UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRONICA
A CURRENT VISION

Digital evidence focused on solid state drives (SSD): a review

Evidencia digital orientada a unidades de estado sólido (SSD): una revisión

Dony Alejandro Martínez Ramírez[1], *Rodrigo Martínez Gonzales*[2], *Gustavo Adolfo Higuera Castro*[3]

INFORMACIÓN DEL ARTICULO

Historia del articulo
Envíado: 12/12/2018
Recibido: 14/12/2018
Aceptado: 12/02/2019

Palabras clave:
Evidencia digital,
Informática forense,
Unidades de estado sólido,
Ciberseguridad

Keywords:
Digital Evidence,
Computer Forensics,
Solid State Drive,
cybersecurity

RESUMEN

El uso masivo de dispositivos electrónicos (celulares, tabletas, computadoras, laptops, entre otros) y su dependencia, han llevado a las personas a crear una necesidad de estar conectados permanentemente con estas herramientas tecnológicas; situación que en el caso de siniestros las hace útiles como material probatorio. Ante la ausencia de literatura académica, este artículo realiza una revisión sobre informática forense, recolección y manejo de evidencia digital en: Argentina, Chile Colombia y México, durante la última década. Para el efecto se usan fuentes emanadas de las bases: IEEE, y organizaciones como la Unión Internacional de telecomunicaciones (UIT), la Fiscalía General de la Nación, el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), y páginas web especializadas. Se realiza un estudio interpretativo de las fuentes relacionadas con ciberseguridad y su orientación hacia las UES y la recuperación de información física y lógica en este tipo de elementos de control.

ABSTRACT:

Nowadays, the massive electronic usage and it's dependance. (Phones, tablets, computers, laptops, among others) it has taken to people in some way the necessity to stay connected permanently on this technology tools; in sinister terms make them really useful such as evidentiary da data. In the academy literature absence, this article checks main topics clarifying from computer forensics concepts to digital evidence, recollections and digital evidence in Argentina, Chile, Colombia and Mexico. During the last decade we use IEEE data base information and organization such as International Telecommunications Union (UIT), the attorney general's office, the Ministry of information and communications (MINTIC) and specializing web sites. Making an interpretative with Cybersecurity resources and their main focus on SSD and the physical information recovery and logically in this type of controlling materials.

[1] BSc. In Telecommunications Engineering, Electronics Technology, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Repair Technician 1 in IGT. E-mail: donyalejandro1@hotmail.com.co ORCID: https://orcid.org/0000-0003-3310-7472

[2] BSc. In Telecommunications Engineering, Electronics Technology, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Sub-Director of Electronics and Reconditioning at PCSHEK. E-mail: datamanager@pcshek.com ORCID: https://orcid.org/0000-0003-3385-5649

[3] BSc. In Electronic Engineering, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Professor at Universidad Distrital Francisco José de Caldas, Colombia, Researcher of ROMA research group, Universidad Distrital Francisco José de Caldas, Colombia. E-mail: gahiguerac@correo.udistrital.edu.co ORCID: https://orcid.org/0000-0001-9691-789X

Cite this article as: D. A. Martinez-Ramirez, R. Martínez-Gonzales and G. A. Higuera-Castro, "Digital evidence focused on solid state drives (SSD): a review", Visión electrónica, vol. 2, no. 1, Special edition, january-june 2019 https://doi.org/10.14483/issn.2248-4728

1. Introduction

In 1978, when for the first time a computer crime was recognized in the state of Florida -USA-, the so-called Computer Crimes Act was created [1]. Since then, digital evidence has been the main component for investigations focused on the role of information technology as a key part of the process. However, given the constant technological change in telecommunications and its components, it is necessary to detail this evidence without losing sight of the fact that the evolutionary requirements of storage media - main containers of digital evidence [2]- are not only reflected in technology, they have also impacted the current regulations for its control. In Colombia, from the creation of Law 1266 of 2008 on which data protection is based (habeas data) to the manual of the chain of custody generated by the Attorney General's Office issued in 2018, there are clear indications of how the importance of advancing at breakneck speed in the procedures, protocols and processes for manipulating digital evidence is a race against time in order to reduce risks of information security and cybercrime [3].

In addition, when working with digital evidence, some elements or characteristics are processed and become a challenge for researchers, since the information is volatile, anonymous, duplicable, alterable and modifiable, or worse, eliminable [4]. These characteristics show the importance of the task performed by people who work with computer forensics, the importance of their organization in procedures and development of investigations. Considering the raw material's fragility and users' requirements, and given the continuous technological evolution, the need to reduce the size and weight of the devices has demanded greater effectiveness and efficiency; this has led to the generation of data storage in solid state drives or also called SSD[4] (Solid State Drive), [5], [6].

However, when it comes to information retrieval in SSDs, the likelihood of success is lower due to its design, as the process entails many limitations in the information retrieval process such as: knowledge of a conditioned number of read-write possibilities, which makes the units write the new information in separate blocks without taking into account the controller thus making it to be used the same number of times avoiding the obsolescence of blocks at different times; the increase up to 25% of the capacity stipulated in the device, additional space that is not easily accessible by the operating system or daily use tools; appearance of algorithms to identify memory blocks that are part of the deleted information, increasing the efficiency of the writing process making that once erased is almost impossible to recover. As can be observed, solid state drives (SSDs) are a challenge in today's computer forensics, because in addition to the use of rigorous methodologies to detect, identify, collect and safeguard the evidentiary material found, it could lose its evidentiary value and allow the impugnation of processes before judicial authorities, [8].

The paper is structured as follows: section one outlines the research methodology that illustrates how the review is carried out; then, based on forensic computing concepts (based on the classification generated by ITU worldwide), subcategorization into three branches is established: Chain of Custody, Cybersecurity, and SSD Units, and an outline of the information retrieval and acquisition processes in these units; it culminates with conclusions referring to forensic processes in SSD devices, [9].

2. Methodology

Since the legal norms that oversee the correct way to conduct an expert appraisal must provide the necessary tools so that the protocols of care, custody, capture, storage and kidnapping, among others, are those required to avoid invalidating the evidence and thereby losing important evidentiary material, the review requires generating information categories and subcategories according to the index method [10].

The foregoing led to the identification of three major branches: Chain of Custody, Cybersecurity and SSD Units. The Chain of Custody describes the processes necessary to fully comply with its requirements. From Cybersecurity, the way in which the ITU has classified the countries at world level, focusing on the compliance that these present to the international security standard allowing to generate analysis and recommendations to increase the cyber protection quality. The last subcategory - SSD units - shows the evolution and how its architecture presents advantages for some

[4] Are solid state units constructed by crystalline semiconductors in which the current is stored in solid components and additional compounds that allow the switching and amplification of the current. Among the solid state components are: transistors, microprocessors and RAM memory chips, leaving out of this list electromechanical devices such as relays, switches, hard disks, [7].

applications. Consequently, the documentary research, endorsed by the ROMA group, led to a review of the bases: IEEE, and organizations such as: ITU, Attorney General's Office, MINTIC, among others. The keywords used were: SSD, Computer Forensics, Chain of Custody, Flash Memories. FTL. The categorization is shown in Figure 1.

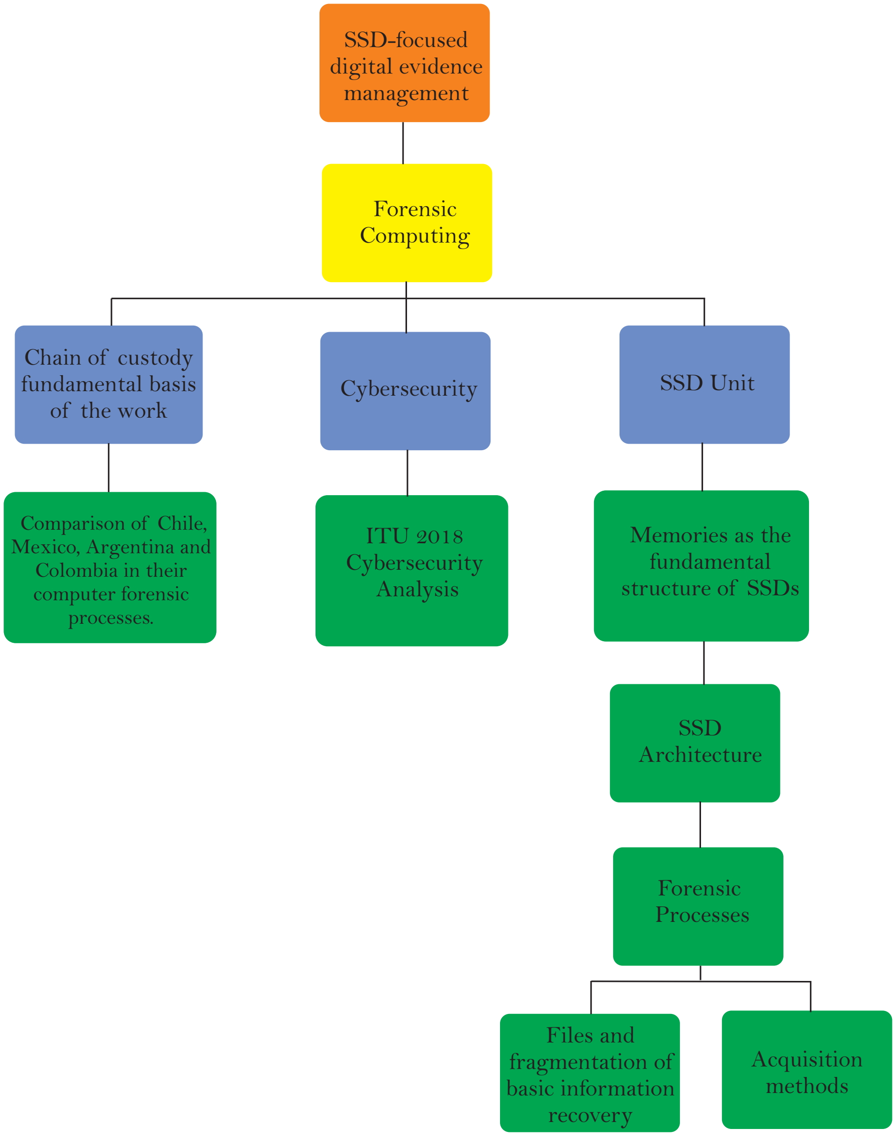
SSD-focused digital evidence management
Forensic Computing
Chain of custody fundamental basis of the work
Cybersecurity
SSD Unit
Comparison of Chile, Mexico, Argentina and Colombia in their computer forensic processes.
ITU 2018 Cybersecurity Analysis
Memories as the fundamental structure of SSDs
SSD Architecture
Forensic Processes
Files and fragmentation of basic information recovery
Acquisition methods

Figure 1. Research model sub-categorization for the developed state of the art. Source: own.

2. Computer forensics.

Computer forensics requires clarification of some concepts that can be observed in Table 1.

CONCEPT	DEFINITION
Computer Forensics	It is a science that arises from the need to acquire, obtain and present data processed electronically and stored in a digital medium. Due to technology, it emerges as an auxiliary discipline of modern justice [11].
Research Information	Incriminating evidence can be used for various crimes such as: fraud characterized by concealment, deceit or breach of trust seeking to obtain property; money or services, child abuse and pornography, network intrusion, homicide, dom estic violence, e -mail threats, harassment and stalking, narcotics, software piracy, identity theft, among others [12].

Digital Research Elements	The most common digital elements in a digital investigation are: conversation log, digital camera software, e -mails, databases, internet activity logs, executable programs, source codes, victim/suspect photos, phone logs, bank records, credit card numbers, victim location maps, victim background checks, cloning software, electronic signatures, [13].
Digital Evidence	Evidence constructed, stored or transmitted by magnetic fields, which can be reported, stored and performed with specific technical tools, i.e. protocols, software and hardware, [14].
Computer Forensic Tools	They arise because of the am ount of files stored, the variety of formats and the need to collect data in an accurate manner. The best known tools are: CAINE, X-Ways Forensics, Autopsy, Cryptcat, Netcat, Air, Foremost, Autopsy, Py -Flag, among others [15].
Cybersecurity	It is the pr otection of information files with a set of tools that allow to safeguard it. This is done through a process of prevention, detection and reaction or response, which must contain an element of learning that allows a continuous improvement of the process. Protecting software, hardware, infrastructure and services, [16].

Table 1. Computer forensics concepts. Source: own.

3. Chain of Custody

The Chain of Custody is directly related to the evidentiary material authenticity, and appears to guarantee the origin and reliability of the evidences obtained, safeguarding the element demonstrative capacity and allowing to give it a veracity value, [17].

Evidentiary material elements and physical evidence (EMP and EF, respectively) are presented, such as the objects, instruments or means of knowledge that will lead to the construction of the truth and the identification of the culprit or culprits of punishable crimes, as well as the reconstruction of the facts, [18].
On the other hand, Article 275 of Law 906 of 2004 on Criminal Procedure classifies the EMP and EF in 6 subdivisions which would contain everything related to fingerprints, traces, stains, residues, vestiges, weapons, instruments, objects, money, goods, material elements obtained through recording, filming, photography or video, material elements discovered, collected and insured during the process [19].

To validate the chain of custody system, certain aspects or unavoidable stages must be taken into account during discovery, collection, packaging, transportation, and storage analysis in order to maintain its authenticity and evidentiary quality.

First of all, there is Authenticity, which belongs to the objective correspondence of EMPs and EFs. Then there is the Demonstrative Capacity, which after carrying out a scientific or technical analysis gives evidential importance, although in some cases it loses its validity due to time restrictions, in the case of biological tests or for analyses that do not produce the same results. Subsequently, the Identity, which corresponds to a detailed description, complete and with all the characteristics of registry necessary for its individualization. Integrity then appears, ensuring that the EMPs and FEs do not show variations from the test finding time. The last 5 elements of the EMP and FE are: Preservation, guarantees that the tests are kept in adequate conditions; Security, which consists in diminishing the possibility of loss or damage of the evidentiary elements; Storage, which allows giving a correct test disposition; Continuity, which gives in a chronological way a traceability to the tests, and finally there is the Registry, by means of which the documentation of the EMPs and FE that intervened in the chain of custody, [18].

Figure 2 shows a description of the material evidence and physical evidence.

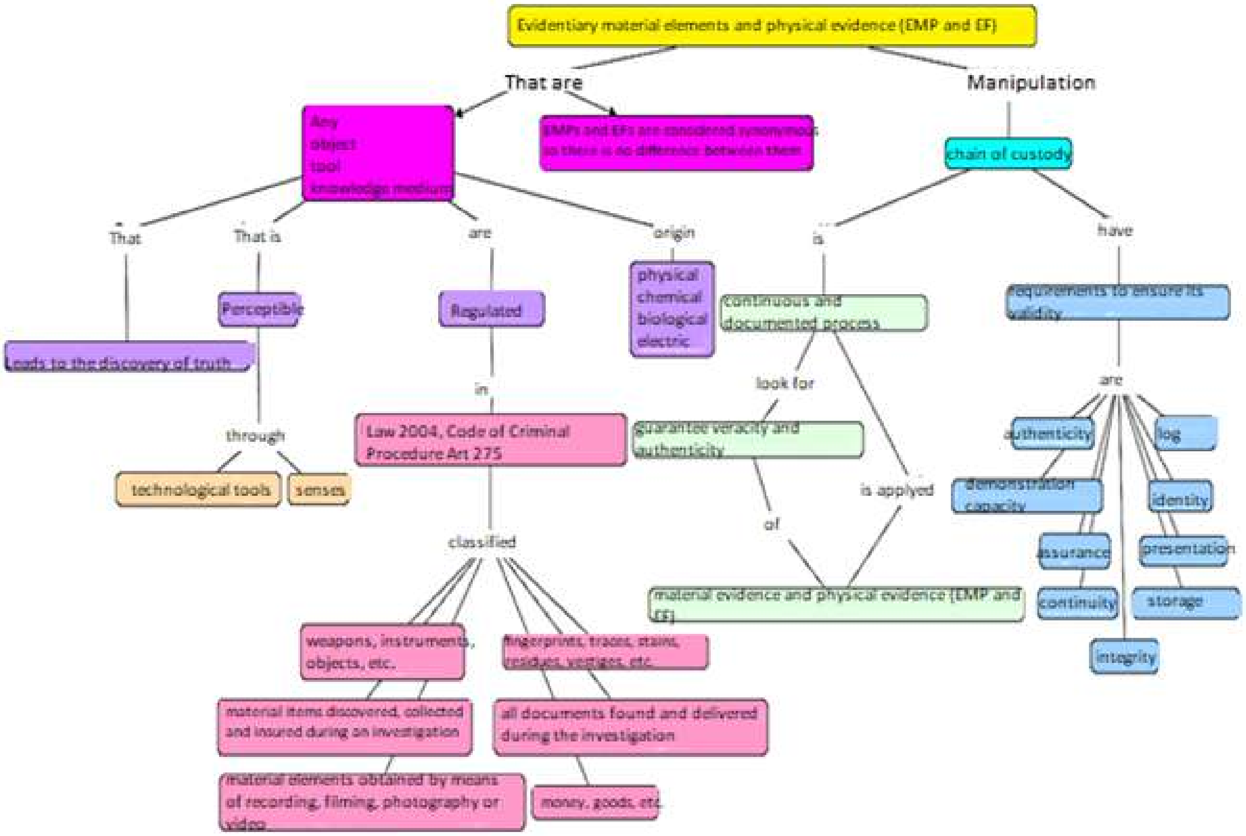
Evidentiary material elements and physical evidence (EMP and EF)
That are
Manipulation
Any
object
tool
knowledge medium
EMPs and EFs are considered synonymous
so there is no difference between them
chain of custody
That
That is
are
origin
is
have
Perceptible
Regulated
physical
chemical
biological
electric
continuous and documented process
requirements to ensure its validity
Leads to the discovery of truth
in
look for
are
through
Law 2004, Code of Criminal Procedure Art 275
guarantee veracity and authenticity
authenticity
log
technological tools
senses
is applyed
demonstration capacity
identity
of
classified
assurance
presentation
material evidence and physical evidence (EMP and EF)
continuity
storage
weapons, instruments, objects, etc.
fingerprints, traces, stains, residues, vestiges, etc.
integrity
material items discovered, collected and insured during an investigation
all documents found and delivered during the investigation
material elements obtained by means of recording, filming, photography or video
money, goods, etc.

Figure 2. Description of evidentiary materials and physical evidence. Source: own.

On the other hand, the Chain of Custody has as its main objective the guarantee for the judge, who must trust these elements and consider them authentic, from the criminalistics point of view, since it requires that the chain of custody guarantees that the evidence collected at the scene is the same as the one being presented to him. There must be a guarantee from detection, identification, fixation, collection, protection, safekeeping, packing, transfer from the real or virtual place, to presentation as evidentiary material, [14].

In order to guarantee the evidence or the evidentiary material granted in a trial, it is important to treat it correctly, from the moment it is collected until it is delivered for evaluation by the agencies in charge of imparting justice; therefore, it is necessary to establish a rigorous and detailed register, [21], with the characteristics described in Figure 3.

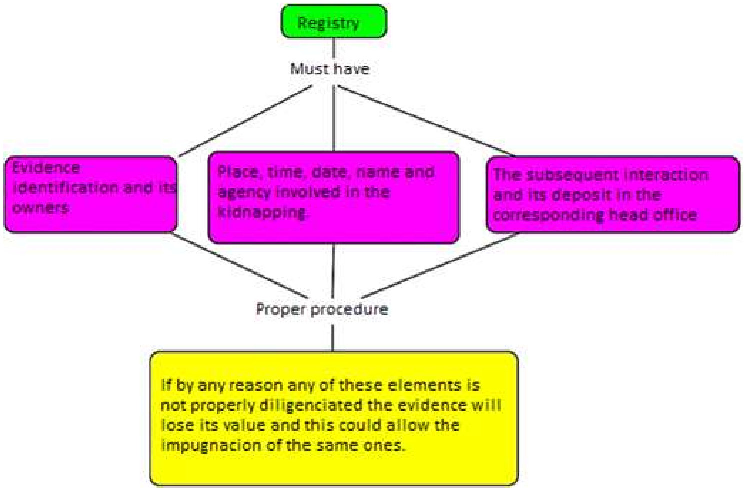
Registry
Must have
Evidence identification and its owners
Place, time, date, name and agency involved in the kidnapping
The subsequent interaction and its deposit in the corresponding head office
Proper procedure
If by any reason any of these elements is not properly diligenciated the evidence will lose its value and this could allow the impugnacion of the same ones.

Figure 3. Probative record in a trial. Source: own.

It should also be taken into account that digital evidence can be presented in different states [20], as explained in Figure 4.

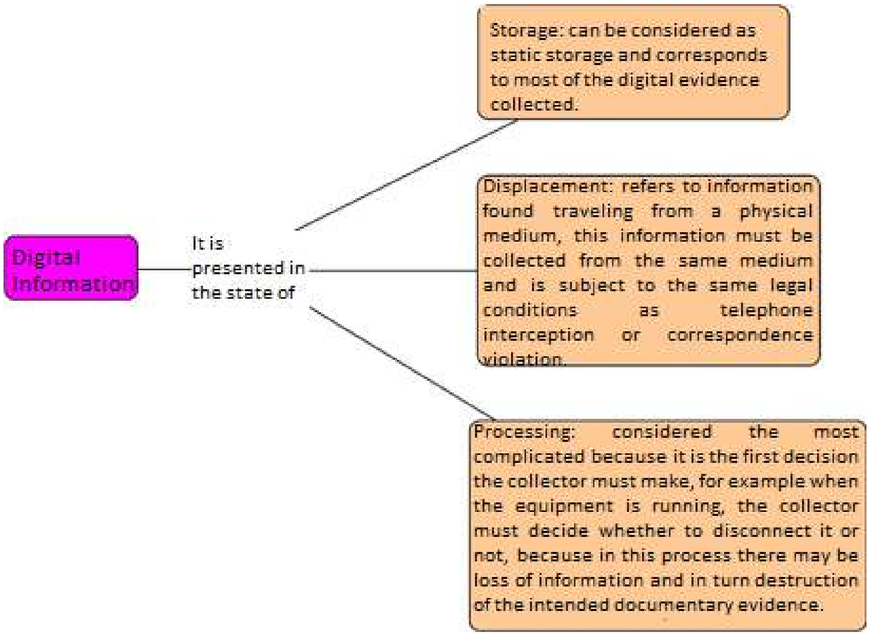
Digital Information
It is presented in the state of
Storage: can be considered as static storage and corresponds to most of the digital evidence collected.
Displacement: refers to information found traveling from a physical medium, this information must be collected from the same medium and is subject to the same legal conditions as telephone interception or correspondence violation.
Processing: considered the most complicated because it is the first decision the collector must make, for example when the equipment is running, the collector must decide whether to disconnect it or not, because in this process there may be loss of information and in turn destruction of the intended documentary evidence.

Figure 4. Digital evidence states. Source: own.

From the foregoing, it can be deduced that one advantage of digital evidence is that for the information gathering a bit by bit copy is almost like having an original, in many cases it is not possible to leave companies out of service and simply remove a piece of equipment; therefore, a copy will be made, which will allow them to continue in operation, [22].

The chain of custody in computer forensics must guarantee that the evidence offered complies with the existing procedural requirements:

Define responsibilities in terms of handling, from the moment of location, through collection up to final disposal.

Include physical elements of all the teams involved.

Perform a description and modeling of the accessed and safeguarded information.

It also must offer reliability, i.e. refer to everything to do with the integrity, authenticity and confidentiality of the information. In this regard, the importance of protecting the information's privacy should also be mentioned; privacy requires reliability and constitutional procedural norms. The condition of illegality could be given by a failure in any of the process steps, [23].

In short, it is essential to have a protocol for the chain of custody in computer forensics. The validity of computer evidence will be directly proportional to the maintenance of security, seeking a strict safeguard and a methodological step structure that allows a correct procedure in the chain of custody, [24]. Failure to comply with these procedures may result in the nullity of the evidence -as occurred in the case of Raúl Reyes' computer in 2011, where this information was not accepted, for not complying with the chain of custody and taking evidence from a cross-border device without the approval of the country's authorities [25]-. These steps are shown in Figure 5:

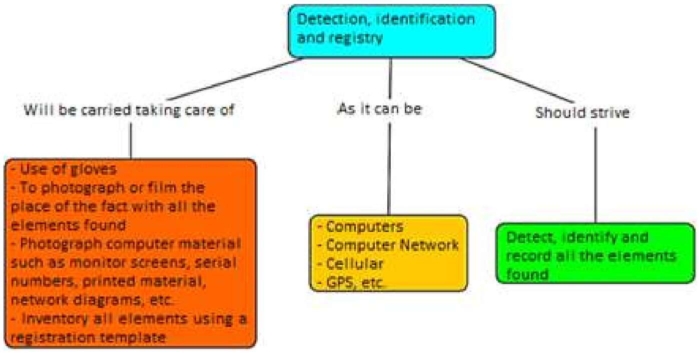
Detection, identification and registry
Will be carried taking care of
As it can be
Should strive
- Use of gloves
- To photograph or film the place of the fact with all the elements found
- Photograph computer material such as monitor screens, serial numbers, printed material, network diagrams, etc.
- Inventory all elements using a registration template
- Computers
- Computer Network
- Cellular
- GPS, etc.
Detect, identify and record all the elements found

Figure 5. Identification and registration detection. Source: own.

Figure 6 shows a possible logical order of the examination and data collection procedure, which is carried out after having identified the possible sources of information, [26].

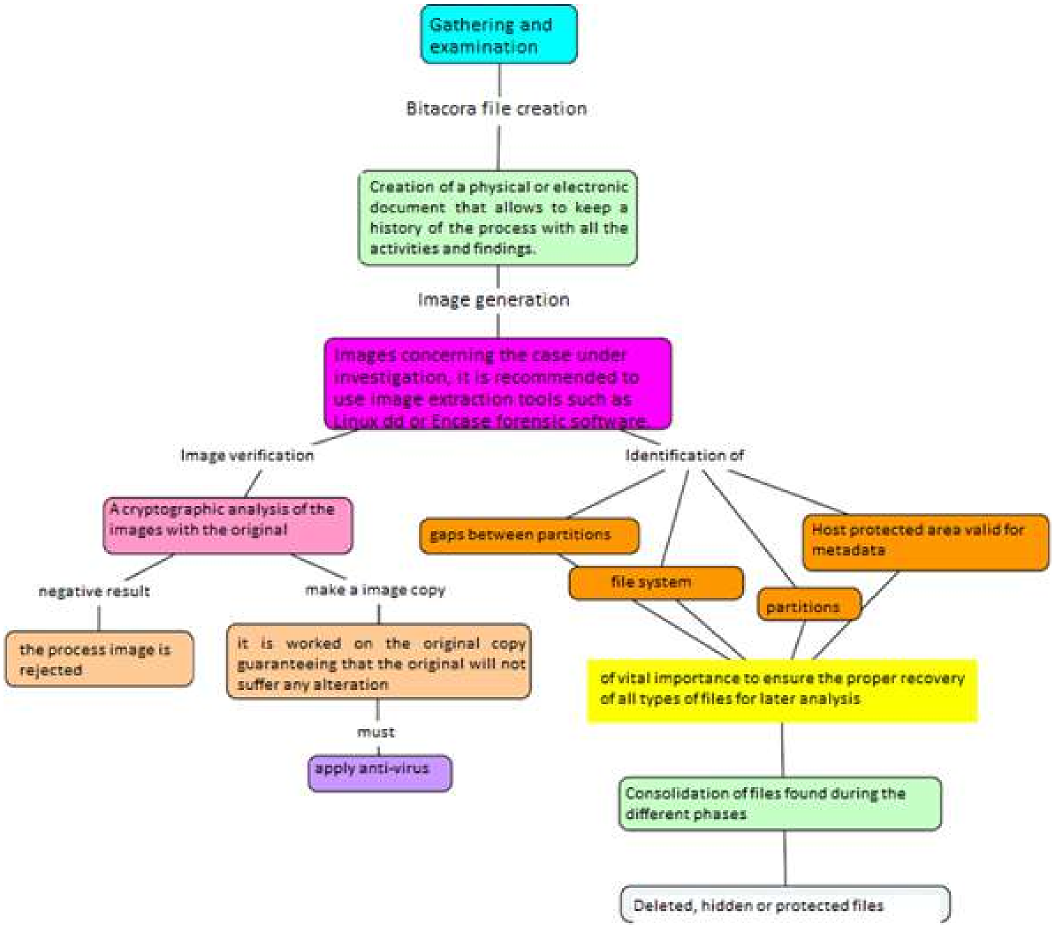
Gathering and examination
Bitacora file creation
Creation of a physical or electronic document that allows to keep a history of the process with all the activities and findings.
Image generation
Images concerning the case under investigation, it is recommended to use image extraction tools such as Linux dd or Encase forensic software.
Image verification
Identification of
A cryptographic analysis of the images with the original
gaps between partitions
Host protected area valid for metadata
file system
partitions
negative result
make a image copy
the process image is rejected
it is worked on the original copy guaranteeing that the original will not suffer any alteration
of vital importance to ensure the proper recovery of all types of files for later analysis
must
apply anti-virus
Consolidation of files found during the different phases
Deleted, hidden or protected files

Figure 6. Examination procedure and data collection. Source: own

3.1 Comparison between Chile, Mexico, Argentina and Colombia in their computer forensic processes

The presented revision is consolidated as a state of the art of forensic computing in some countries that, due to their culture, language, traditions, among others, can be a reference point for the evolution in the expert and legislative branch. In this way, it provides guidelines in favor of turning these tools into allies to combat crime. Table 2 shows the comparison of forensic investigation in Argentina, Chile, Colombia and Mexico.

EVALUATION ITEM	COUNTRY	DEFINITION
Experts	Argentina	Experts in Argentina must possess a title that guarantees them as such and can only refuse to carry out their work if they present any legal impediment. In addition, it is recommended that official entities and the parties carry out the expertise in order to prevent one of them from taking advantage by accessing data without the consent or knowledge of the other party, thereby leading to nullity, [27].
	Chile	Chile has a department that specializes in investigating cybercrime. The experts who carry out the work are part of the CHean Carabineros or Investigative Police (PDI); the process is carried out by order of the prosecutor's office, instructing which of the two entities will take the case [28].

	Colombia	Colombia's criminal procedure law does not take into account the specific profile of the forensic expert and his or her training. There are shortcomings in the terminology used, causing problems between the technical and judicial parts, affecting the information [29].
	Mexico	Mexican experts are required to have a professional identity card and those who are part of the official services must prove that they have completed their studies [30].
Chain of Custody	**Argentina**	The evidence for the law has to be protected from the scene of the fact, being responsible a suitable person who will assume as (Digital Evidence First Responder, DEFR). To demonstrate integrity, continuity, legitimacy, each process and movement must be carried out in physical documents (paper) to the elements that are part of the evidence, [31].
	Chile	The chain of custody is stipulated in the criminal procedural code, and its development involves government agencies, the Chilean Investigation Police, Chilean Carabineros, Chilean Gendarmería, Legal Medical Service, Public Prosecutor's Office and the Ministry of Health. There is a two-part form for recording evidence, the form label and chain of custody data [32].
	Colombia	In 2016, the prosecutor's office generates the document that determines the procedure on the evidentiary material, becoming the guide for the chain of custody. Despite this, some laboratories have not completed the migration of their processes and are currently based on ISO 27.037, [33].
	Mexico	An official document establishes the requirements for preserving integrit y, reliability and legitimacy, requiring the personnel in charge to demonstrate the changes made to the evidentiary material, without prejudice to the information contained in the device [34].
	Argentina	The evidence must begathered using a digital imaging method or device seizure; images must be made using a HASH function to ensure data integrity; in the case of a seizure procedure, the evidence must be packaged and protected with all chain of custody regulations [31].
	Chile	The gathering procedure is carried out through the seizure of evidence, including the chain of custody process, specifying the characteristics of the device, to carry out the expertise under ISO 27.037, [32].
	Colombia	Article 235 of the Code of Criminal Procedure guarantees the interception of communications; Article 236 allows for the seizure of evidence containing information on a presumed crime; as for the information contained in the cloud, there is no specific legislation making it difficultto obtain the evidence [33].
Evidence gathering	**Mexico**	The gathering of evidence is in the midst of a transition from a prosecutorial system to a prosecutorial system, determined by the state of the expert, thus changing the gathering procedure, [34].
Standard	**Argentina**	The Specialized Cybercrime Fiscal Unit (UFECI) makes its own standard based on the compilation of international standards, but the laboratories have not yet migrated to this protocol and continue to have no clarity on the standard to use,[35].
	Chile	There is no specific standard defined in Chilean law, so they use the ISO 27.037 standard, training cybercrime specialists and, as an additional method, use personnel from outside judicial institutions [30].
	Colombia	ISO 27.037 inEnglish is the protocol currently used to perform expertise, since in the chain of custody documentation does not define a standard as a procedural basis, in addition to this the failure to define the professional profile of the expert entails serious flaws, [33].
	Mexico	The first condition of the Mexican forensic process is represented in the Constitution, which defines the inviolability of communications (Article 16), the National Code of Criminal Procedure establishes the principles of the forensic informatics process, defines the educational level and characteristics that forensic experts must possess, [36].

Table 2. Comparative forensic investigation in Argentina, Chile, Colombia and Mexico. Source: own.

4. Cybersecurity

ITU's global survey in 2017 published the Global Cyber Security Index, which measures the commitment level of more than 193 ITU member countries. Colombia was then the 46th country globally and ranked 6th in the Americas after United States, Canada, Mexico, Uruguay and Brazil, [37], Table 3.

AMERICAS Zone		
Country	**Score**	**GlobalRanking**
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	61
Argentina	0.482	62
Ecuador	0.466	65
Peru	0.374	78
Venezuela	0.372	79

Table 3. Colombia's position regarding the global cybersecurity commitment of ITU Member States publication 2017. Score by region. Source: Global Cybersecurity Index 2017.

4.1 Cybersecurity Analysis ITU 2018

Taking the European context as a reference, the commitment is greater in terms of legal and technical areas. However, the situation in the African and American regions requires continued commitment and support.

The ITU published a heat map that allows observing the national and international cybersecurity commitments of the 193 member countries, where the defined eta commitment level from green (highest) to red (lowest), [37].

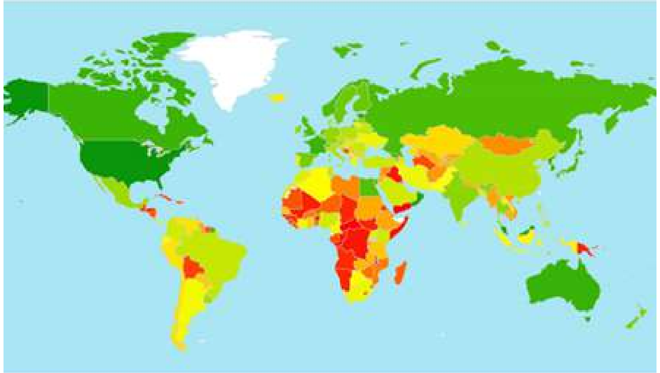

Figure 8. World heat map cybersecurity year 2017. Source: Global Cybersecurity Index 2017.

Colombia appears in a special statement for its contribution to cybercrime legislation, [37], thanks to Law 1273 of 2009, which modified the criminal code, [38].

However, a more recent version of ITU (2018) found that Colombia no longer ranks 46th globally in terms of cybersecurity, it is now 73rd and 7th in Americas zone, after United States, Canada, Uruguay, Mexico, Paraguay and Brazil, [39], Table 4.

AMERICAS Zone			
Country	Score	Regional Ranking	Ranking Global
United States of America	0,926	1	2
Canada	0,892	2	9
Uruguay	0,681	3	51
Mexico	0,629	4	63
Paraguay	0,603	5	66
Bra zil	0,577	6	70
Colombia	0,565	7	73
Cuba	0,481	8	81
Chile	0,470	9	83
Dominican Republic	0,430	10	92
Jamaica	0,407	11	94
Argentina	0,407	11	94

Table 4. Colombia's position regarding the global cybersecurity commitment of ITU Member States publication 2018. Score by region. Source: Global Cybersecurity Index 2018.

5. SSD Units

SSDs can be defined as storage units, composed of electronic components such as floating gate transistors, non-volatile memory base, preventing them from being energized to maintain stored information [40].

History indicates that the torid memories or magnetic core memories designed in the 50s, which were part of the computers until the 70s, were simple to operate; a node matrix was generated which was crossed by two threads, an X and a Y, that when energized allowed a data or bit to be stored in the toroid; in order to be able to read the information a third thread was required, a Z, which returned the data stored in this toroid, with possible values of a logical one or zero. At the same time, IBM was developing a type of non-volatile memory called CCROS by its acronym (Charged Capacitor Read Only Store) [41]. Another type of memory that contributed to the evolution of the SSD units was the bubble memory, based on a film of magnetic material, which had magnetization areas where each one of the bits was stored; to access these, the bubbles moved by action of a magnetic field to the reading zone [42].

5.1 Memories as the fundamental structure of SSDs

SSDs were initially generated with Dynamic Random Access Memory (DRAM). This type of technology presents a high speed in its writing process due to the fact that it does not need to be erased previously as it happens in flash memories [43]. Another advantage is to eliminate the wear in the silicon elements due to the writing process evidenced in the transistor gate of the flash units, which decreases its useful life. However, they had disadvantages: higher production cost, requirement of a backup power source for being a volatile memory. Designers usually included a backup battery. But the convenience of flash memory has outweighed the benefits of DRAMs. As a result, most SSDs are composed of NAND architecture memories [44]. These are constructed with floating gate transistors that are generated by two gates insulated from each other by an oxide layer, which passes through the control gate; in this way the floating gate is loaded and due to an insulation layer allows this load to be maintained for many years. To erase the information is connected to ground thereby achieving that electrons are repelled and remain without them the floating gate. In order to read the information, a high voltage is applied to the control gate and if the floating gate maintains its charge, this implies that it was charged and had a certain value or bit, but this practice caused the components and the physical structure to be over-exploited, resulting in a limited life time for the units, [34].

The NAND SLC units (Single-Level-Cell) allow only one level of cell or bit, [46] the NAND MLC units (Multi-Level-Cell) allow two levels or 2 bits of data [47] and finally there are the NAND TLC (Triple-Level Cell), [48].

5.1.1 SSD Architecture

Just as other storage devices require a control system and a data storage unit, it is necessary to be more specific in describing each of their main parts and the functions performed by each one.

Controller: is the unit processor, performing very specific functions in administration, management and intercommunication of flash memories with possible input output interfaces, additional to it executes a software at firmware level, and is highly responsible for the speeds reached, in storage, by its management, other tasks performed are Error Correction, [49].

- Bad or assignment block.
- Read and write, Cached information.
- Trash gathering.
- Encryption.

Cache: similar to the HDD units the SSD units also have a small cache with the difference of being of DRAM technology, [50].

Capacitor: high performance capacitor that simulates a battery for a short period of time becoming a sufficient power source to maintain the data integrity in case of an accident due to abrupt power cuts, [51].

Memory slots: are NAND or NOR technology chips connected to each other in charge of storing data, [52].

Host interface: possessing data and a high speed is something interesting, but if you do not have an effective way to access this data would not be more useful. It is for this reason that the controller includes in its tasks to have assigned a way to deliver this data to the computer and this is how it includes a communication interface that fits the standards, [49].

- Serial ATA (SATA).
- Serial Attached SCSI.
- PCI Express.
- USB.

Every device that precedes a technology presents evolution on its predecessor. Table 5 illustrates the pros and cons of SSDs.

5.1.1.1 Forensic Processes

Residual data because of subsequent writing

The flash drives allow to carry out recovery of residual data, this information is left involuntarily and can be present at any level of the system, has the characteristic of being able to be recovered in any medium, as a cause of the procedure of protection of sectors that have the SSD, when a file is deleted, this is marked as a dirty page, staying in this place until the device requires space and the new information is not written in this location, on the contrary it is written in a free zone, this because of the files Flash Translation Layer FTL [55], additional to recovery, it is possible to recreate versions of files still existing in the media or it is allowed to investigate the version originality.

SSD pros	SSD cons
Higher reading speed [53]	High cost per storage Gigabyte
Low read/write latency	Average life time less than HDD units per number of possible write cycles
Opening and start-up of applications in less time [53]	
Reduced energy consumption and absence of mechanical components	
No noise due to the absence of mechanical components [54]	
Immunity to the magnetic disks fragmentation	
Less weight compared to HDD	
High resistance to drops, shocks and vibrations [54].	
Increased security in the deletion process	
Fast stored data cleaning	

Table 5. Comparative pros and cons of SSD units. Source: own

5.1.1.1.1 Files and fragmentation of basic information recovery

The following table shows the main files involved in the residual processes in the SSD, [56], Table 6.

FILE	DESCRIP TION
FLASH TRANSLATIO N LAYER (FTL)	FTL It is a host system, like a block device that uses a FAT system; the host system will try to rewrite the files in the same block because it is based on the logical level. Since this is only a change in the FAT file, the FTL will write the data on the first page clean and mark the previous data as obsolete by altering the input data block allocation maps, the page will not be deleted until it is required, because the device is full and it is necessary to delete dirty pages. TrueFFS has a feature called FAT filter that supervises FAT, to see the clusters that have been released marking the pages that are obsolete, allowing the associated blocks to be available for collection as garbage and thus increasing the residence time of the residual data, [34]
Yet Another Flash File System (YAFFS)	YAFFS is a file in charge of managing the dirty pages to carry out erasure and overwriting of information, coming from discarded pages, allowing to have residual information relative to the use of the device [57]
Journaling Flash File System JFFS	JFFS enters into function when a page is marked as obsolete by an update, allowing not to be marked as completely obsolete when a high structure of the same is maintained, giving way to the retrieval of information as it keeps the page active [58].
Journaling Flash File System 2 JFFS2	JFFS2 divides the page lists into three: 1 clean list, 2 dirty lists and 3 free lists, when a new block is needed to write data, 99 times out of 100 the garbage gathering process will choose a block from the dirty list to erase and the rest will select a block from the cleaning list [59].

Table 6. Files involved in the emulation of SSD units. Source: own.

File that increases the SSD efficiency

IBSF: software module method applied to the flash translation layer, in charge of delaying the writing requests, minimizing the unit over-writing processes, its process is based on a verification of the redundant indexes, by means of the buffer memory, generated by a data field that indicates the modified file location, which will be stored every time there is a request, this is carried out in a memory area with the characteristic of being volatile, remaining in this place, until the request for final saving is generated, sending the information to the flash memory sectors at this time, the advantages of this procedure can be clearly seen in the increase in useful life of the flash memories but in return it can be seen that in case of unexpected loss of energy can cause the loss of data, [45].

Fragmentation Effects on Data Recovery

After the process of filling a Flash device for the first time, the way in which Flash or FTL file systems decide to write new data is no longer based on location, at this time depends on variables such as the number of dirty pages in a block and will no longer be placed spatially, thus allowing a fragmentation, generating two possible impacts [60].

The first visible impact is that larger files are more difficult to recover the more the device is used, which is why the probability of recovering data will be greater in files that are one page or less than 512 bytes, since it is difficult to create files with multiple fragmentation points, delimiting the recovery capacity to small text files and low resolution images [60].

The second flaw will be seen at the time of formatting, since this process may look like a new unit, but it will actually leave fragments and possible blocks that have not been removed as garbage, resulting in a possible fragmentation from the beginning.

5.1.1.1.2 Acquisition methods

Due to their characteristics, SSD drives have a low probability of information recovery with respect to HDD drives. However, specialized software and hardware have been developed that perform their work efficiently in physical acquisition and logical acquisition of information, which is why we will analyze a division of these two methods in Table 7.

METHOD	CHARACTERISTICS
PHYSICAL ACQUISITION	Physical acquisition is understood as the process carried out directly on the electronic components, in which each one of the memory chips is extracted or manipulated and a backup is made. The method to use will be the JTAG (Joint Test Action Group) as physical method to produce an image of a flash memory, having as purpose to obtain a copy with a minimum of changes in the data, since when loading the software it must initiate the unit and in such case by its characteristics, this must be turned on and at the moment of turning on the device is subject to possible changes in the information. The complex process of the JTAG method is to achieve the identification of each one of the pads, due to the fact that manufacturers sometimes do not identify them or on the contrary do not possess them; they require a direct connection on another component, so sometimes a specific algorithm is needed for the identification of the pads, despite these limitations it has the advantage of generating the most reliable copies and with minimum alteration of the information. Another method is the use of a flasher tool, this is a specific tool designed and used by the manufacturers to make updates, but in contrast they are not generic, reason why it is not possible to make a flash tool for all the models of unit, additional to it requires a preparation onthe part of the user, since an error in its manipulation can cause damages in the integrity of the information. A third method proposed to make a physical acquisition is to make use of a chip programmer, a process that involves removing the memory from the PCB and placing it in a reader in order to access the information stored on the chip. Once this procedure is done, the logical layer is reconstructed, something that is even more complex, there is no information about the controller with ease, this fault has been resolved with some controller simulators, which allow the information to emulate in a very clear way the operation of the controller and thus be able to reconstruct the data that needs to be analyzed.[60]

METHOD	CHARACTERISTICS
LOGICAL ACQUISITION	It is based on low-level data acquisition, with minimal changes in the information without relying on the multiple existing ports and non-standard cables used by manufacturers, using both licensed and open source software, this bearing in mind that the validity of a test is affected when using open source tools, as existing standards do not provide for the veracity and integrity offered by free software [60].

Table 7. Data acquisition methods in SSD units. Source: own.

6. Conclusions

It is evident how the effort and work made by governments and their institutions to achieve a procedure according to the legislation needs in the scientific framework of forensic informatics do not comply with all the requirements, leaving gaps that allow the information collected in a forensic process to lose validity, eliminating the support of important cases and allowing for technical concepts the communication between experts and lawyers is not adequate, which is why it requires preparation of those involved in the processes and clearly define the concept to be used as evidence..

ICTs in their continuous evolution should not be limited by a nation's resources. The constant change in the digital world and the need to be prepared for cybercrime and cybersecurity requires valuable global partnerships such as ITU to ensure strategic alliances that allow member countries to organize a protected digital environment for all.

The ITU's analysis of cybersecurity procedures is constant, as in the 2017 report, Colombia was given special recognition for the creation of chain of custody protocols by MINTIC, placing it in 46th place, but with constant improvements in the countries registered, In the 2018 report, Colombia dropped vertiginously to 73rd place, showing how it is necessary to be at the forefront of security, not only by a position in reports worldwide, but driven by crime and the way in which criminals evolve their criminal processes, since they are overcoming the laws and protocols imposed by countries to control the risks of information.

It could be seen how the amount of files and control hardware components involved in the data storage of solid state drives, generate a complication in the data retrieval in a forensic process, if these are not found as residual data and have not been sent by the controller as a dirty page, produce that the data gathering is almost null.

It will be open the possibility of carrying out laboratories that allow demonstrating the difficulty of extracting the information in SSD units and also generate processes or methods for the gathering of digital information, based on the possibility offered by the control unit files and the characteristics of each one of them.

References

[1] D. Jaramillo, M. Torres, "Estado del Análisis Forense Digital en Colombia", Trabajo de Grado, Facultad de Relaciones Internacionales Estrategia y Seguridad, Universidad Militar Nueva Granada, Bogotá, Colombia, 2016

[2] A. Jansen, "Digital Records Forensics: Ensuring Authenticity and Trustworthiness of Evidence Over Time", 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2010 https://doi.org/10.1109/SADFE.2010.20

[3] Congreso de la Republica, Ley estatutaria 1266 de 2008. http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

[4] Z. Tiaan, M. Li, M. Qiu, Y. Sun, S. Su, "A secure digital evidence framework using blockchain," *ELSEVIER information sciences* vol. 491, pp. 151-165, July 2019. https://doi.org/10.1016/j.ins.2019.04.011

[5] Quang Do, B. Martini, Kim-Kwang R. Choo, "A Cloud-Focused Mobile Forensics Methodology", *IEEE Cloud Computing*, vol. 2, pp. 60 – 65, July-Aug. 2015 https://doi.org/10.1109/MCC.2015.71

[6] L. Caviglione, S. Wendzel, W. Mazurczyk, "The

•Future of Digital Forensics: Challenges and the Road Ahead”, *IEEE Security & Privacy*, vol. 15, app. 12 – 17, November 2017 https://doi.org/10.1109/MSP.2017.4251117

[7] J. Rook, S. Medhat, “All change at IBM”, *Computing & Control Engineering Journal*, vol. 7, pp 80 -85, April 1996. https://doi.org/10.1049/cce:19960204

[8] H. S. Lee, S. Park, D. Lee “RMSS: An Efficient Recovery Management Scheme on NAND Flash Memory based Solid State Disk” *IEEE Transactions on Consumer Electronics*, vol. 59, pp. 107-112, march 2013. https://doi.org/10.1109/TCE.2013.6490248

[9] P. D. Dixon, “An overview of computer forensics”, *IEEE Potentials*, vol. 24, pp. 7 – 10, December 2005.https://doi.org/10.1109/MP.2005.1594001

[10] R. H. Sampieri, C. F. Collado P. B. Lucio “Metodología de la investigación”, 4ta. Ed, Mexico, McGraw-Hill, 2006.

[11] D. Rico Bautista y J. Rueda. (11-05-2016) La informática forense en dispositivos Android. [En línea] Disponible-en:https://www.researchgate.net/publication/316427536_La_informatica_forense_en_dispositivos_Android

[12] C. R. García. Cadena de custodia digital de las evidencias para la realización de un peritaje. 2014. http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

[13] A. Yasinsac, R. F. Erbacher, D. G. Marks, M.M. Pollitt, P.M. Sommer, “Computer forensics education”, *IEEE Security & Privacy*, vol. 1, pp. 15-23, July-Aug. 2003 https://doi.org/10.1109/MSECP.2003.1219052

[14] M Elneser, “La evidencia digital eximiente de violación a la protección del dato personal a partir de la autorregulación,” *Academia y Derecho* vol. 10, pp.119. 156,Julio. 2015.https://doi.org/10.18041/2215-8944/academia.10.351

[15] O. A. Reina. (2016, Julio) Investigación Forense de Discos Duros Virtuales. https://bibdigital.epn.edu.ec/bitstream/15000/16634/1/CD-7260.pdf

[16] K. Wang, M. Du, Y. Sun, A. Vinel, Y. Zhang, “Attack Detection and Distributed Forensics in Machine-to-Machine Networks” *IEEE Network*, vol. 30, pp. 49 -v55, December 2016 https://doi.org/10.1109/MNET.2016.1600113N

[17] G. Burbano “La eficiencia, eficacia y credibilidad de la cadena de custodia en delitos flagrantes, por parte de grupos de intervención primaria” Skopein, vol 16, pp. 42-53.

[18] Fiscalía General de la Nación. (Aprobación 18-04-2018) Manual del Sistema de Cadena de Custodia, Versión 4. https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

[19] Poder Público-Rama Legislativa, ley 906 de 2004, art 275. “Código de Procedimiento Penal”. http://www.oas.org/juridico/spanish/mesicic2_col_Ley_906_2004.pdf

[20] L. E. Arellano y C. M. Castañeda. La cadena de custodia informático-forense. 2012. http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/45/42/0

[21] Pedro Javier Arnedo Blanco (2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1

[22] M López Análisis Forense Digital. 2007. https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[23] J. Henao. La Cadena de Custodia en el Sistema Penal Acusatorio.2012.https://repository.udem.edu.co/bitstream/handle/11407/277/La%20cadena%20de%20custodia%20en%20el%20Sistema%20Penal%20Acusatorio.pdf,sequence=1

[24] D. A. Ramírez y E. F. Castro (2018) Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia. . . . . https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17370/1/86078250.pd

[25] El Tiempo, Redacción de Justicia (01 de agosto de 2011). Caída de pruebas del PC de Reyes no afecta proceso de Piedad Córdoba. https://www.eltiempo.com/archivo/documento/CMS-10064845

[26] MINTIC, vive digital Colombia. (2016, 03, 18) Seguridad y Privacidad de la Información / Evidencia Digital. https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

[27] Ministerio de Justicia y Derechos Humanos, (2019, Feb, 08). Código Procesal Penal Federal. https://www.argentina.gob.ar/normativa/nacional/decreto-118-2019-319681/texto

[28] M. Duce, "Prueba pericial y su impacto en los errores del sistema de justicia penal: antecedentes comparados y locales para iniciar el debate", Revista Ius et Praxis, vol 24, no. 2, pp. 223 – 262, dic 2018 https://doi.org/10.4067/S0718-00122018000200223

[29] Congreso de la República Colombia, (2012, julio, 12), Código General del Proceso, http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012_pr001.html

[30] Área Digital Asociación por los Derechos Civile, La investigación forense informática en América Latina, 2018. https://adcdigital.org.ar/wp-content/uploads/2018/04/Investigacion-forense-informatica-Latam.pdf

[31] Ministerio de Justicia y Derechos Humanos, Guía para el levantamiento y conservación de la evidencia, 2017. http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf

[32] Biblioteca Nacional del Congreso Nacional de chile (2013, abril, 06), Guías de Procedimientos de Tanatología, https://www.leychile.cl/Consulta/m/norma_plana?org=&idNorma=1049932

[33] MINTIC, (2016, Julio, 29), Seguridad y Privacidad de la Información, www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[34] Fiscalía General del Estado de Morelos, (2015, septiembre, 28) Guía Nacional de Cadena de Custodia,http://fiscaliageneral.morelos.gob.mx/sites/pgj.morelos.gob.mx/files/12_-VF%201_0%20Gu%C3%ADa%20Nacional%20de%20Cadena%20de%20Custodia%20%2028-10-2015.pdf

[35] Ministerio Publico Fiscal (UFECI), (2016, marzo, 31) Guía de obtención, preservación y tratamiento de evidencia digital, https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[36] Congreso General de los Estados Unidos Mexicanos (2016, Junio, 17), Código Nacional de Procedimientos Penales, http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_250618.pdf

[37] UITpublications. Global Cybersecurity Index (GCI) 2017. https://www.UIT.int/dms_pub/UIT-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[38] Congreso de la Republica, Ley 1273 de 2009. http://www.mintic.gov.co/portal/604/w3-article-3705.html

[39] UIT publications. (Publicado en Suiza 2019) Global Cybersecurity Index (GCI) 2018. https://www.UIT.int/en/UIT-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

[40] S. Boyd, A. Horvath, D. Dornfeld "Life-Cycle Assessment of NAND Flash Memory", *IEEE Transactions on Semiconductor Manufacturing*, vol. 24, pp. 117 - 124, february 2011. https://doi.org/10.1109/TSM.2010.2087395

[41] T. Urabe, Y. Sakurai, "Magnetic analog memory elements of a single core", *IEEE Transactions on Magnetics*, vol. 3, pp. 470 -475, September 1967 https://doi.org/10.1109/TMAG.1967.1066084

[42] A. Linz (Julio de 1977). Diseño y Construcción de la unidad de memoria para una minicomputadora. https://bibdigital.epn.edu.ec/bitstream/15000/10713/1/T1268.pdf

[43] V. Leo Rideout, "One-Device Cells for Dynamic Random-Access Memories", Fifth European Solid State Circuits Conference - ESSCIRC 79, Southampton, UK, 2010.

[44] Kingston technology (2012). Guía de productos de memoria flash. https://media.kingston.com/pdfs/FlashMemGuide_LA.pdf

[45] Y. Park, J. Lee, S. Soon Cho, G. Jin, E. Jung, "Scaling and reliability of NAND flash devices", 2014 IEEE International Reliability Physics Symposium, Waikoloa, HI, USA, 2014

[46] K. Kwon, D. Hyun Kang, Y. Ik Eom "An advanced SLC-buffering for TLC NAND flash-based storage", *IEEE Transactions on Consumer Electronics*, vol. 63, pp. 459 – 466, November 2017. https://doi.org/10.1109/TCE.2017.015070

[47] M. Murugan, D. H.C. Du, "Hybrot Towards Improved Performance in Hybrid SLC-MLC Devices", 2012 IEEE 20th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, Washington, DC, USA, 2012 https://doi.org/10.1109/MASCOTS.2012.60

[48] P. Feng, Q. Li, P. Zhang, Z. Chen "Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics for Android Applications", IEEE Access, vol. 7, pp. 16695 – 16703, January 2019. . https://doi.org/10.1109/ACCESS.2019.2894643

[49] Y. J. Seong, E. H. Nam, J. H. Yoon, H. Kim, J. Choi, S. Lee, Y. H. Bae, J. Lee, Y. Cho, S. L. Min "Hydra A Block-Mapped Parallel Flash Memory Solid-State Disk Architecture", *IEEE Transactions on Computers*, vol. 59, pp. 905 – 921, March 2010 https://doi.org/10.1109/TC.2010.63

[50] GTI, (2016, junio, 28), Partes de una SSD, http://noticias.gti.es/servidores-y-almacenamiento/partes-de-una-ssd/

[51] J. Castillo, Qué es SSD, como funciona y para qué sirve. 2018. https://www.profesionalreview.com/2018/11/05/que-es-unidad-ssd/

[52] G. Juárez, Memorias Flash de Última Generación. 2011. https://www.academia.edu/17959406/memorias_flash

[53] Seagate, (2019), SSHD vs SSD: Unidad híbrida da un paso adelante en el ámbito de los juegos de PC. https://www.seagate.com/la/es/tech-insights/sshd-vs-ssd-hybrid-drive-for-desktop-gaming-pc-master-ti/

[54] Lenovo (2019), SSD vs HDD: ¿Which is the best for my PC? https://www.lenovo.com/gb/en/faqs/pc-life-faqs/what-is-ssd-vs-hdd/

[55] J. Kim, S. Seo, D. Jung, J. Kim, J. Huh "Parameter-Aware I/O Management for Solid State Disks (SSDs)", *IEEE Transactions on Computers*, vol. 61, pp. 636 – 649, April 2011 https://doi.org/10.1109/TC.2011.76

[56] M. C. Stamm, K. J. Ray Liu "Anti-forensics of digital image compression", *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 1050 -1065, February 2011 https://doi.org/10.1109/TIFS.2011.2119314

[57] V. Ianikeev, (2018, February 21,), NAND Flash Memories: Bad Block Management and the YAFFS File System. https://biblioguias.uam.es/citar/estilo_ieee

[58] C. S. Park, T. H. Han, "Fast mounting method for NAND flash memory file system using offset information", 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, South Korea, 2010

[59] Linux Devices Staff, (2003 Oct, 13) JFFS2 NAND Flash support arrives in stable Linux tree. http://linuxdevices.org/jffs2-nand-flash-support-arrives-in-stable-linux-tree/

[60] J. Regan, "The Forensic Potential of Flash Memory" M. S Thesis, Naval Postgraduate School Monterey, Monterey, California, USA, 2009