Article **ECORFAN Journal-Spain**
December, 2019 Vol.6 No.11 1-9

Proposal for a digital forensic investigation model in accordance with the legislation in Mexico

Propuesta de modelo de investigación forense digital acorde a la legislación en México

ORTEGA-LAUREL, Carlos†*, SANDOVAL-GUTIERREZ, Jacobo, LOPEZ-SAUCEDA, Juan and SERRANO-OROZCO, Adan Fernando

Universidad Autónoma Metropolitana, Department of Information Systems and Communications, Unidad Lerma, Av. de las Garzas No. 10, Col. El Panteón, Lerma de Villada, Estado de México.C.P: 52005

ID 1er Autor: *Carlos, Ortega-Laurel* / **ORC ID**: 0000-0001-6072-8480, **CVU CONACYT ID**: 104250

ID 1er Coautor: *Jacobo, Sandoval-Gutierrez* / **ORC ID**: 0000-0002-5578-4389, **CVU CONACYT ID**: 173501

ID 2do Coautor: *Juan, Lopez-Sauceda* / **ORC ID**: 0000-0001-5174-6046, **CVU CONACYT ID**: 164466

ID 3er Coautor: *Adan Fernando, Serrano-Orozco* / **ORC ID**: 0000-0003-0595-2185, **CVU CONACYT ID**: 205838

DOI: 10.35429/EJS.2019.11.6.1.9 Received September 10, 2019; Accepted December 15, 2019

Abstract

In this paper we collect and observes the existing digital forensic investigation models, which are essentially the application of information systems and communications engineering for forensic purposes. In addition, a review of the federal criminal situation in Mexico is presented (through the revision of the regulations in the Federal Criminal Code), because the Code indirectly describes the reality of what can be prosecuted and admitted as evidence, criminally speaking, with the application of digital forensic investigation models in Mexico. This is due to the significant deficiency in the proposal of digital forensic investigation models, in which there is not enough emphasis on the potential admissibility of the evidence gathered through the models, to give attention to the need to provide "evidence" to Institutions responsible for the impartation of justice, as if doing digital forensic investigation to be a technological issue and not as it really is: a socio-legal-technological issue. Therefore, considering the criminal reality in Mexico, locating the practices of existing models that make sense in accordance with the norm, an abbreviated model is proposed that really helps successful prosecutions.

Custody Chain, Digital forensic investigation model, Evidence

Resumen

En este artículo se recoge y observa los modelos de investigación forense digital existentes, que son en esencia la aplicación de la ingeniería en sistemas de información y comunicaciones con propósitos forenses. Además, se presenta una revisión de la situación penal federal en México (a través de la revisión de lo normado en el Código Penal Federal), mandato en que se describe indirectamente la realidad de lo que puede perseguirse y admitirse como prueba, penalmente hablando, con la aplicación de modelos de investigación forense digital, en México. Esto en atención a la significativa deficiencia en la proposición de modelos de este tipo, en que no se pone suficiente énfasis en la admisibilidad potencial de la evidencia reunida a través de tales, para dar atención a la necesidad de aportar "evidencia" a las Instituciones encargadas de la impartición de justicia, como si el hacer investigación forense digital fuese una cuestión tecnológica y no como realmente es: una cuestión socio-legal-tecnológica. Por lo anterior, considerando la realidad penal en México, ubicando las prácticas de los modelos existentes que hacen sentido en atención a la norma, se propone uno abreviado que realmente ayude a enjuiciamientos exitosos.

Cadena de custodia, Modelo de investigación forense digital, Evidencia

Citation: ORTEGA-LAUREL, Carlos, SANDOVAL-GUTIERREZ, Jacobo, LOPEZ-SAUCEDA, Juan and SERRANO-OROZCO, Adan Fernando. Proposal for a digital forensic investigation model in accordance with the legislation in Mexico. Journal-Spain. 2019. 6-11: 1-9

*Correspondence to Author (c.ortega@correo.ler.uam.mx)
† Researcher contributing as first author.

Introduction

Intuitively we recognize that when an act is committed that can potentially be constitutive of a crime, it becomes imperative to "preserve the crime scene." We have observed how in the streets of our cities, when a latent criminal incident occurs, the area is “cordoned off” to preserve the scene, which in the physically palpable world it is affordable to do, through the proper execution of the chain protocols of custody depending on the type of act, but few have stopped to think what happens in cases where the crime scene is not physical ?, but logical, because the crime has materialized not in the physical world, but in the digital world, in the world of computers, in the world of network networks such as the Internet or some other, technologies in which of course digital evidence plays a key role, given the ubiquity that enable.

This is how, given the need for the preservation of the digital crime scene, which will seek to reconstruct the facts, clarify the crime and point to the culprit, in this work a model is proposed, which meets the primary purpose of the preservation and prosecution of the evidence, such that such evidence manages to generate full conviction in the reasoning of the judge at the time of sentencing in a fact constituting a crime.

In addition, the aforementioned model to be proposed addresses the need for communication so that experts, judges, lawyers and police have knowledge about the best practice in the field of preservation and processing of evidence or evidence, in the digital field, related to an alleged criminal act, This is because those who are public servants, who in exercise of their powers come into contact with the evidence, are obliged to preserve the “digital place of the facts” and / or the finding and, consequently, to execute the processing appropriate, as provided in article 123 BIS of the Federal Code of Criminal Procedures.

It is not overlooked that any “corruption” of the evidence, in a digital crime scene, given its nature, can significantly alter the value of the evidence, with the corresponding consequences in the criminal judicial process, and the case may even occur that, given the “corruption” of the evidence.

The wrong person or persons are acquitted or condemned by the simple fact of not preserving the digital reality and / or processing it correctly, hence the relevance and importance of the model to be proposed.

Therefore, given the need detected, in this research work the proposal of a digital forensic investigation model according to the legislation in Mexico is made, for crimes with digital evidence, as an engineering application in which, as part of the forensic analysis practice, a structured investigation is carried out, while maintaining a documented chain of evidence, to find out exactly what happened and who was responsible for it, with a view that, once the forensic investigation is completed, it may be presented before the corresponding court of justice and the application of some or any of the criminal types provided for in the Mexican Federal Criminal Code is feasible.

Existing digital forensic investigation models

It is feasible to document in the literature various models of digital forensic investigation, since its appearance in 1995 with the model named “Computer Forensic Investigation Process” (CFIP), (Pollitt, 1995), (Selamat et al., 2008), the “ Digital Forensic Investigation Model (DFIM) (Kruse II et al., 2002), the "Digital Forensic Investigation Workshop" (DFRW) (Palmer, 2001), the "Abstract Digital Forensic Model" (ADFM) (Reith et al ., 2002), the “Integrated Digital Research Process” (IDIP) (Carrier et al., 2003), the “Digital Research Process Improvement” (EDIP) (Baryamureeba et al., 2004), the “Model Extended Cybercrime Investigation ”(EMCI) (Ciardhuáin, 2004), the“ DFM case relevance information ”(CRIDFM) model (Khan et al., 2016), the“ Computer forensic field triage process ”(CFFTP) model) (Beebe et al., 2004), the “Four Step Forensic Process” (FSFP) (Khan et al., 2016), the “Framework for a digital forensic investigation ”(FDFI) (Rogers et al., 2006), the“ Common process model for incidents and DF ”(CPMIDF) (Freiling et al., 2007), the“ Dual data analysis process ”(DDAP) (Pilli et al., 2010), the “Digital Forensic Investigation Framework” (DFIF) (Khan et al., 2016), the “Two-dimensional evidence reliability amplification process model” (TDERAPM) (Khan et al ., 2016), the “Digital Forensic Mapping Process” (MPDF) (Rahayu et al., 2008).

ISSN 2444-3204

The "Digital Forensic Model based on the Malaysian Investigation Process" (DFMMIP) (Perumal, 2009), the "DFM generic forensic network" (NFGDFM) (Khan et al., 2016), the "Digital forensic model for digital forensic investigation" (DFMDFI) (Ademu et al., 2011), the "systematic digital forensic model" (SDFM) (Agarwal et al., 2011), the "structured and consistent DFM" (SCDFM) (Khan et al., 2016), the "proactive and reactive DFM" (PRDFM) (Khan et al., 2016), the " Forensic Model generic informatics "(GCFM) (Yusoff et al., 2011), the" Common phases of computer forensic investigation models "(CPCFIM) model, (Khan et al., 2016), the" Comparative digital forensic model "(CDFM) (Dhananjay et al., 2013), the "event reconstruction model" (MER) (Carrier et al., 2004), and other very specific purposes that more than models represent techniques for specific technologies.

After collecting and reviewing the already listed and cited models of digital forensic investigation, it is possible to mention that there are a series of phases that we can refer to as "often used" in its structure, which is visualized, seek to help researchers execute the due processing to obtain a conclusion at the end of the investigation. As a summary, the stages defined repeatedly in the aforementioned models are rescued:

Collection: in this step, one observes, collects, searches, confiscates and obtains digital evidence, it is a primary phase and has the goal of not ignoring absolutely anything as discrete as it seems, however, there is no relation of the models with the chain of custody established in any standard.

Examination: at this stage, various techniques are applied to recognize and extract data, there are some sophisticated and simple techniques, however, it is perceived in all cases that the techniques describe technical procedures for obtaining information derived from scrutiny, processing or inspection, without documenting with the due evidence, which allows to give certainty of the manipulation of the evidence, to at any given time reliably prove the facts.

Analysis: in this phase the ilation is sought, the consequences are sought, the probable causes, inferences are made, it is deduced, it is hung, it is adduced, it is derived, it is deduced, and everything properly through using data and resources collected for Prove the case. The analysis is subject to rigor in terms of examining data and resources, however, there is a subjective part in that the conclusion reached is derived from the expertise in the analysis, and it is clear that there is no link with the chain of evidence custody.

Reports: in the last step, of the revised models, all the information obtained is presented in court. Here it is appreciated that there is an overflow of information, certainly not necessarily processed for the understanding of the audience to which it is delivered (normal people and learned in legal matters). In this phase in the common it is appreciated that the results are what the technical tests yield without an interpretation being made, so that what is communicated without the need for interpreters is plain, in practically all the referenced models, it is assumed that there is a generalized understanding of the digital and the interpretation is ignored in normal (non-technical) language, as if all citizens were natives or digital scholars.

Based on this review, a digital forensic investigation model is proposed in accordance with the legislation in Mexico.

Criminal reality in Mexico

Since 2008, the criminal justice system in Mexico has been gradually transforming into an accusatory one (Ornelas-Anguiano, 2015), with which the work of the experts in general, and especially the experts in forensic informatics, acquired great relevance, in fact the legal intervention of the experts and police officers, is the scientific basis of the investigation of the crime (Peña, 2016), without a legal intervention, no matter how sophisticated the forensic investigation model is, it will be before a scenario of illicit evidence.

ISSN 2444-3204

The ninth title, on the revelation of secrets and illicit access to computer systems and equipment, in its chapter II, entitled “illicit access to computer systems and equipment” of the Mexican Federal Criminal Code, portrays the criminal reality, and indirectly the reality of what can be pursued with the application of digital forensic investigation model according to the legislation in Mexico (with the application of forensic computer science in particular). This is how, assessing the "criminal type" that can be reached is to prove "illegal access to computer systems and equipment", which is in the first instance from the Code punishable by such, and in the second instance, what from the forensic can be reached, for presentation before a federal court of justice and it is feasible to apply the penalties provided by the Code.

For this, that is, the presentation is feasible, there are two major stages: preservation and processing based on articles 2, section II; 3, fractions VI, IX, X, subsection e, and XIII; 69; 123 BIS; 123 TER; 181; 182; 208, second paragraph; 209; 210, 211 and 220, of the Federal Code of Criminal Procedures (PGR, 2012); and it is in this sense that it is elucidated, there is evidence that, especially of the digital type, the manipulation of these in many of the cases implies the modification or alternation of such, so in view of the importance of which they are coated, require certain protection requirements for authenticity known as “chain of custody”, provided for in articles 227 and 228 of the National Code of Criminal Procedures (PGR, 2012).

Given that in Mexico, in accordance with the “Support Guide for the study and application of the National Code of Criminal Procedures” regarding Chain of Custody, the Attorney General's Office through Agreement A / 002/10 published in the Official Gazette of the Federation on February 3, 2010, issued a “Guide for the application of the General Code of Criminal Procedures in the chain of custody” (Ortega-Rosado, 2014), in order to establish and implement the processes, legal procedures and technical-scientists made by the members of the police institutions and the experts in aid of the Agent of the Public Ministry of the Federation, the protocols that integrate this chain (PGR, 2012), are:

– Knowledge of the commission of the crime by the Federal Public Ministry Agent (AMPF) or by the police.
– Preservation of the place of events by the police.
– Processing of the evidence or evidence by the authorized police units and / or experts directed by the Public Ministry (MP).
– Continuity of the Chain of Custody at the ministerial headquarters (integration in the previous investigation of the Chain of Custody).
– Continuity of the Chain of Custody in the expert headquarters (realization of the expert tests).
– Storage of evidence or evidence.

In this sense, it is reaffirmed, as documented by (Peña, 2016), that the legal intervention of experts and police officers is the scientific basis for the investigation of crime. Thus, in order to establish the guidelines that all public servants must observe for the proper preservation and processing of the place of the facts or of the finding and of the indications, traces or vestiges of the criminal act, as well as of the instruments, objects or products of the crime, since the protocols clearly state that the public servants referred to are those who in their actions must comply with the “chain of custody”, the Attorney General issued the Agreement A / 078/12 published in the Official Gazette of the Federation on April 23, 2012, in which it indicates, the minimum information that should be available in the chain of custody for a specific case (PGR, 2012), (Ortega-Rosado, 2014), namely:

a. Record of Chain of Custody, where the main data on description of the indication, dates, hours, responsible for the indication, identifications, charges and signatures of who receives and from whom they deliver are recorded;
b. Personal receipts kept by each person responsible for the indication and in which the data similar to the Chain of Custody Records appear;
c. Labels that are attached or printed to the packaging of the signs, for example, to plastic bags, paper bags, paper envelopes, manila envelopes, jars, cardboard boxes, among others;
d. Record books of entrances and exits, or any other system (for example: computer), which must be kept in the analysis laboratories, in the offices of the Public Ministry and in the warehouse; and

ISSN 2444-3204

e. Registration of storage conditions (temperature, humidity, etc.).

Therefore, from the rescue, it is contributed that what is relevant in a digital forensic investigation model, according to the legislation in Mexico, is to establish bases for the legal intervention of the experts and police, which are the scientific basis of the investigation of the crime, such that from its intervention, it is possible to demonstrate that all the links of the chain of custody, which are basically the date and place in which the evidence was received and delivered, the way in which it was guarded, is what will give "recognition to the test ", being therefore the minimum protection requirements for its authenticity, and in view of the importance of the chain being coated, it also prevails for the digital, because if the chain is not followed for the tests in the various models of digital forensic investigation documented in the literature, no model will achieve the legitimacy and incorporation of the evidence, so that you can inquire about any information that s and detach from it, doing this the fundamental thing and therefore what is rescued in the proposed model.

Model proposed to the reality of the regulations in Mexico

In this section, the proposed model will be described. The model consists of 4 phases and the flow structure is illustrated in Figure 1.

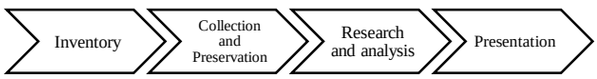

Figure 1 Proposed model of digital forensic investigation according to the legislation in Mexico
Source: Self Made

A. Inventory phase

The chain of custody according to the regulatory framework requires strict control over those who are involved in the lifting and manipulation of the evidence, without the completion of this stage, with due care and dedication, no proof as valuable as it may be. utility in no court. This phase is proposed as a stage of preparation of the evidence input, in fact, it is a period of time in the research model, where all the work and activities that allow the control and evidence of the evidence have to be carried out.

That will make it irrefutable, and must be done before the actual investigation is carried out, to strengthen the chain of custody. It obviously includes the study of the applicable forensic laws and guidelines, obtaining the investigation orders (to avoid the illegality of the evidence), the management support and the configuration of appropriate strategies and tools to avoid the corruption of the digital evidence, it can even be considered as a planning stage, but it should not be delayed but happen in the act, but in an organized manner, which is just what is proposed. This stage is completely lacking in existing models, but it is proposed because without it it is highly probable that no evidence is valid if it is not carried out.

B. Collection and preservation phase

The collection and preservation phase is where the contact with the evidence begins, it is in fact where the beginning of the life cycle of the evidence is located. The tasks performed include securing the crime scene, identifying and collecting volatile and non-volatile evidence, all of this: labeling and packaging, transporting, acquiring, storing and preserving evidence, according to the chain.

In the digital case, at this stage you can even collect monitoring devices or information such as the Intruder Detection System (IDS), the Intruder Prevention Systems (IPS), the Honeypot / Honeynet and other similar tools, which Although they may be digital equipment, which is not directly involved with crime, they are equipment that contains information that can give traceability, since in most cases of use of this type of technology, they are used for detection and prevention, depending on the nature of the network in which it is instructed, but which may well contribute to the clarification of the crime.

This even though they are not of specific purpose to preserve details of crimes, they may at one time be decisive for having indirectly substantiated facts.

In general, it can be mentioned that this phase is where the relevant data must be captured, stored and made available for the next phase, absolutely everything, however inconsequential it seems, must be preserved intact.

ISSN 2444-3204

Here, the consideration that must be untouched is highly relevant, because in digital the evidence is highly volatile, for example, if a computer equipment is seized, it is turned off and on again, each time this procedure is performed, it will be losing evidence, due to the nature of the digital system, hence it must be ensured that this does not happen.

Therefore, in this phase it becomes especially relevant, managing with the first phase, each element sought and seized, because each element is itself part of the evidence and hence it is increasingly important and essential (not physical, but logical element). These may be, to mention a few examples, access control, application control, operating system, network architecture, security infrastructure, and any others that are in the digital crime scene, which must be legally obtained., at all costs to avoid objection through the path of illicit evidence. For the above, in the specific case it is necessary to try to exist: the simple view, the search order, consent, and other protocols that are met for the evidence in the physical, but that must be executed in the digital field, with the intention that certainty be given, to what has already been highlighted, that it must be properly documented (keeping in mind the chain of custody), in accordance with the Mexican evidentiary norm.

As regards preservation, it is imperative to be cautious in the manipulation of evidence, it is reiterated: everything digital is highly ethereal, which can lead to the destruction of evidence without intention, and although scenario simulations offer An alternative to not directly manipulate the evidence, is not necessarily the best way because it can be objectionable, in this understanding, the cloning of the evidence to manipulate the evidence object, with all its attributes and limitations.

It is worth mentioning that the existing models, did not consider these activities, in a lot because it is not a technological issue, but it is in the techno-legal duo, and as it was already externalized to the problem it is treated as a purely technological issue.

C. Research and analysis phase

In the investigation and analysis it is where qualified forensic experts and experts seek evidence, for the case in the digital, that gives certainty, certainty or security to a reality in the field of digital, where digital data, translated or interpreted as information strongly support, refute or contradict what is seen or said in theses or hypotheses of those involved in digital events. Basically, what is sought to clarify is the reason for the state of the digital data, the intangible data being the entity that seeks to know, examine and analyze, in terms of status, sign and content, such that it gives guidance to support what which is intended in the case, to be preserved by the multicited chain of custody, which operates for one or several digital devices that at a given time were legally seized and properly preserved through the chain protocols.

This is where the scientific, technological and technical work is carried out, in the highest feasible detail, always using approved guidelines, so that they are recognized by the courts (and the procedures that lead to such conclusions are even repeatable) and invariably accredited forensic tools (since, if they are not, they lose credibility), all to intelligently achieve the traceability of the whole event, that is, to outline the path from the source of the crime and finally track who committed it without giving rise to error or set the doubt.

The evidence that will be generated in this phase of investigation and analysis will depend on the scope of the available techniques, the nature and the means used to commit the crime. It is also worth mentioning that it will depend on the initial legal hypothesis, which is sought to administer with the evidence available to prove a certain “criminal type”, since rather than prove what is technically or technologically available, the result sought is delineated by what the norms can punish, and hence the line, since even at a certain moment if the legally regulated does not elucidate the technological reach, that is, it can be done more than legally valid, then it can even be contradict what sensibly should be, or not of the initial hypothesis, with the development of investigation and analysis, in order to prove guilt in the court of justice.

ISSN 2444-3204

D. Presentation phase

The result of the investigation and analysis phase is compiled or summarized, and presented to the corresponding authority for consideration, this operates both in the case of digital tests, as in the case of physical tests. In the case of the presentation of the evidence, the guidelines for incorporating the evidence, described in the Criminal Procedure Code, which basically constrict to: the accreditation of the evidence, list as evidence (mark), give view to the counterpart, get the recognition of the test, achieve the incorporation of the test; So to bring the procedure to fruition, in the case of digital it is imperative to make prior preparation for the presentation.

It must be clear that this is the critical stage of the investigation, since all the evidence can be accepted or rejected, especially by the type of test, that is, digital, in which, if special care is not taken in what makes the chain of custody, can be widely questioned, objected and even discarded.

In this sense, the admissibility of the evidence before the court of justice, for example, depends on certain factors that include, among others, whether the evidence is conserved materially and adequately (in which cloning was already suggested, but such must be valid), if the evidence is relevant, duly identified and legally obtained, that is, if the procedure for obtaining it was missed, also if the language used in the presentation is simple and concise to be understood by the judge or jury, especially because in technical or technological jargon there are a number of technicalities that may be subject to interpretation and inaccuracies can lead to subjectivities that make you lose all objectivity, so this will require special attention, even in the presentation of evidence should consider if the prosecution and its team can put it into use in favor of the cause, that is, to defend and prove the intention, the motive, the identity tity or any detail against the challenges that may be presented to the test, given its digital feature, which is always objectionable, and the criticisms that are noticeable by the defendant's team or even the defendant himself, who generally pursue to undermine the validity of this type of evidence by its special nature.

It is relevant to state and always keep in mind that the critical point in this phase is to present the results to convince, since any evidence is a means of conviction, which will allow in any case to prove a case before the judge or jury in a court of justice and this is of all importance.

Recommendations for this tool to be applied in society

For the application of the proposal in society, or another model, it is recommended that experts, judges, lawyers and police, be trained in the matter through the communication of the model, as minimum guidelines to follow, for a first involvement and later, this in order not to violate protocols, and from this they are nourished by their experience using it, which is what will give them the inertia that will reach experts in the knowledge about the best practice in terms of preservation and processing of evidence or evidence, both from the digital and physical fields.

In this sense, although it is not feasible to certify the competence in the matter, given the diversity of scenarios, models, etc., if it is feasible that the lessons learned by those involved, at the time of use, in the practice itself , to the interaction, such feedback the model, to generate a knowledge base based on the practice, so that in a given breath, the evolution of the proposal is nourished by the practice of digital forensic investigation models, which is where it emerges the relevant It is absolutely clear that for the success of any model it is imperative to disseminate, share and use it, either to replicate it, standardize it or remodel it..

Conclusions

To date, the research models that have been proposed systematize the research work from the point of view of the application of engineering techniques, which is useful, but not essential. This is how such a design idea generates a large area of opportunity by being absent from what is really toral, which is: the legal framework adjustable from the model to be used.

ISSN 2444-3204

And it is that without proper understanding of the applicable legal framework, for example the Mexican: how it is intended to apply the laws of the procedure, and in the same way the application of the Codes that rescue the criminal types of cyber crimes, which is certainly punishable, creating a vacuum for the proper application of research models, with a view to substantiating evidence for judicial proceedings, because since its design, they are not created to be connected with the legal framework in which they are going to use.

Certainly, given the lack described, in the execution of any inquiry with the use of existing research models, the need to properly process the chain of custody, that is to say according to the law, cannot be forgotten, as any " contamination "of the evidence in a crime scene, however sophisticated the investigation model may be, can significantly alter the final result in a criminal proceeding and thereby condemn or acquit the wrong person or persons, maximally the legal intervention of Experts and police officers, is the scientific basis of crime investigation.

With the proposed model, the entire investigation is justified, the areas of improvement are identified and the considerations are established for each stage, ranging from the beginning of the investigation to the preparation for presentation in judicial proceedings. One characteristic, which we describe as excellent in the proposal, is that it is a model of a legal techno nature and, therefore, will help the investigation to be successful since it takes special care of the legal forms, which if not saved could be used as arguments that will prove faults to the procedure, arguing the illegal intervention of the experts and police.

A future work that can be raised for this investigation is the ideation of a digital forensic investigation observatory, which would focus the details of the investigations and their results, this to serve as a repository of experience to be used for future cases or instrumental improvements to peers, all with due handling of the evidence and the permissible display of sensitive information. It is a fact that the experience acquired and the lessons learned with digital forensic investigation models could well be knowledge that is relevant to share and use, whether to replicate, standardize, model or even train new stakeholders in the subject.

The cases could also be classified according to their status in the judicial procedure, and the observations made regarding whether the case is complete, suspended, pending and ongoing, this to have a timely follow-up start-effect-conclusion. In addition to the above, it can be mentioned that it would even be useful, in judicial proceedings in which they are made to run through all possible judicial instances, such that, at any given time, if required, the knowledge and evidence obtained allows guiding the various instances until they are exhausted by the promoter, such as a judicial appeal, the amparo, among others, where there is no other case, but the same in another instance and from the observatory everything that is considered useful as a reference can be provided, contributing to cooperation and information exchange, which can effectively favor successful prosecutions.

Additionally, by making intelligence on the information that is possessed, it would be feasible to develop investigative capacities, such as obtaining methodologies, which would effectively equate law enforcement agencies, to develop forensic investigation strategies and techniques, which can also contribute effectively to successful prosecutions, all to cement the scientific basis of crime investigation.

References

Ademu, I.O.; Imafidon, C.O; Preston, D.S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation, *International Journal of Advanced Computer Science and Applications*, 2(12), 175-178.

Agarwal, A.; Gupta, M.; Gupta, S.; Gupta, S. C. (2011). Systematic digital forensic investigation model, *International Journal of Computer Science and Security*, *5*(1), 118-131.

Baryamureeba, V.; Tushabe, F. (2004). The enhanced Digital Investigation Process Model, *Proceedings of the Fourth Digital Forensic Research Workshop*, 1-9.

Beebe, N. L.; Clark, J. G. (2004). *A Hierarchical, Objective-Based Framework for the Digital Investigations Process, Proceeding of Digital Forensic Research Workshop*, 2(2), 147-167.

ISSN 2444-3204

Carrier, B.; Spafford, E.H. (2003). Getting Physical with the Investigative Process, *International Journal of Digital Evidence*, 2(2), 1-20.

Carrier, B. D.; Spafford, E. H. (2004). Defining event reconstruction of digital crime scenes. *Journal of Forensic Science*, 49(6), JFS2004127-8.

Ciardhuáin, S.O. (2004). An Extended Model of Cybercrime Investigations, *International Journal of Digital Evidence*, 3(1), 1-22.

Dhananjay, K.; Jain, N. (2013). Comparative Digital Forensic Model. *International Journal of Innovative Research in Science, Engineering and Technology*, 2, 3414-3419.

Freiling, F. C.; Schwittay, B. (2007). Common Process Model for Incident and Computer Forensics, *Proceedings of Conference on IT Incident Management and IT Forensics*, 19-40.

Khan, M.A.; Nasir, A.; Ali, M.N.; Farooq, U.; Malik, S.A., (2016). Crime Detection using Digital Forensic Technology, *International Journal of Computer Science and Information Security*, 14(10), 487.

Kruse II, W.J; Heiser, G. (2002). *Computer Forensics: Incident Response Essentials*, Addison- Wesley.

Ornelas-Anguiano, O. D. (2015). La Cadena de Custodia en el Proceso Penal Mexicano, *Estudios Forenses*, (1), 1-24.

Ortega-Rosado, A. P. (2014). *Guía de apoyo para el estudio y aplicación del Código Nacional de Procedimientos Penales*, Suprema Corte de Justicia de la Nación.

Palmer, G. (2001). A Road Map for Digital Forensic Research, *First Digital Forensic Research Workshop*, 27-30.

Peña, J. A. (2016). La prueba pericial en el nuevo sistema de justicia penal en México, *Gaceta internacional de ciencias forenses*, (20), 16-24

Perumal, S. (2009). Digital Forensic Model Based on Malaysian Investigation Process, *International Journal of Computer Science and Network Security*, 9(8), 38-44.

PGR, (2012).Protocolos de Cadena de Custodia. Dos grandes etapas: preservación y procesamiento. Instituto Nacional de Ciencias Penales.

Pilli, E. S.; Joshi, R. C.; Niyogi, R. (2010). Network Forensic frameworks: Survey and research challenges, *Digital Investigation*, 7(1-2), 14-27.

Pollitt, M. (1995). Computer Forensics: An Approach to Evidence in Cyberspace, *Proceeding of the National Information Systems Security Conference*, 2, 487-491.

Rahayu, S.; Yusof, R.; Shaib, S. (2008). Mapping Process of Digital Forensic Investigation Framework, *International Journal of Computer Science and Network Security*, 8(10), 5-10.

Reith, M.; Carr, C.; Gunsch, G. (2002). An Examination of Digital Forensic Models, *International Journal of Digital Evidence*, 1(3), 1-12.

Rogers, M. K.; Goldman, J.; Mislan, R.; Wedge, T.; Debrota, S. (2006). Computer Forensic Field Triage Process Model, *Journal of Digital Forensics, Security and Law*, 1(2), 27-40.

Selamat, S. R.; Yusof, R.; Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, 8(10), 163-169.

Yusoff, Y.; Ismail, R.; Hassan, Z. (2011). Common Phases of Computer Forensic Investigation Model, *International Journal of Computer Science and Information Technology*, 3(3), 17-31.

ISSN 2444-3204