v. 4, n. 1, 2024

Journal of
Engineering
Research

THE ANALYSIS OF DIGITAL EVIDENCE OF CHILD PORNOGRAPHY IN STORAGE MEDIA

Isabela Dias Magnani
``Faculdade de Tecnologia do Estado de São Paulo`` – FATEC
Araraquara – SP
https://lattes.cnpq.br/7738413997483124

Fábio Papini Fornazari
``Faculdade de Tecnologia do Estado de São Paulo`` – FATEC
Araraquara – SP
http://lattes.cnpq.br/4582985051285651

DOI: https://doi.org/10.22533/at.ed.1317412409016

Abstract: Computer forensics aims to investigate digital evidence, contributing to the resolution of crimes. With technological developments, the crimes of dissemination and possession of child pornography have been facilitated by the numerous means in which records can be stored and disseminated. Thus, we seek to understand the challenges in the analysis phase of digital evidence of the crime of child pornography by comparing the Autopsy and IPED software. In the theoretical framework, the works of Eleutério and Machado (2010) and Hassan (2019) stand out, which present techniques and describe the difficulties in forensic examination. Using different parameters, it was possible to evaluate the convenience of using each software. However, regardless of the tool used, conclusive analysis carried out by humans is essential.

Keywords: Computer Forensics, Child Pornography, Software Analysis.

INTRODUCTION

Digital forensics consists of the area of forensic science that uses scientific knowledge to collect, analyze, document and present digital evidence of virtual crimes so that it can be used in a court of law. The purpose is to answer questions about what happened, when and who did it. In any digital forensic investigation process, rigorous procedures must be followed that maintain and document the chronological history of traces collected from crime scenes or victims, with the aim of tracking their possession and handling from recognition to disposal, which is called chain of custody, as provided in art. 158-A of the Criminal Procedure Code.

Regarding the means used to commit crimes, the investigation is carried out on all devices that store digital data and from which it is possible to legally extract evidence, such as computers, cell phones, USB drives, *pendrives*, tablets, disks rigid, among others.

Storage devices are used to carry out illegal activities, such as the crimes of dissemination and possession of child pornography set out in art. 241-A and 241-B of Law 8,069/1990 – the Child and Adolescent Statute (ECA), which is recurrent and requires specific techniques for its investigation. According to data from Safernet Brasil, reports of child pornography grew 33.45% in 2021, considering that, between January and April, 15,856 pages related to child pornography were reported to Safernet Brasil, surpassing the historical record for reports recorded in the year 2020.

Considering the various steps observed in digital forensics, the general objective of this work was to carry out a case study of the procedure for analyzing supposed digital evidence found on a pendrive in relation to the crime of child pornography and to understand the difficulties observed during the procedure. As specific objectives, this article sought to study the functioning of software in cases of encrypted, deleted files and keyword search, through two software used in forensics, namely Autopsy and IPED (Evidence Indexer and Processor). Digital), observing their facilities and difficulties for the user and, finally, making considerations about the results obtained from both software and discussing the main challenges encountered during the analysis of digital evidence.

To do so, it will be assumed that all previous procedures were carried out correctly and in a legally valid manner.

COMPUTER FORENSICS

Digital forensics or computer forensics is the area of forensic science that uses knowledge to collect, analyze, document and present digital evidence found, in order to assist in investigations.

> Forensic Computing's main objective is to determine the dynamics, materiality and

> authorship of illegal acts linked to the IT area, with the main issue being the identification and processing of digital evidence in material evidence of crime, through technical-scientific methods, checking probative validity in court (ELEUTÉRIO; MACHADO, 2010, p. 16).

Through a set of techniques and procedures, information is sought regarding past events in an investigation, which may be criminal or also civil, in particular cases in which it is not desired to seek legal action at first. Based on the analysis of the events that occurred, it is possible to reconstruct the actions carried out on the various equipment and storage media questioned. Furthermore, an extremely relevant feature in forensic computing is the guarantee of the integrity of the evidence obtained, that is, ensuring that no type of alteration has occurred in order to prevent forensic reports from being invalidated due to doubts about possible manipulation or contamination. of the questioned material. Therefore, the expert must be careful when handling equipment and media received for analysis (VECCHIA, 2020).

In order to identify the authorship and materiality of the crime, cybercrime investigations require computer expertise with traces left by the criminal practice. In these cases, both computers and media have files, system records and other information that constitute evidence of the crime and can be used as material evidence. As a means of helping to clarify and convince the court regarding illicit content, the expert examination and the report produced will be used (CARNEIRO, 2017).

EXAMS ON COMPUTATIONAL STORAGE DEVICES

Regarding in-device examinations of computational storage devices, Eleutério (2010, p. 20) asserts that "they are the most requested expert examinations in Forensic Computing and basically consist of analyzing files, systems and programs installed on hard drives, CDs, DVDs, Blue-Rays, *flash drives* and other storage devices." In most cases, only the components that store user information are relevant, with the hard drive being the component where user files are generally located.

When an expert receives a computing device for analysis, a series of steps must be followed, depending on the type of equipment, as the main characteristics of digital storage media are fragility, sensitivity to lifetime and use and ease of copying. Specifically, regarding these media, most Forensic Computing exams are carried out in four main phases, ranging from receiving the material to completing the report, namely: preservation, extraction, analysis and formalization (ELEUTÉRIO; MACHADO, 2010).

In the preservation phase, the aim is to ensure that the information stored in the questioned material does not undergo any changes, so that integrity is ensured. To this end, forensic examinations must be carried out on copies of the original equipment by mirroring, which consists of copying data bit by bit from one device to another, or image, in which data is copied to files.

Such computational techniques are carried out using forensic software. In the extraction phase, all information contained in the copy of data from the preservation phase is recovered, bearing in mind that all procedures will be carried out on the copy. In the third phase, data analysis is carried out, a stage in which the information extracted in the previous phase is examined, with the aim of identifying digital evidence present in the material examined that is related to the crime investigated, one of the ways being research by keywords, which is an efficient way to locate digital evidence necessary for preparing the forensic report. Finally, the last phase is formalization, in which the expert prepares the report, bringing the results and presenting the digital evidence found in the materials that were examined. Furthermore, the report must include the main procedures used in the stages of preservation, extraction and analysis of content (ELEUTÉRIO; MACHADO, 2010).

CRIMES OF SHARING AND STORING CHILD PORNOGRAPHY

In line with constitutional precepts, the Child and Adolescent Statute (ECA), in its art. 1st established the so-called Principle of Comprehensive Protection of Children and Adolescents, with a person up to twelve years of age being considered a child, and an adolescent being anyone between twelve and eighteen years of age.

Child pornography consists of an illegal form of pornography characterized by the use of erotic images of children and adolescents and is a major cause for concern on the internet, considering that the supposed anonymity that involves the use of the internet can represent a field full of possibilities for adopting behaviors that would not be adopted if the individual had to expose themselves. Thus, the internet can prove to be an environment conducive to the dissemination of child pornography or the commission of crimes against children and adolescents with a sexual connotation (JORGE; WENDT, 2013).

When analyzing art. 241-A of Law 8,069/1990 – the Child and Adolescent Statute – it is possible to observe seven nuclear verbs of this type. The first hypothesis is expressed by the verb offer, which consists of the presentation or proposal for something to be accepted. The second verb is "exchange" and consists of an exchange of one thing for another. The third verb "make available" relates to cases of hosting and sharing files so that third parties can make copies or downloads. The fourth verb "transmit" is related to the sending of material involving pornographic content between peer-to-peer Internet users, as occurs with messaging applications such as WhatsApp, Telegram, among others. The fifth verb "distribute" is generally carried out through emails in the form of spam so that the content is conveyed to a multitude of users. With regard to the sixth nuclear verb "publish", the conduct takes place directly, through exposure of the scene through social networks, such as Facebook, for example, or blogs. Finally, the seventh nuclear verb of the type "disclose" by any means consists of making the content known, but not directly, as occurs in publication, which could be, for example, through the use of a link that directs the user to the content. Furthermore, the first paragraph, items I and II, of art. 241-A of the ECA typify the crime of ensuring means or services for dissemination. Unlike someone who commits the crime of producing or circulating, in this case, the agent's conduct consists of securing the means, such as DVDs, hard drives or others that can store files containing photographs, scenes or images of child pornography (SILVA, 2017).

The actions described in the criminal category are related to the dissemination of child pornography, whether through photography, video, or other recording that presents an explicit sex or pornographic scene containing children and adolescents. Furthermore, art. 241-B of the ECA on the acquisition, possession or storage, by any means, of photographs, videos or other forms of recordings containing explicit sexual or child pornography scenes.

In view of this, it is possible to observe that the aim is to ensure full protection for children and adolescents, in addition to recommending, for this purpose, the union of efforts between the family, society and the State to realize these rights (BRITO, 2013).

EXPERTISE IN COMPUTER DEVICES THAT CONTAIN CHILD PORNOGRAPHY

To detect child pornography on computer storage devices, it is necessary for the expert to look for the storage of photos or videos with this type of content. As Eleutério (2020, p. 256) states, "in laboratory exams, this search covers active files, those that were sent to the trash and even those that were deleted and recovered, using *data carving* techniques". There are also cases in which files of this nature are found, but which were not stored on the device directly by the user, such as, for example, temporary images from internet browsers (ELEUTÉRIO, 2020).

USE OF ANTI-FORENSIC TECHNIQUES: ENCRYPTION

Antiforensic science consists of the set of techniques used to hinder forensic analysis, seeking to interrupt and disrupt investigations, making the capture and analysis of digital evidence a very difficult or impossible process. Through the use of anti-forensic techniques, the aim is to destroy or hide evidence to frustrate the work of investigators (HASSAN, 2019).

Encryption consists of the practice of hiding information by obfuscation so that it becomes unreadable to unwanted recipients. Despite playing an important role in information technology systems, the wide dissemination of encryption tools has made investigation difficult or even impossible without the suspect's cooperation, and can be used as an anti-forensic technique. According to Hassan (2019, p. 273), "in cryptography, a key is a string of bits used by an algorithm to change information from plain text to cipher text and vice versa".

> The most common and widespread anti-forensic technique today is the use of encryption of a file, volume or entire medium. Although legitimate to guarantee data confidentiality, the use of encryption becomes malicious when the protected information constitutes traces of criminal actions or crimes (CAMARGO; RODRIGUES, 2020, p. 487).

DATA RECOVERY

Digital data from storage devices is organized in such a way that not only data is visible to users. In other parts of the disk, there are hidden, temporary, encrypted files, fragments, among other information. Through the use of specific techniques, it is possible to recover data that has been deleted. This is because when you delete a file, you do not overwrite all the content occupied by the file with zeros and/or ones, there is only control over which parts of the disk are occupied or available. Generally, file recovery is based on searching for signatures, also known as headers, of known files across the entire available area of the disk. When finding a signature, the content of the file is searched, recovering the original information in full or in part, in the latter case, the complete content is not available because part of it has been overwritten by another file. The process of recovering files based on signatures is called *data carving* (ELEUTÉRIO; MACHADO, 2010).

FILE NAME CHECK

The way child pornography files are shared over the internet is the main reason for using the file name verification technique. Often, countless files of this nature are exchanged using P2P sharing programs. To find files with this type of content, users use typical expressions and keywords referring to child pornography. According to Eleutério (2020, p. 259), "once downloaded, child pornography files are saved on the user's computer device and the names of these files contain at least one of the searched expressions or keywords". This way, if the files are not renamed, a simple search for these expressions is enough to find them. According to a study carried out in 2009, some of the most used keywords to search for child pornography files in sharing programs were mapped, such as "childporn", "pedo", "pthc" (ELEUTÉRIO, 2020).

SOFTWARE USED IN THE CASE STUDY: AUTOPSY AND IPED

Autopsy is a graphical user interface program that provides easy access to the command-line tools as well as the C library included in Sleuth Kit and other digital forensic tools. Most of the forensic analysis tasks required in many investigations can be done automated by Autopsy, such as recovering deleted files, inspecting unallocated disk space, among others. According to Hassan (2019, p. 178), "Autopsy provides additional features that help examiners to be more productive during analysis work".

IPED – Digital Evidence Indexing and Processor – is open source software that can be used to process and analyze digital evidence, much of it seized at crime scenes by police officers or in corporate investigations by private experts. This indexer is a tool implemented in Java and was developed by forensic experts from the Federal Police. Since its creation, the tool's objective has been to process data efficiently and stably. Some important features of the tool are: command-line data processing for batch case creation, cross-platform support, tested on Windows and Linux systems, execution possible from removable drives, and integrated and intuitive analysis interface.

Both software was used in the case study developed in this work. Using the tools, an image analysis of a pendrive was carried out, in which procedures related to the recovery of deleted files, the search for keywords, the detection of encrypted files and the existence or not of nudity detection resources were compared, with the aim of understanding how each software performs such activities.

METHODOLOGY

In order to achieve the objectives outlined for the article, a bibliographical survey was carried out for the conceptual basis of the topic, which included research in books and on the Internet. In addition to the bibliographical survey, a case study was carried out with the aim of comparing two forensic software: Autopsy and IPED.

To this end, steps were followed. First, a 2GB pendrive was quickly formatted. After that, text files were created, some named with keywords that refer to the crime of child pornography, such as "pedo", "childporn", "lolitas", JPEG photos and mp4 videos were added, one of them being an advertisement for a children's product showing babies in a nude situation, encrypted files, PDF, Excel, files downloaded from the Internet and messaging applications. Some of these files have been deleted. Next, an image of the pendrive was created using the Forensic Toolkit - FTK software. The image created was loaded into the Autopsy and IPED software for processing the evidence, comparing the following parameters: accessibility, related to the possibility of anyone accessing the product, regardless of its conditions, including hardware and software; functionality, generally evaluated by the number of features provided; usability, which consists of the ease of using the program; performance, which can be measured by the time in which tasks are performed, and accuracy, related to the precision of results.

Some common features were analyzed, such as recovering deleted files, detecting encrypted files and searching by keywords, as well as exclusive functions related to the crime of child pornography.

It was assumed that the procedures prior to the analysis phase respected the chain of custody, maintaining the integrity of data and information.

RESULTS/DISCUSSION

In terms of accessibility, Autopsy proved to be easily accessible, as it does not require *plugins*, while IPED requires the installation of *plugins* for the operation of some features, including for its own installation it was necessary to update Java to version 11, which highlights its lower accessibility.

Regarding functionality, both Autopsy and IPED carried out the search by keywords, including the possibility of creating lists to carry out such a search in both programs. Furthermore, both software detected encrypted files and recovered files that were deleted. In the latter case, both Autopsy and IPED brought files that were on the *pendrive* before the quick format was performed. However, IPED's biggest difference, with regard to the crime of child pornography, is the ability to detect images and videos with possible nudity, since images and videos containing nudity were highlighted. Despite the existence of false positives and false negatives, the resource proved to be fundamental in helping to detect images and videos with nudity and, consequently, in the possible configuration of the crime of child pornography.

Regarding usability, Autopsy proved to be easier to use, considering that it has a simple interface, in which the results are found in a single tree on the left, while IPED proved to be more complex, as it is necessary Search menus and apply filters to find the information you are looking for. Furthermore, IPED has tool configuration files in which certain features can be enabled or disabled through commands, which demands greater knowledge on the part of the user and highlights greater complexity in use.

Regarding performance, Autopsy is faster in processing evidence, considering that the forensic image from the *pendrive* was loaded in a few seconds. IPED, in addition to being slower in processing evidence, depending on the resource enabled, processing becomes unfeasible considering the computational capacity. For example, when enabling the feature called Yahoo NSFW Detection, an algorithm that indicates possible pornography images, in addition to the need to install several plugins, when trying to run the program with this feature enabled, it was indicated that finishing processing the evidence would take more than 30 thousand hours, showing that performance is affected depending on the functionality enabled.

Finally, the last parameter analyzed was accuracy. Regarding the accuracy of the results, both Autopsy and IPED brought the searched keywords. However, in practice, despite the searched keywords being included, these would be false positives, given that, in the case at hand, they do not indicate the consummation of a crime. As far as encrypted files are concerned, they were all detected and indicated accurately. Regarding the recovered files, both software brought files that were deleted after being created after quick formatting and files that were on the device prior to formatting, that is, even though the pendrive was formatted, files remained on the device. media. IPED has additional capabilities for detecting images and videos with possible nudity, in which false positives and false negatives have been observed. Even so, for the purpose of searching for evidence of child pornography, IPED is more accurate as it indicates images and videos of possible nudity, essential to the crimes in question.

CONCLUSION

Considering accessibility, usability and performance, for non-technical researchers, Autopsy is the most recommended tool as it is less complex and brings satisfactory results. In the case of experts who need tools with more resources to assist in the analysis process, IPED is more recommended, although more complex, as it brings more assertive results and with greater agility through resources and filters that assist in detection. nudity of children and teenagers.

However, it is worth highlighting that the tools are only a support, as the human eye is essential, considering that, in addition to the large number of false positives and false negatives, it is necessary to analyze the context in which the images and videos were recorded. For example, it is essential that the investigator has common sense and attention, as family photos containing children and babies in everyday situations, swimming in the pool, taking a shower do not constitute an illicit act, considering that, for it to be considered a crime, images or videos of a child or adolescent must indicate involvement in explicit, real or simulated sexual activities.

REFERENCES

BRASIL. **Constituição da República Federativa do Brasil**, promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 20 set. 2022.

BRASIL. **Decreto-lei nº 3.689, de 03 de outubro de 1941**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 19 nov. 2022.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 19 set. 2022.

BRASIL**.** Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crime s_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 20 set. 2022.

BRITO, AURINEY. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense**. São Paulo, Novatec Editora, 2010.

HASSAN, Nihad A. **Perícia Forense Digital: Guia Prático com Uso do Sistema Operacional Windows.** São Paulo: Novatec Editora Ltda, 2019.

IPED Digital Forensic Tool. Disponível em: https://github.com/sepinf-inc/IPED. Acesso em: 21 set. 2022.

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2 ed. Rio de Janeiro: Brasport, 2013.

SAFERNET. **Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil**. [S.I.], 2021.
Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 20 set. 2022.

SILVA, Ângelo Roberto Ilha da (Org.), SHIMABUKURO, Adriana (et al.). **Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infanto-juvenil, infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas**. Porto Alegre: Livraria do Advogado, 2017.

VECCHIA, Evandro Dalla. **Perícia digital: da Investigação à Análise Forense**. 2 ed. Campinas: Millenium Editora, 2019.

VELHO, Jesus Antonio (Org.). **Tratado de Computação Forense**. Campinas: Millenium Editora, 2020.