توجيهية لإجراء تحقيق ناجح في جرائم الكمبيوتر. فإن كان إنفاذ قوانين المعلومات هو خطوة في الاتجاه الصحيح نحو أمن سيبراني راسخ قائم على المعرفة والتقنية، فان القوانين وحدها لا تكفي لتنفيذ مواجهة صحيحة وفعالة ضد مرتكب الجريمة الالكترونية. وبناء على ذلك، فإن هذه الورقة هي دعوة لدراسة العوامل والعناصر المشتركة في قضية جريمة الحاسوب، مثل التحقيق الجنائي، والحاجة إلى الحفاظ على عملية خارطة طريق مناسبة لإطار التحقيق الجنائي الشرعي، للحفاظ على تعاون وثيق بين الأطراف من خلال الاستخدام الفعال للمفاهيم والتكنولوجيا المرتبطة بالقانون. ، النقاش في الورقة يستعرض التحديات الرئيسية والأساسيات اللازمة للتعامل معها، مع الوقوف عن كثب على تحقيق محاكمة ناجحة ضد المجرم السبراني. وتتناول الورقة بشكل اساسي المتطلبات القانونية واهم أطر التحقيق في الجريمة السيبرانية ، والممارسات التقنية المطلوبة في كل مراحل التحقيق في الجرائم السيبرانية، وقواعد الإثبات في المحكمة، وتتعرض الورقة لذلكفي شكل نقدي و تاريخي يشمل دراسة المحازير المفروضة علي قبول الدليل الرقمي.***

## INTRODUCTION

This paper is an attempt to provide the needed guidelines for a successful computer crime investigation. The enforcement of information laws is a step in the right direction towards a knowledge-based well established cyber security, however having laws alone isn't enough for carrying out prosperous investigation as well as it is not enough to carry out a real trial against cyber criminal.

All over the world, the number of computer users is increasing, and the usage of technology of information and communications infrastructure to run regular life activities is mounting [1].

Cyber security is crucial for the prosperity of digital potentials [2]. To construct secured, and trustworthy Internet services all over the world it is essential for all concerned, and information and communication providers to create procedural and policy elucidations that will allow beneficiaries to use computer technology in a protected, private, and unswerving mode [3].

Cybercrimes also not new, however, the ways and means of committing the crime are new. Numerous computer crimes are notorious, and their jurisprudence is palpable [4] .

Recent lawbreaking adjacent to the process of computer technology are likewise new similar to the spread out of the digital technology development situation [5][6] . The central purpose of the prosecution is to take along the offender to justice and have him punished [7][8]. Generally, little number of computer criminals is punished even though in many parts of the world, tough preventive actions are known. [9] Also many cybercrimes are targeted by the new laws in many countries (e.g. Sudan new law) [10].

**Objectives**

This is a critical literature review paper. The paper is tracking legal and computer technology complications facing the process of investigating and presenting digital evidence that is putative by law through deliberating ideas and solutions to these glitches. Consequently the argument in the paper will go through some areas that will comprise:

1. Rules of evidence, and types of evidence and importance of digital evidence in cybercrime investigations.
2. The paper is intended to cover types of cybernetic evidence, and new opportunities for investigation and digital forensics to reach discussion points that conclude the points needed to be observed to have legally adequate digital evidence.
3. The paper puts a deduction to the findings based on the covered phases. Also the paper will point out the points needed to be observed to obtain and process legally acceptable digital evidence.
4. The paper will conclude with the major point that will include judges, prosecutors, lawyers, police men together with all who handle the stages of the digital evidence and their need of high level of expertise and training to analyze, evaluate and understand the nature of the evidence at hand.

**Methodology**

This is a debate paper, and an invitation for more notions. The information stated in the paper is based on data selected from variety and obtainable references.

Sources of the information used in this paper include some information from papers presented in conferences and published in scientific journal publications, discussions and study reports, in concert with particulars from the literature, in addition to some examples and occasional comparisons.

**Rules of evidence**

Criminal law principally identifies a crime as an action purposely comes to existence against law by the act of the accused. [7]Evidence must be introduced to the court through the accepted legal means of introducing evidence to a court. [[12]

**Evidence admissibility**: The admissibility of the evidence in a trial, needs the proof to be trustworthy, pertinent, and relevant to the case, and it must be submitted incompliance with the convention of evidence. [10]

**The introduction of evidence**: The introduction of proof in all kinds of legal actions is an apparent crisscross; however glitches are greater when computers are involved. [2]Extraordinary familiarity with law and technological details is needed to situate, gather evidence, preserve and reposition the evidence line of attack to preserve the trustworthiness and reliability of all storing devices implicated.

**Achieving appropriate investigation tasks**: To attain the best procedure andto accomplish appropriate investigation tasks the following steps are vital:

- Defend the computer system entangled during the forensic assessment to prevent any modification, destruction of data, data exploitation or virus simplicity. Discern files contained in the beleaguered system which embraces obtainable regular files, files deleted but they are still left over in the area, secreted files, files protected by password and encoded files.
- Recuperate all conceivable, deleted files.Divulge the hidden files to check their contents and also check temporary files which could be used by the operating system and the application programs. Check the secured or hidden files if reasonable and legal.
- Evaluate all important data found in precise areas of the disk.

✓ Make a report that contains general analysis of the questioned computer system. This analysis must contain a list of all pertinent files and discovered file data. The report also must make available a summary of the system design; file structures and data information of origin. All attempts to hide, guard, delete, or encrypt information will also be exposed through the report.

✓ Make available professional opinions: The statement of the expert as a witness would be required to launch the arguments of the case in the court.

Computer related evidence is intangible and it usually comes in forms of electronic pulse or magnetic charge so this enlightens how it differs from traditional evidence.

**Evidence Types**

The popular definition of digital evidence is that it is the new beginning era of proof. It is also referred to as a computer technology used to ware house or communicate any data that chains the hypothesis of how a wrong doing was committed. [9]The most well-known types of proof are:

✓ **Direct**: this type is unswerving and strait verbal testament, by which the knowledge is attained from any witness and it is a verification or negative response to a fact in a trial. [13]

✓ **Real**: this type is made up of substantial objects that provide evidence or refute guilt. [14]

✓ **Documentary**: this type composed of data introduced to the court in definite accepted forms or conventions such as manuals.

✓ **Demonstrative:** this type of evidence is used to help the court to comprehend the matters in the trial such as expert testimony. [15]

**Digital evidence Importance in investigating cybercrime**

It is conceivable to differentiate between the two main phases of investigating digital evidence:

**The First phase**: this phase is the investigation phase which include four processes of the investigation (identification, gathering of evidence, safeguarding of evidence, and finally examining of evidence)

**The Second phase**, which includes, the processes before the court, the introduction, and then the employment of evidence in the trial procedures. [16]

Computer forensics corresponds to the disciplined examination of IT apparatus with the intention of piercing for evidence, and this is where we notice the relation between the first phase and computer forensics. The amounting volume of data stored in digital format shows the logistic challenges of investigations.

Conducts of automated forensic actions using hash-value based searches, or keyword searches have a significant role when conducting physical investigations. Computer forensics include all actions taken by the criminal, and special attention must be given to hardware and software usage, likewise deleted files are needed to be captured, in addition to uncovering users of the Internet by scrutinizing the interchange of data. [17]

The second phase differs from the first phase in that it relates to the introduction of the evidence to the court using special procedures which are required to be displayed with the use of computer technology a phase that needs well trained expertise.

**Types of computer-generated evidence:**

Computer generated evidence is digital evidence obtainable from the computer machine or, available in the hard drive and live memory junkyards [18]

The types of computer generated evidence are:

➢ On the monitor visual output.

➢ Printed hard copies.

➢ Plotters printed evidence.

➢ Recorded material on disk or CD etc...

➢ The authentic, unique evidence in the memory.

**New opportunities for digital evidence**

The most discerned advantage of digital evidence is that it is less exposed to impacts that can affect its safeguarding compared with other types of evidence.

Another characteristic that can be an advantage of digital evidence is the impartiality and dependability of this evidence. Most spreadsheets and databases are not usually copied, or printed on paper. Also, many activities in the internet are digital and can’t be found outside of the virtual area. Most of the activities in the internet has unambiguous traces which allow investigators to acquire important evidence, crack criminal cases and put a stop to crimes.

Generally, when criminals use information and communication technology and internet services, they usually leave traces that lead to their accusation and almost certainly good evidence against them. A good example for evidence generated from using communication technology and internet service is IP address, as well as identity information recorded as a result for requests to use search engines with criminal intentions. [20] Another decent example is when the suspect needs to produce unlawful image the felonious needs digital cameras that provide geoformation in the file that enables investigators to spot the position where the image was taken. One more example is that in some cases offenders download unlawful materials from networks and the wrong action can be spotted by the exclusive assigned ID generated as a result to the setting up of the file-sharing software. Finally, as a last example for traces left by suspects, the fabrication of digital document may create metadata that enables the innovative author of the document to establish the evidence against the perpetrator.

## Digital forensics

The emergence of forensics is caused by the occurrence of unlawful behaviors.[1]The role of forensics is generally classified a sex tents that accelerate investigations of criminal activities using procedures, techniques and frameworks together known as digital forensics and investigation framework. [21] The mentioned zones are manipulated to safeguard, collect, examine and provide systematic and scientific evidences for the courts; and law enforcement action.

Great number of digital forensics investigation procedures, or frame works was recognized on investigating digital crimes, and they were developed for tackling diverse tools used in the examined devices. This part of the paper will go over the most important frameworks:

**One of the early methodologies for handling potential evidence (1995) suggested four steps as a framework of this methodology which is acquisition, identification, evaluation and admission as evidence. The production of the methodology is media (substantial context), facts (rational context), and information (lawful context) [11].** In 2001(DFRWG) -The Digital Forensics Research Working Group-introduced a nonspecific investigation process include identification, conservation, gathering, examination, analysis, presentation and conclusion. The stepson this framework is termed 'classes of task' and single tasks are termed 'elements'. This framework is very important because it supports all future work on investigation frameworks.

The abstract digital forensics framework based on (DFRWG) was introduced in 2002 [26].

The abstract framework is based on DFRWG, however it consists of more phases which are, identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence.

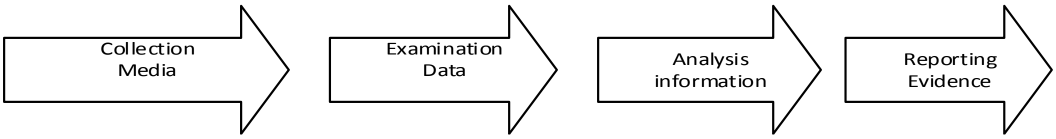

Figure 1: Cyber Crime Investigation Process

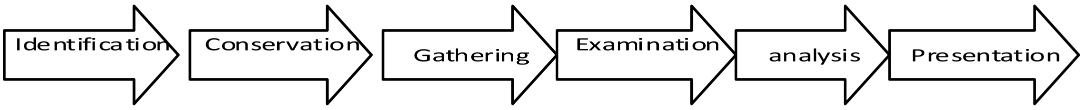

Figure 2: DFRWG Framework

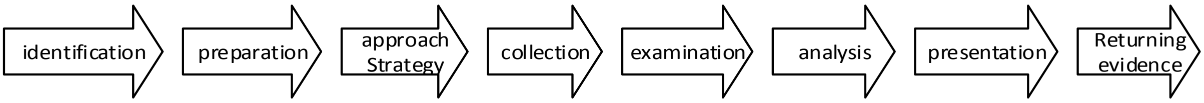

Figure 3: Abstract Framework

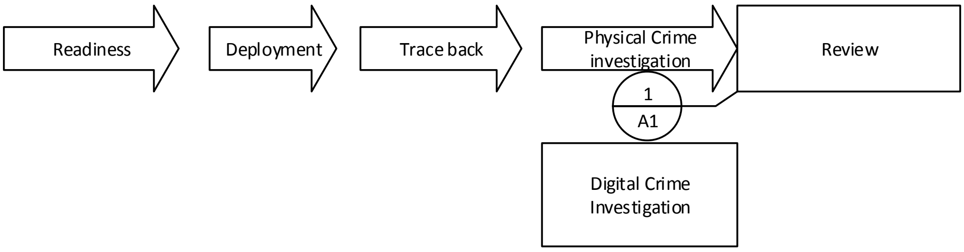

**Figure 4: IDIP Framework**

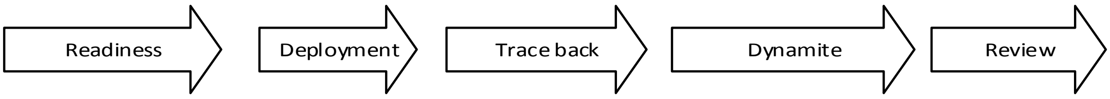

**Figure 5: EIDIP Framework**

In 2003 a framework with high level phases - Integrated Digital Investigation Process- (IDIP) is an introduction for investigating realistic crime scene. It arranges the processes into five groups that contains phases which highlight events rebuild a way that lead to incidents emphasize and view the whole task and build a mechanism for quicker forensic examination.[25] (IDIP) uses processes in DFRWS as a class and activities as elements.

A framework named End-to- End digital Investigation Process (EEDI) is introduced after IDIP. Using this framework the investigator targets preserving, collecting, examining and scrutinizing digital evidence. The investigator using this framework collects the images of the victim computers, all logs of midway devices on the internet, logs of targeted computers and obtainable logs and available data from incursion uncovering systems, firewalls, and the like.

In 2004, [1] the (IDIP) is upgraded and introduced as (Enhanced Integrated Digital Investigation Process Framework(EIDIP).the upgraded framework splits the investigations at the main and minor crime scenes while showing segments iteratively as a substitute of lined. To maintain consistency addition of two more phases is needed so as to trace back and to separate the investigation into main crime scene (the machine) and the subordinate crime scene (the physical).

Following the EIDIP an Event-based Digital Forensic Investigation Framework by Carrier and Spafford was introduced as a part of the strive to define the framework using the lack of exclusivity of examination phase in IDIP as a motive for different action before streamlining the framework and adding three new phases, Safeguarding, Exploration and Rebuilding phase.[4] However, the extra three phases contains no clue of entirety of any phase, and it is not obvious if the framework is satisfactory for Digital forensic Investigation.

Agreed about opinion stated that, the framework which is acknowledged as the furthermost comprehensive to date framework is the one introduced by Rogers, in 2006 [7] because it has faultless phases to follow in the course of the investigation beginning by arranging for the investigation when the criminal act reaches the knowledge of the law enforcement authorities, ending with the case presented to court. The framework consists of activity phases part of it is awareness, approval, planning, notification, search and identification, gathering, conveyance, storing, scrutiny, theories, exhibition, proof/defense and dissemination. The framework also provides a source for the enhancement of methods and tools to support the investigators performance [13].

The above mentioned types of frameworks, and the majority of investigation frameworks as general, are single tiered process which has only one layer procedure a reason led to the proposal of multitier process, composed of the first tier that include preparation, incident response, data collection, data analysis, presentation and incident closure, in addition to the second phase which is the data analysis phase that includes survey, extract, and examination phase.

In the two tier framework, the objective-based tasks perception is followed in the analysis phase. The introducers of this framework suggested that, this framework offers exclusive assistances in the areas of practicality and detailed objectives. The problems faced in the framework suggested by Carrier &Spafford, 2004 could also be evaded. [5].A four phase's framework is proposed by Kent in 2006 [10] the four phases of this framework include gathering, inspection, analysis and recording. The production for respectively every phase is related to the later introduced process [12]. The media in this framework is changed into evidence that can be used by law enforcement authorities' or inside the private organization. The first, change happens when gathered data is studied which excerpts data from media and converts it into a set-up that enables investigators to process it using forensic tools. The second change happens, when the data is transformed into facts through examination and lastly, the information is converted into evidence throughout the writing phase [2].

In 2006 a new framework is introduced by Kohn, Eloff, & Oliver, in which the idea is to form a new framework using all the present frameworks and accumulate a rationally comprehensive framework [3] [5] [6] [15] [17] [7]. This study has underlined two significant ideas; the first is the familiarity with relevant lawful base before forming the framework is vigorous because it will stand the entire investigative course; and the second is the process should group all the phases now available into three stages (preparation, investigation and presentation) to comply with the forensic definition [11].

In this framework the legal requirements understanding is clearly addressed, at the start of the investigation. Two requirements are necessary at each level; (legal necessities of an exact system) and (credentials of all the stages). This framework can simply be extended to contain any amount of additional phases required or found helpful for enhancing the investigation efficiency in the upcoming time.

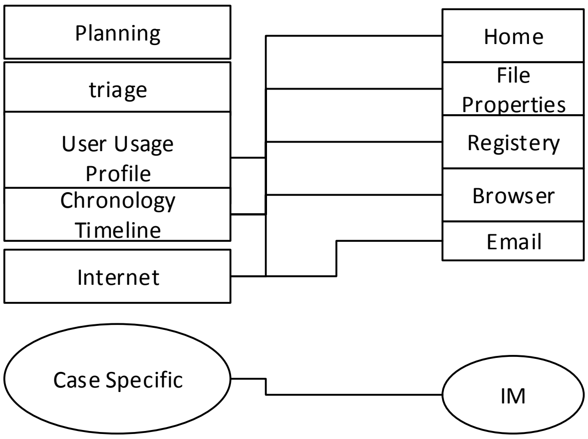

**Figure 6: CFFTPM Framework**

K.Rogers, Goldman, Mislan, Wedge, &Debrota, in 2006 introduced CFFTPM(Computer Forensic Field Triage Process Model)which is a method for providing the proof of identity, examination and clarification of digital evidence in a quick time and with no need for taking the systems/media to be examined in the lab or to acquire different forensic image.[9] The CFFTPM process is derivative from the IDIP framework [5] and the(DCSA) Digital Crime Scene Analysis basis.[18]The stages comprised in this process are planning, triage, user profiles, sequence of events, internet movements and case precise proof.

This framework is a reinforcement of physical world investigative methods that have refined into an official course framework. CFFTPM is noticeably pragmatic and balanced because it was established in reverse of many other Digital Forensic Investigation Framework, and it is not always appropriate or well-matched for all investigative circumstances. The Incident Response and Computer Forensics two notions were implemented to Common Process Model for Incident and Computer Forensics and introduced as a new process framework to investigate computer security incidents [8] and its aim is to combine the two notions to improve the whole process of examination.

The Common Process Model for Incident and Computer Forensics entails Pre- Incident Preparation, Pre-Analysis which contains all stages and events that are done before the definite analysis starts, Analysis that takes place in the Analysis Phase, and Post- Analysis Phase which is needed for writing the report documentation of the whole activities during the investigation, while the framework mainly targets analysis. Using this framework the investigators will be able to experience incident response while implementing principles known from Computer Forensics within the authentic analysis phase and it mixes the forensic analysis with the Incident Response framework.

## Discussion

Some of the discussion points touched in this paper seem like conclusions however, they are susceptible to aggressive arguments. The general principles for the acquired evidence to be compatible with the best evidence rule and legally accepted are that the evidence must be Authentic, Reliable, and Complete. A reason that strapped the notion of looking at the elements that typically cause digital evidence to be unique, then consequently needs distinct attention when used in criminal investigations. The major reason for that notion is that new encounters for forensic examination are expected to appear in the future.

The searching procedures, seizing procedures and analyzing procedures of digital evidence need to be based on methodically reliable doctrines and measures. Meanwhile that permissible standards controlling digital evidence hadn't been realized adequately and only part of the courts are able to deal with digital evidence [19].

Notwithstanding that computer and network machineries are used universally and encounter similar issues related to the acceptability of digital evidence in court. A perceptible factor is that investigators are challenged by the situation of high cost of physical storage of documents compared to low cost of digital storage of high volume of digital proofs which creates logistical situations.

Stages of handling the digital evidence necessitate all practitioners including judges, prosecutors, lawyers, and police men to have high level of expertise and trained individuals to analyze, evaluate and understand the nature of the evidence at hand. [20]

Digital evidence needs special control by experts in a way that makes it reliable and adequate because, digital evidence can easily be deleted, modified, or lost a matter makes it very essential to use effective techniques to collect evidence and process it (suitable frameworks).

For retrieving actions that could not be stored automatically to be retained in later times to investigate actions such as keystrokes and click, installation of surveillance software is always required. [19]Unless other actions are done by the suspect such as opening email or register to any service that could not be acquired without registration the identification of suspects who are using internet café to access unlawful area is not always available. Specialists consider this as a situation that leads to a coating of idea that can present mistakes [19]. Changes of courtrooms design are required because digital evidence needs special requirements and tools for its presentation such as screens [24]. To grantee effective investigation training associated with continuous new changes of technology and changes needed for procedures and tools together are important. As it is important to be up to date with new versions of hardware and software accessing old versions could be needed some times to extract evidence using original or old versions of software [23].

In 2005/2006 a study carried out in Europe underlined many capacities of sameness of digital and traditional evidence [18]. The shared likeness includes electronic documents and hard copies in paper form. More similarities between the two types of evidence are found such as between email and regular mail, e-signature and hand signatures, and e notarial deeds and regular notarial deeds [18].

The last significant point in this discussion for the purpose of distinguishing between the usages of digital evidence as a replacement of traditional evidence and as extra evidence that completes the traditional evidence (e.g. for the evidence as a replacement is the cumulative usage of e-mail as a substitute of letters. In situations where no hand written letters are directed, investigations need to distillate on electronic evidence)[20] and the presentation of digital evidence as extra evidence that completes the traditional evidence[21] (e.g. crimes that contain financial contacts or moneymaking conversation, investigations can correspondingly comprise histories set aside by financial groups in order to recognize the felon) [22][23].

## Conclusion

The course of gathering digital evidence and its acceptability by the court is the central concern of investigating and presenting digital evidence a situation that constitutes a good reason for studying and comparing investigation frameworks and always developing according to new circumstances. The fundamental rules of accepting digital evidence by the court are the same rules that govern the acceptability of traditional evidence, despite the conspicuous differences between the two groups. Digital forensics is concerned principally with legal measures, guidelines of evidence and lawful processes. The principal cause given that forensic evidence miscarries to bring in a court is not the technical quality of the evidence, but somewhat issues linking to how it was collected, who collected it, what training and experience they have, sequence of guardianship, appropriate documents, and the storage amenities used [19].

The acceptability of traditional evidence and digital evidence equally require lawfulness of proof. The lawfulness requirement enforces the need for digital evidence to be gathered, examined, conserved, and introduced in court in accordance with suitable legal measures and without disrespectfulness of the basic rights of the accused person [24][25][26].

Investigators always need to remember that evidence security is the most essential part of their job, consequently, they need to guarantee the evidence is not exposed to modification in any unlawful all through the phases it was produced, communicated or stored by lawful source [27].

Best Evidence Rule can only be contented through shielding integrity and ensuring dependability and correctness of the evidence a mission that needs technology experience, a well and advance training, in addition to resolutely binding by and following the standard of lawfulness.

**References:**

[1] Parker, D. (1983) “Fighting computer crime” New York, NY: Charles Scribner’s Sons.

[2] Carrier, B., Spafford, E. H. (2003) “Getting physical with the digital investigation process” International Journal of Digital Evidence, 2(2). Accessed July2017

[3] Casey, Eoghan (2004) “Digital Evidence and Computer Crime”, Second Edition. Elsevier.

[4] Various (2009). In Eoghan Casey Handbook of Digital Forensics and Investigation” Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 2 September 2017.

[5] Daniel J. Ryan; Gal Shpantzer "Legal Aspects of Digital Forensics” International Journal of digital evidence 3 (2) Retrieved 31 August 2017.

[6] "State v. Schroeder, 613 NW 2d 911 - Wis: Court of Appeals 2000". 2000.

[7] "US v. Bonillo" Court of Appeals, 9th Circuit. 1988. Retrieved 1 September 2016.

[8] Pollitt, MM. "Report on digital evidence" CiteSeerX: 10.1.1.80.1663.

[9] "ACPO Good Practice Guide for Computer-Based Evidence" ACPO. Retrieved 24 July

[10] 2017.

[11] "Federal Rules of Evidence #702", Retrieved 23 August 2017.

[12] Hoover, T. W. (2002). An introduction to the DoJ’s manual on searching and seizing computers (Vol. 11,No. 1). Federal public defender report. March, 2002.

[13] Verdelho, The effectiveness of international cooperation against cybercrime International Journal of Digital Evidence Winter 2004, Volume 2, Issue 3

[14] Zuckerman/McLaughlin, Introduction to Internet Architecture and Institutions International Journal of Digital Evidence Winter 2008, Volume 2, Issue 3.

[15] Pocar, F., (2004} New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, 10(1):27-37.

[16] Calderoni, F., 2010. The European legal framework on cybercrime: striving for an effective implementation. Crime, Law, and Social Change, 54(5):339-357.

[17] Report of the open-ended intergovernmental expert group on the comprehensive Study of the problem of cybercrime (E/CN.15/2011/19)).

[18] Digital Evidence & Computer Forensics, David Nardoni CISSP, EnCE

[19] Coughlin/Waid/Porter (2005), 50 Years of Progress and Technology Innovation, Tech papers/DISK the Disk Drive [ACCESSED February 2017]

[20] Zdziarski, (2008} “New Foundational Requirements for the Authentication of Digital Images”, Journal of Law & Policy 2008

[21] Abramovitch, “A brief history of hard drive control, Control Systems Magazine”, EEE, 2002, Vol. 22, Issue 3

[22] Bazin, Outline of the French Law on Digital Evidence, “Digital Evidence and Electronic Signature” Law Review (2008), No. 5

[23] U.S. Department of Justice (2009).Searching and seizing computers and obtaining electronic evidence investigations.

[24] Casey, in criminal Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2

[25] Cohen, “Digital Still Camera Forensics”, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1,

[26] Stephenson, P. (2003) “A Comprehensive Approach to Digital Incident Investigation” Elsevier Information Security Technical Report.

[27] Reith, M., Carr, C., & Gunsch, G. (2002) “An Examination of Digital Forensic Models” International Journal Digital Evidence, (1-3).

[28] Judd, R, “An Explanation of computer Forensics” Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3 [ACCESSED February 2017]