Deep Dive into digital forensic case management

by Washington Almeida

The choice of appropriate methods and procedures for digital forensic case management takes into consideration several aspects. In the Brazilian digital forensic scenario, it is common for the forensic approach to be based on the knowledge of the forensic professional working in a digital forensic process. But does this approach provide robust support in a forensic work process?

Particularly, in my work on digital forensics, I consider those methods and procedures that meet high standards of compliance, such as those developed by NIST for Incident Response. Why did I opt for NIST? NIST stands for National Institute of Standards and Technology, an American institute widely recognized for the high level of its technical studies and research, whose publications have accreditation by several institutes of quality around the world, such as INMETRO in the case of Brazil,

the National Institute of Metrology, Standardization and Industrial Quality, a Brazilian federal autarchy linked to the Ministry of Development, Industry and Foreign Commerce.

According to the NIST Special Publication 800-86 [1], forensic science is generally defined as the application of science to the law. The process, the methodology used, and the approach in conducting a digital forensics case investigation is critical to the outcome of such an investigation. The guideline and the approach of a robust method with legal support for digital forensic case management is what this article seeks to contribute.

What is digital forensics?

The best definition that I have read about digital forensics is one that has been defined by Gary L. Palmer as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations [2].

Due to the wide variety of data sources coming from various technologies, and the differences in the legislation in each country, it is difficult to build a global model for digital forensic case management. However, it is possible to segment the areas of forensic activity to determine specific research techniques in digital forensics.

Digital Forensics policies

Developing policies and procedures that establish the patterns for forensics work is very important when considering work in digital forensics.

The definition of policies implies reflecting on the question of the theoretical and scientific foundations used in cases of investigations and incident response. The policies and procedures should consider defining all requirements for the activities to the forensic work from the first pictures taken until the preparation of the final report.

It is also just as important to consider the recommendations of entities globally recognized such as the NIST institute that has been mentioned throughout this article and the reason why we consider its recommendations. This approach drives the outcome of very robust digital forensic work.

The Digital Forensics process

The main objective of a forensic process is to obtain the better understanding of the past events that can be investigated by using a methodology and appropriated techniques in order to allow the reconstruction of these events that aim to clarify the facts that may not be evident or may be hidden in digital information. According to the NIST Special Publication 800-86 document, the forensic process is represented by figure 1 shown below.

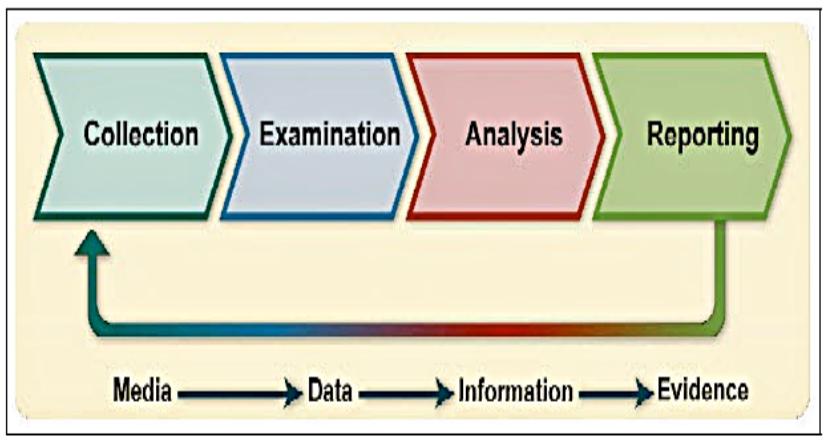

Figure 1: Forensic process

According to my learning at the Polytechnic School of the University of São Paulo, I would like to propose the same figure with a small change, adding the preservation process involved in the initial phases. Thus, in the same vein of the NIST forensic process, I just added the preservation process inserted in the forensic process as shown in figure 2.

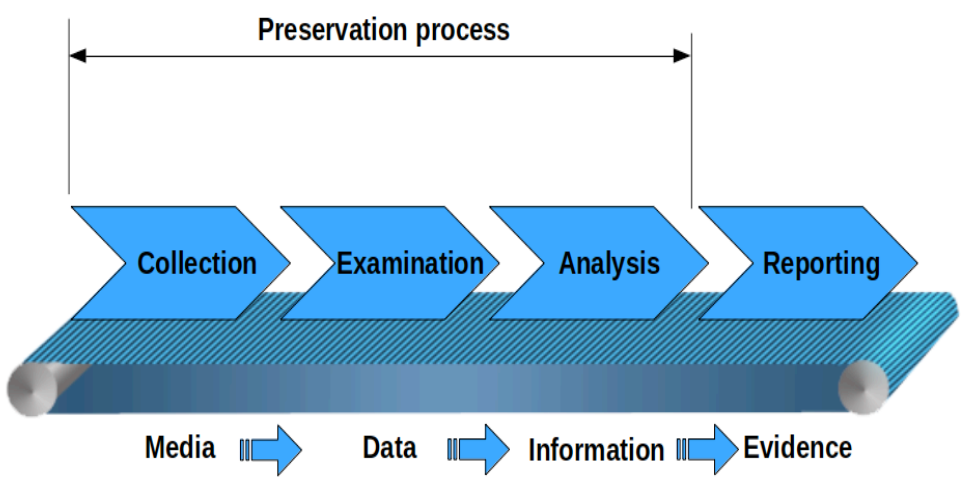

Figure 2: Preservation process inserted in the Forensic process

It is important to mention that this does not change the idea published in the NIST document and I reinforce that the NIST document is very well documented by the north American institute. Figure 2 just put emphasis on the concern with the preservation process that must be part of the collection, examination and analysis phases. This is important to put in evidence because, unfortunately, the deficiency in the preservation process present in these phases implies in forensic work faults and consequent impacts for the judicial process. In order to maintain the chain of custody, the digital forensic professional must be sure to preserve the evidence from the time it is collected to the time it is presented in court.

The preservation process should provide the capacity of reproduction of the analysis at any time by another forensic expert in the field of knowledge. This point is especially important because of the right to the full defense and contradictory present in legislation. Also this analysis may be requested by the other party to be analyzed by the technical assistant, which is the name given to the legal expert who is not appointed by a judge. Additionally, at any time, a judge may require a complement of the forensic.

Note that the preservation process is not only important in dealing with technical issues but also in regarding the legal aspect. This makes digital forensic work a multidisciplinary activity where professionals in the information technology and the legal areas need to work together to address cases properly. Once we have defined the concept of the digital forensic process, let us study each of the digital forensics phases in a little more detail.

Digital Forensics phases

In almost all literature and publications, we can find four phases that comprise digital forensics investigations: collection, examination, analysis and reporting. According to what I could learn from the discipline Computational Forensics in the Polytechnic School of the University of São Paulo, one of the most reputable educational institutions in Brazil, taught by the Doctor and Teacher Vera Kerr [3], I would add the preservation process as part of each phase excepting reporting, which constitutes the report output.

According to Vera Kerr, the concern for the scenario investigation's preservation is so important that often the nonobservance or small carelessness with this theme may jeopardize the forensic work even if it has been done with all the best techniques.

Preservation process: This phase is crucial so as to ensure that the data collected are free from contamination and it involves tasks such as management, which aim to ensure an acceptable chain of custody. This process should be taken as part of the collection, examination and analysis phases.

Collection phase: The tasks performed under this phase are related to the identifying, labeling, acquiring, collecting, transporting and storing of the data. In general, this phase is where all relevant data are captured, stored and made available for the next phase.

Examination phase: The examination phase constitutes the forensic processing of collected data that can be realized with a combination of automated and manual methods to assess and extract data of interest to the investigation always having in mind the concern with preserving the integrity of data. It is no coincidence that I care so much about preservation and for this reason, this topic is mentioned at almost every stage of a forensic investigation.

Analysis phase: The analysis phase involves the scientific methodology of the forensic procedures that will be applied to the analysis of the data collected and constitutes the work on the content obtained during the examination phase, using legally the justifiable methods and techniques. In her classes in the PECE/USP, Dr. Vera Kerr puts a lot of emphasis on adopting a scientific methodology that will support the forensic research work, always with the concern of preserving the integrity of the data. She knows that grounding the work based on an appropriate scientific methodology will bring robustness when evaluating the forensic work.

Reporting phase: The digital forensic professional is responsible for accurately reporting the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record each step taken during the digital evidence examination as explaining how the tools and procedures were selected. In this phase, it is important also to inform which scientific methodology has been used and the reason why it was chosen, since it will be assessed by lawyers and judges and they need to have the information with the highest level of accuracy and detail taking into consideration they can use this information to make important decisions.

Digital Forensics approach

Having in mind the concern with preservation, let us consider the approach of a preservation process by using digital forensic techniques while dealing with smartphones. It is common to see companies rooting smartphones during the forensic process. What is wrong with this approach? Rooting a smartphone, for those that have never heard about that, means giving yourself root permissions on your phone. It's similar to running programs as an administrator in Windows, or running a command with sudo in Linux.

The procedure of rooting the smartphone devices is so invasive that in doing so, the user is automatically giving up the warranty of the device. This would in itself be enough reason to avoid performing "root" on mobile devices, however, the motivation of the concern with this method is related to the legal implications involved in this procedure. Rooting changes the way the device will work and by consequence, it changes the original device configuration after it was delivered for forensic analysis.

Thus, rooting the mobile devices violates a basic principle of digital forensics: the preservation. Even if this method obtains the information needed to be presented to the justice, the forensic professional must be meticulous when choosing an appropriate scientific methodology to be adopted in such a procedure because the wrong choice can put in question all work deployed in the forensic analysis. In very specific cases, the information brought to justice by rooting the smartphone device may be accepted as valid evidence, however, if I were a lawyer I would question such a method.

This is a little example on how the wrong digital forensics approach of the appropriated methodology can bring impacts to the forensics works. So the preservation process must be at the top of the digital forensic specialist's concerns.

Digital Forensics in incident response

When performing forensics activities to support an incident response, the forensic professional must take care when taking decisions. Some actions taken without proper care may jeopardize the work already in the collection phase. It is important to have a well-defined forensic approach strategy when

presented to the situation. This scenario may become a bit more complex when several forensic professionals work together in response to an incident.

For example, we can mention the classic situation where one of the forensic specialists shuts off the computer as the first action upon contact with the evidence. In this simple mistaken action, the forensic professional may have lost forever the cryptographic keys stored in RAM.

This example tells us that all the professionals of a digital forensic team need to be very well aligned with the policies and procedures they should observe when making decisions regarding the many situations they may come to face.

This is the reason why I initiated this article with the topic Digital Forensics policies. Procedures documented in a well-defined policy will guide the forensic professional or digital forensic team in the best flow in a logical tree of decision-making.

Qualification for digital forensics

A skilled and well-prepared workforce is critical to doing digital forensics. The variety of digital systems, which include hardware and software, the complexity involved in each of these systems and the speed with which these technologies are recycled present a big challenge for professionals who work with digital forensics. These professionals need to be in constant process of learning and in continuous monitoring of technological evolution while at the same time having to deal with the answers to the incidents that every day devastate the judicial system.

Professionals in law and information technology will have to join forces to deal with new models of crimes involving technologies and the challenges in digital forensics tend to be treated by multidisciplinary areas as digital forensics area because it has the professionals prepared to treat with the complexity that the technologies bring and by the area of law that has the professionals prepared to guide the digital forensic professionals in how evidence can become useless if the bases of the laws are not observed.

Summary

As we can see, any digital evidence is fragile enough to be easily altered, damaged, or destroyed by improper handling. The original evidence should be acquired in a manner that protects and preserves the integrity of its data. The challenges in digital forensics are immense by virtue of the constant and rapid transformation in the assets of the information technology environment, such as hardware and software, as well as open and proprietary technology solutions. A challenge in proving chain of custody can arise when forensics specialists fail to place the information required in the collection phase.

If presenting a digital forensic work that is based on best practices and following guidelines of referenced entities, such as NIST and educational institutions such as the Polytechnic School of the University of São Paulo, one of the most renowned in Brazil, it is a good way to have a job technically irreplaceable and with the robustness expected by the agents of justice.

Finally, the work of making policies and procedures well detailed and defined takes a long time. However, each second of the work is worth the time invested when considering the positive results that this work brings as return to the justice and consequently for society.

About the author: Washington Almeida

Washington Almeida is an Electronic Engineer specialized in Digital Forensics and Cyber Security with more than 25 years of experience in the Information Technology and Engineering areas, working for large companies in the sectors as Engineering, Information Technology, Consulting, Chemical and Mining. Experienced professional with Cisco and Microsoft MCSE certifications acts as Digital Forensics with in-depth knowledge of computers hardware, network technologies, telephony, programming, data communication protocols and a vast amount of information security knowledge with a set of skills known by ethical hackers where this knowledge base is fundamental to assist the Justice.

Web page: www.washingtonalmeida.com.br

Images in text:

Figure 1: This image shows the NIST Forensic process;

Figure 2: Preservation process inserted in the NIST Forensic process;

References:

[1] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Access in January 03, 2017.

[2] Gary L Palmer.(2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

[3] Vera Kerr is Teacher of the Specialization Course in Law and Information Technology of the Continuing Education Program of the Polytechnic School of the University of São Paulo (PECE-USP), responsible for the discipline Computational Forensics.