RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.
Year IV, v.1, n.2, Aug./Dec. 2024. | submission: 2024-12-01 | accepted: 2024-12-03 | publication: 2024-12-05

LITERARY ANALYSIS OF COMPUTER FORENSIC TOOLS IN THE FIGHT AGAINST IMAGES OF CHILD ABUSE AND EXPLOITATION

LITERARY ANALYSIS OF COMPUTER FORENSIC TOOLS IN COMBATING IMAGES OF CHILD ABUSE AND EXPLOITATION

Ana Maria Cardoso de Souza[1]– State University of Mato Grosso Prof. Ma.
Déborah Barbosa Camacho[2]– State University of Mato Grosso Prof. Ma.
Raquel da Silva Vieira Coelho[3]– Mato Grosso State University

SUMMARY
This article addresses the role of free computer forensics tools, such as Autopsy, IPED, and NuDetective, in combating child abuse and exploitation in digital environments. The analysis, based on a literature review and exploratory research, highlights the importance of these tools by assessing their effectiveness and identifying limitations. The work also seeks to align them with the guidelines of the Child and Adolescent Statute (ECA) and the General Data Protection Law (LGPD), ensuring that the application of such technologies respects legal and ethical rights. The results indicate that, despite the limitations in relation to paid tools, free solutions are useful when combined with technical training and public policies, contributing to the investigation and prevention of these crimes in cyberspace.
Keywords: Computer Forensics; Cybercrime; Forensic Tool; Pedophilia and Child Exploitation.

ABSTRACT
This article addresses the role of free computer forensic tools, such as Autopsy, IPED and NuDetective, in combating child abuse and exploitation in digital environments. The analysis, based on a literature review and exploratory research, highlights the importance of these tools when evaluating their effectiveness and identifying limitations. The work also seeks to align them with the guidelines of the Child and Adolescent Statute (ECA) and the General Data Protection Law (LGPD), ensuring that the application of such technologies respects legal and ethical rights. The results indicate that, despite the limitations in relation to paid tools, free solutions are useful when combined with technical training and public policies, contributing to the investigation and prevention of these crimes in cyberspace.
Keywords: Computer Forensics; Cybercrime; Forensic Tool; Pedophilia and Child Exploitation.

1. INTRODUCTION

Child abuse and exploitation are deeply concerning issues that affect children around the world, regardless of their socio-economic, cultural or ethnic background. With the advancement of technology and the expansion of internet use, these crimes have adapted to the digital environment, taking on new forms, such as the production, distribution and consumption of child abuse material online. This scenario creates significant challenges for authorities and society at large, as images and videos of child abuse can circulate indefinitely, perpetuating the suffering of victims and making it difficult to eradicate this type of crime.

In the fight against these criminal activities, Forensic Computing emerges as an essential tool. Forensic Computing can be defined as the process of identifying, collecting, preserving, analyzing and presenting digital evidence for use in legal proceedings. According to Maras (2015), forensic computing rense covers the entire lifecycle of digital evidence, from its collection to its presentation in court. This area of forensic science is crucial for the investigation of cybercrimes, including those involving child abuse and exploitation. As pointed out by Chawki, Darwish and Khan (2015), cybercrimes encompass a wide range of crimes, with child abuse being one of the most serious.

This article aims to conduct a literary analysis of some of the main free Computer Forensics tools used to combat images of child abuse and exploitation. The purpose is not only to identify and discuss these tools, but also to contextualize them within the Brazilian legal framework, including the Statute of Children and Adolescents (ECA) and the General Law for the Protection of Personal Data (LGPD). In addition, the study intends to enumerate and discuss related works that address the

use of these tools in protecting children's rights.

In the current scenario, there are several free forensic tools available that can be used effectively to combat online child abuse. The choice of this topic is justified by the seriousness of the problem and the alarming growth in the number of reports related to child abuse images, as evidenced by data from the NGO Safernet, which recorded a 77.13% increase in reports from 2022 to 2023.

Therefore, the literary analysis proposed in this article seeks to contribute to the understanding of the capabilities and limitations of Computer Forensics tools in combating online child abuse, providing *insights* that may be useful to professionals and researchers in the fight against this violation of children's rights.

2. THEORETICAL BASIS

This section aims to present the subsections of this article in a clear and concise manner. Subsection 2.1 addresses the definition of Computer Forensics, which is crucial for the investigation of cybercrimes. Subsection 2.2 explores several fundamental tools for digital forensics, such as Autopsy (2.2.1), IPED (2.2.2), and NuDetective (2.2.3), each contributing specific features for the investigation of digital crimes.

Subsection 2.3 emphasizes cybercrimes, with a focus on the investigation of images of child abuse and exploitation (2.3.1), discussing the techniques needed to deal with this type of crime. Subsection 2.4 addresses relevant legislation that protects data and images, including the Child and Adolescent Statute (2.4.1) and the General Data Protection Law (2.4.2), guaranteeing rights and regulating the processing of personal information.

Finally, section 3 presents the methodology used to develop the article, while section 4 reviews studies and works that explore the use of Forensic Computing tools in combating the misuse of child abuse images.

2.1 Computer Forensics

Forensic Computing can be defined as an area of Computer Science that is gradually developing to meet the demand arising from Criminalistics and as a part of Criminalistics that appropriates the fundamentals of Computer Science (Melo, 2009). This area is based on investigating and reconstructing illegal acts through the identification, collection and analysis of evidence or information magnetically stored or encoded (Mercuri, 2005).

In practical terms, forensic computing can be summed up as a set of practices adopted for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence that is valid in legal proceedings (Silva Filho, 2016).

Its main object of investigation is cybercrimes. According to Maras (2015), are defined as “The use of the Internet, computers and related technologies in the commission of a crime”. Cybercrimes are identified and investigated with the help of various tools, as described in subsection 2.3.

2.2 Computer forensics tools

Forensic tools play a crucial role in the search, detection and recovery of potential digital evidence from storage and processing devices. Their use is essential for investigating cybercrimes, including child abuse and exploitation. The tools: Autopsy, IPED System and Nu-Detectives who help investigators identify image files, videos, messages and records of relevant activities, thus contributing to holding those responsible for these crimes accountable.

2.2.1 Autopsy

Autopsy Linux is an open source digital forensic tool that allows the analysis of a file system of a given forensic image, and can be used for military and corporate purposes in order to reconstruct the events that occurred on a given host and that led to its compromise (Autopsy, 2003).

According to Richardson, Marjie, (2018)*apud*Evaristo (2023) the autopsy is known for its The ability to perform temporal analysis, allowing investigators to view events on a timeline, i.e., detailing everything from file creation to deletion. This is essential for understanding the sequence of activity on a device and identifying suspicious patterns or actions. Another significant feature is the keyword search functionality, which makes it easy to quickly identify relevant information.

The tool also has a variety of built-in modules that allow users to identify specific data, such as web browsing histories, connections, or geolocation records. In addition, the forensic community can develop and share their own modules, further expanding the tool's capabilities (Richardson; Marjie, 2018*apud*Evaristo, 2023).

2.2.2 Digital Evidence Indexing and Processing System (IPED)

According to the Brazilian Federal Police (Polícia Federal, 2019), IPED is an open-source system developed in Java, used for indexing and processing digital evidence, which searches for and organizes data of interest in visible files. In addition, IPED recovers hidden, deleted and fragmented files that are on devices such as hard drives, flash drives, memory cards, SSDs, CDs, DVDs and other types of storage media.

IPED is a free tool that has excellent performance and high processing speed, which is necessary for large volumes of data on high-capacity media used by Brazilian experts. This software has a simple, intuitive and integrated interface for detailed analysis and expert examinations of stored data (Federal Police, 2019).

The tool offers a wide range of features common in forensic software. These include image processing, file categorization, detection of encrypted files, calculation and querying of hashes, and, above all, content indexing. This last feature is the most advantageous, as it speeds up and increases the efficiency of searches (Federal Police, 2019).

2.2.3 NuDetective

NuDetective is a free forensic tool that is available only to authorities and public institutions, and was developed by criminal experts from the Brazilian Federal Police, Mateus de Castro Polastro and Pedro Monteiro da Silva Eleutério. It is used to examine data stored on electronic devices, with the aim of locating possible child exploitation and abuse materials.

It has four main functionalities: image analysis, name analysis, hash analysis, and finally, it includes video analysis in the most recent versions (Eleutério, Machado, 2011).

The tool filters images and videos using textual information, unique signatures and skin detectors. It is able to search for the file name, comparing it with a list of predefined names and phrases commonly used to share child pornography data on the Internet (Polastro, Eleutério, 2010).

By detecting suspicious files stored, the NuDetective tool uses comprehensive methods to identify them. Initially, it employs automatic nudity detection to analyze images, identifying skin pixels and applying computational geometry techniques. It then performs a linguistic analysis of file names to identify common expressions associated with pedophilia. In addition, it compares the hashes of the files with a known list of illegal hashes, called KFF (Known File Filter) (Polastro, Eleutério, 2010).

In the case of videos, it extracts optimal frame samples and applies nudity detection algorithms to analyze the visual content. These procedures are essential to identify potential cases of pornography. children's nography (Eleutério, Machado, 2011).

2.3 Cybercrimes

Over the last few decades, technology has undergone rapid development and, consequently, computers have also become increasingly faster, more efficient and smaller. Nowadays, computers and cell phones are present not only in companies, but also in the homes, hands and daily lives of people all over the world. The popularization of the Internet has allowed computer users to spread out

around the world could exchange data and information in a short space of time, making communication between machines and people faster (Eleutério, Machado, 2011).

This technological advancement has brought countless benefits to humanity, but on the other hand it also serves as a stage for various cyber crimes, which take advantage of system vulnerabilities and global connectivity to carry out illicit activities (Almeida *et al.,* 2015).

Cybercrimes encompass a variety of illicit activities, ranging from simpler actions, such as phishing and identity theft, to highly sophisticated schemes, such as financial fraud and corporate network hacking. Some of the main examples of cybercrimes include:

- Phishing – This is one of the oldest scams on the internet. According to Olivo (2010), Phishing is a technique that uses social engineering to trick victims by persuading them - those with the aim of capturing personal information and then using it in a way that causes harm to them.
- Identity theft - "Identity theft" is characterized by the simultaneous exploitation of the victim's identifying elements by the victim and the offender (Koops *et al.,* 2009).
- Malware Attacks - This type of attack involves installing malicious software on computers or networks without the user's consent. Malware can be designed to steal secure information such as passwords or banking details, damage systems, or remotely control computers to send spam or carry out other attacks. Examples of malware include viruses, worms, Trojan horses, and ransomware (Melo *et al.*, 2011).
- Ransomware - Ransomware is a type of malicious code (malware) that prevents access to files or computer systems, demanding a ransom for its release (Pinto, 2018).

2.3.1 Images of child abuse and exploitation

According to the Ministry of Health (Brazil, 2015), violence is defined as actions carried out by individuals, groups, classes or nations, which result in physical, emotional, moral and/or spiritual harm to oneself or others. Specifically, violence against children and adolescents is classified in the following ways: physical, psychological, sexual and neglect.

Brazilian legislation for the protection of children and adolescents is one of the most advanced in the world. However, indicators from a G1 survey point to an alarming statistic according to which around 41.2% of these individuals are victims of some form of violence (Garcia, Mazui and Parreira, 2023). As provided for in the Federal Constitution (Brazil, 1988), society and the State are responsible for ensuring that children and adolescents have their fundamental rights respected.

In 2008, Safernet registered 56,115 new reports (Graph 1) of images of child abuse and exploitation, "The year in which reports received by Safernet of images of child sexual abuse and exploitation on Orkut exploded. Owner of the Google platform, it signed an agreement with the MPF on July 2, and began to hand over information about criminals to the authorities" (Safernet, 2024).

In 2020, a total of 46,019 new reports were recorded (Graph 1) "First year of the COVID-19 pandemic. With social isolation, the number of connected devices and screen time increases, as well as non-face-to-face interaction between people and reports of all types of crimes to Safernet" (Safernet, 2024).

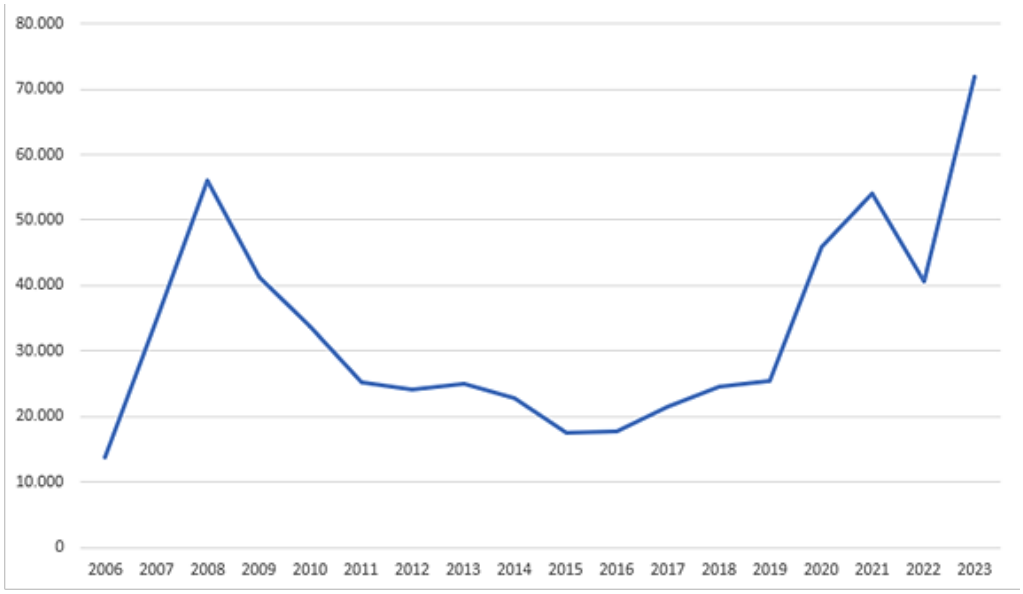
And in 2021, 53,960 new complaints were registered (Graph 1), "Second year of the COVID-19 pandemic. Social isolation continues and the number of connected devices and screen time remains high. New consecutive record of complaints received by Safernet since 2009" (Safernet, 2024).

And in 2023, 71,867 new complaints were registered (Graph 1), Safernet (2024) states that this year saw a historic record of complaints of images of child sexual abuse and exploitation. A combination of factors explains the increase:

1) the initiation of Artificial Intelligence for the creation of this type of content;
2) the illegal trade in images of nudity and sex self-generated by adolescents;
3) Large technology companies carried out mass layoffs, of teams such as: security, integrity and content moderation of platforms.

Graph 1 shows the timeline of reports of images of child sexual abuse and exploitation.

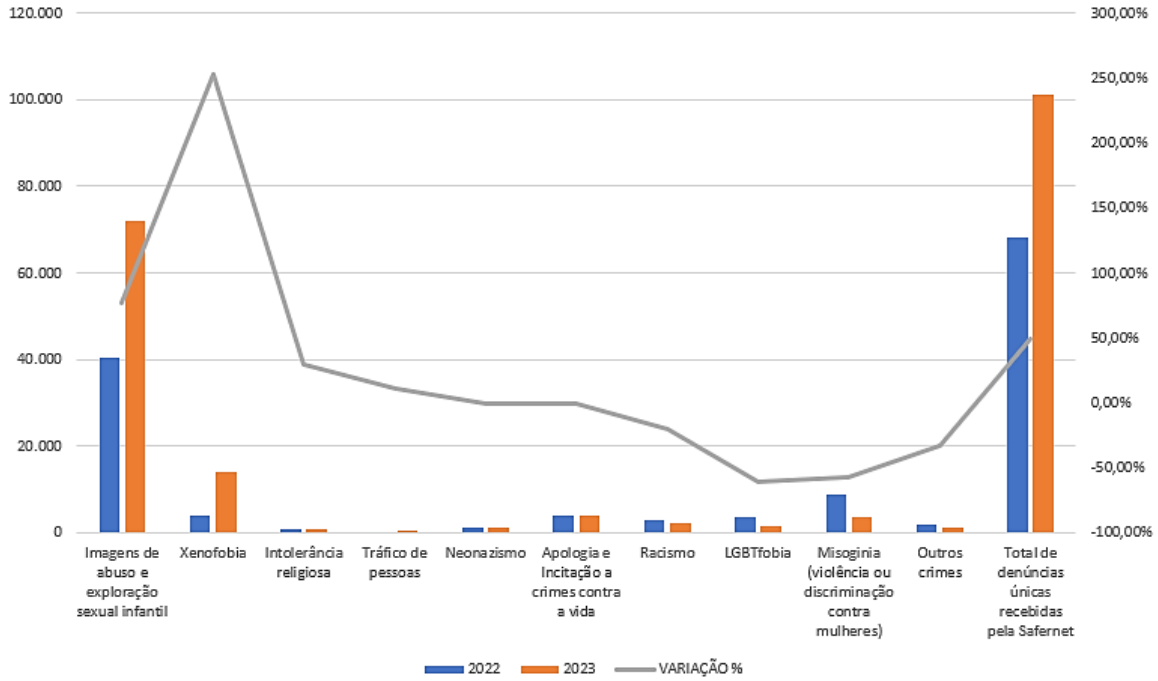
Graph 1 - Timeline.



Source: (the author, 2024)

It is possible to see in Graph 2 that during the years 2022 and 2023, images of child sexual abuse and exploitation are the type of crime that receives the most reports.

Graph 2 – New Complaints Received by Safernet, by Crime.



Source: (the author, 2024).

Provided for by Brazilian Legislation in the Statute of Children and Adolescents, according to decree no. 11,829, of November 2008, Child Pornography is a crime punishable by law for anyone who possesses, produces, reproduces, sells, discloses or publishes, by any means of communication – virtual or non-virtual -, photographs, videos, illustrations or other types of images with pornography, explicit sex scenes involving children or adolescents, or any representation of a child's sexual organs for sexual purposes or pornographic display (Brazil, 2008).

2.4 Current legislation on the protection of images and data

In Brazil, protecting the images and data of children and adolescents is a fundamental issue, and many laws deal exclusively with privacy and data security. The main laws are the Statute of Children and Adolescents described in subsection 2.4.1, the LGPD presented in subsection 2.4.2, and some specific rules and provisions of the Civil Code.

The article of the Brazilian Civil Code (Law No. 10,406/2002) also addresses the issue of image protection. It provides that the use of a person's image without their authorization or that of their legal representative may result in civil liability. In the case of minors, authorization from their parents or guardians is required for the use of their image (Brazil, 2002).

2.4.1 The provisions of the Statute of Children and Adolescents, Federal Law No. 8,069, of July 13, 1990, applicable

The Child and Adolescent Statute (ECA), Federal Law No. 8,069, of July 13, 1990, is Brazilian legislation that establishes the fundamental rights of children and adolescents, regulating their comprehensive protection.

As described in the ECA in its Art. 4, it is the duty of the family, the community, society and the public authorities to ensure with absolute priority the realization of rights relating to life, health, food, education, sport, leisure, professionalization, respect, freedom and family and community life (Brazil, 1990).

Current Brazilian legislation defines as a crime the conduct of "presenting, producing, selling, providing, disclosing or publishing, by any means of communication, including the Internet, photographs or images containing pornography or explicit sex scenes involving children or adolescents" (Brazil, 2008).

Furthermore, the ECA also provides in Art. 17 (Brazil, 1990) "The right to respect consists of the inviolability of the physical, psychological and moral integrity of children and adolescents, including the preservation of image, identity, autonomy, values, ideas and beliefs, personal spaces and objects."

While Art. 247° prohibits:

> Disclosing, in whole or in part, without due authorization, by any means of communication, the name, act or document of police, administrative or judicial proceedings relating to a child or adolescent to whom an infraction is attributed: Penalty - fine of three to twenty reference salaries, with double the amount being applied in the event of a repeat offense (Brazil, 1990, p. 1).

Therefore, such provisions aim to guarantee full protection and respect for the rights of children and adolescents, ensuring that they are treated with dignity in all circumstances.

2.4.2 Provisions of the General Data Protection Law (LGPD): Law No. 13,709/2018 applicable

The General Data Protection Law (LGPD), Law No. 13,709, came into force in September 2020. It regulates the processing of personal data, whether by individuals or legal entities, public or private, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the natural person's personality.

Regarding the division of Law No. 13,709/2018 Pinheiro (2020), says that:

> [...] is divided into 10 Chapters, with 65 articles [...]
> • Chapter I - Preliminary Provisions (articles 1 to 6).
> • Chapter II - Processing of Personal Data (arts. 7 to 16): has Section I (Requirements for Data Processing), Section II (Processing of Sensitive Personal Data), Section III (Processing of Personal Data of Children and Adolescents) and Section IV (Termination of Data Processing).
> • Chapter III - Rights of the Holder (arts. 17 to 22).
> • Chapter IV On the Processing of Personal Data by Public Authorities (arts. 23 to 32): has Section I (Rules) and Section II (Responsibility).
> • Chapter V - International Data Transfer (arts. 33 to 36).
> • Chapter VI - Personal Data Processing Agents (arts. 37 to 45): has Section I (Controller and Operator), Section II (Personal Data Processing Officer) and Section III (Responsibility and Compensation for Damages).
> • Chapter VII - Security and Good Practices (arts. 46 to 51): has Section I (Security and Data Confidentiality) and Section II (Good Practices and Governance).
>
> • Chapter VIII - Inspection (arts. 52 to 54): has Section I (Administrative Sanctions).
> • Chapter IX National Data Protection Authority (ANPD) and the National Council for the Protection of Personal Data and Privacy (arts. 55 to 59): has Section I (National Authority for the Protection of Personal Data (ANPD) and Section II (National Council for the Protection of Personal Data and Privacy) - presidential veto.
> • Chapter X - Final and Transitory Provisions (arts. 60 to 65). (Brazil, 2020, p. 9-10)

The LGPD establishes fundamental principles for the processing of personal data. According to Art. 6, Section VI guarantees transparency to holders of clear, precise and easily accessible information about the processing of their data, respecting commercial and industrial secrets. Furthermore, according to Article 6, Section VII, technical and administrative measures are required to ensure the security of personal data, protecting against unauthorized access and incidents of destruction, loss or unlawful alteration. Article 6, VIII, of the LGPD determines the adoption of preventive measures to avoid damages resulting from the processing of personal data (Brazil, 2018).

The law also pays special attention to the processing of data from children and adolescents. According to Art. 14, § 1, specific and highlighted consent from at least one parent or legal guardian is required for the processing of children's data. Art. 14, § 3, establishes that, in specific and controlled circumstances, personal data from children may be collected without consent to contact the parents or for the protection of the child, as long as they are not stored or shared with third parties without the aforementioned consent (Brazil, 2018).

These provisions of the LGPD aim to ensure that the processing of personal data is carried out in a responsible, transparent and secure manner, protecting the fundamental rights to privacy and data protection, especially for vulnerable individuals such as children and adolescents.

3. MATERIAL AND METHOD

This article will use exploratory research to analyze the literature on forensic computing tools used to combat images of child abuse and exploitation. Through this research, we aim to obtain a comprehensive understanding of the available tools and their effectiveness in combating this type of crime.

According to Leão, exploratory research:

> [...] aims to provide more information about a subject under investigation, to familiarize oneself with the phenomenon or to gain a new understanding of it, in order to be able to formulate a more precise research problem or create new hypotheses. It can also be the initial step in a research process. Exploratory studies only lead to hypotheses, they do not verify or demonstrate. (Leão, 2016, p. 14).

The bibliographic research methodology will also be adopted to collaborate in the investigation of tools.

tools. Through this approach, we seek to explore the existing literature to obtain an in-depth understanding of the available tools, their applicability and the results obtained in previous studies on the subject. Casarin says that bibliographic research:

> [...] makes use of articles, theses, dissertations, books, etc., written by other authors on the topic in question. In this type of research, it is possible to verify what has already been produced in previous studies on the subject. (Casarin, H. and Casarin, S., 2012, p. 47).

To describe the related works, the research will use the systematic literature review. For Galvão and Ricarte, the systematic literature review can be defined as:

> [...] research modality, which follows specific protocols, and which seeks to understand and give some logic to a large documentary corpus, especially by verifying what works and what does not work in a given context. It is focused on its reproducibility by other researchers, explicitly presenting the bibliographic databases that were consulted, the search strategies used in each database, the process of selecting scientific articles, the criteria for inclusion and exclusion of articles and the process of analyzing each article. It also explains the limitations of each article analyzed, as well as the limitations of the review itself. (Galvão and Ricarte, 2019, p. 58-59).

It will use the Google Scholar, CAPES Periodicals Portal and Science Direct platforms as research bases, searching the platforms for the following keywords: *forensic tools* and *exploitation of child images*, in the periods from 2018 to 2024.

Initially, 45 articles were found in the CAPES Journal Portal, of which 29 were selected for further analysis. Of these, 27 were excluded, resulting in 2 articles suitable for the final search. In Google Scholar, out of a total of 6,100 results, 100 were selected, but only 3 met the relevance criteria. In Science Direct, out of 502 initial results, 100 were analyzed, resulting in 3 articles chosen after the exclusion of 97.

Thus, 229 relevant articles were identified on the consulted platforms. However, some of these articles were excluded because they were repeated or not relevant to the research topic, thus ensuring the quality and accuracy of the selected data. Based on this initial screening, the titles and abstracts of the articles were analyzed, with the aim of identifying those that best aligned with the focus of the study. The articles considered less relevant were discarded, which resulted in the selection of 8 articles that met the previously established criteria. These final articles constitute the basis of the analysis and discussion presented in the study, which is based on the scientific contribution of the selected sources to enrich the understanding of the research topic.

4. RELATED WORKS

As described in section 2.3.1, child exploitation and abuse constitute serious violations of the fundamental rights of children and adolescents, encompassing practices such as physical, psychological, sexual violence and neglect (Brazil, 2015). Although Brazil has advanced protective legislation, including the Statute of Children and Adolescents (ECA), the country still faces high rates of child violence, with 41.2% of children and adolescents being victims of some type of abuse (Garcia, Mazui and Parreira, 2023). The NGO (Non-Governmental Organization) Safernet has recorded an alarming increase in reports of child sexual exploitation in recent years, especially during the COVID-19 pandemic, when the use of connected devices increased significantly (Safernet, 2024). In 2023, reports reached a record high historical, highlighting the urgency of strengthening the application of legislation and coordinated actions between the State and society for the comprehensive protection of minors.

Therefore, this section presents some of the main related works. For this research, the search string (*forensic tools* AND *exploitation of child images*), with the selection of works published in the period from 2018 to 2024, as described in Section 3. Table 1 “Related Articles” presents the works selected for the research.

Table 1 - Related Articles

Author/Authors	Tools	Crimes Investigated
Parizotto, Neves and Pinheiro (2022)	FTK, Encase and Autopsy.	Child pornography
Salih and Ibrahim (2023)	Stellar, FTK, Nmap, OS-FMount and Autopsy.	Phishing, Money Laundering, Bank Fraud and Exploitation childishness.
Andrade (2024)	FTK, CAINE, Autopsy, ImageJ, FotoForensics and The Sleuth Kit.	Phishing, Ransomware, Financial Fraud, Cyberbullying, DDoS Attacks and Pornography childish.
Gangwar *et al.,*(2021)	AttM-CNN and NuDetec-I had.	Child pornography
Westlake and War (2023)	PhotoDNA	Child sexual abuse
Okutan and Çebi (2019)	EnCase, Enterprise, Forensic, Fastbloc and Guidan-ce Software.	Child pornography, Malware, Trojans, Cyberterrorism, Cyberstalking and KeyLogger.
Sanchez *et al.,*(2019)	Autopsy, Forensics Toolkit, Magnet Forensics and Cellebrite.	Child pornography
Sarkara and Shukla (2023)	Autopsy, EnCase, Sleuth Kit and Nmap.	Child exploitation, Pornography celebrity scams, spreading misinformation, cyberbullying and financial fraud.

Source: the author (2024)

Parizotto, Neves and Pinheiro (2022) explore the relevance of computer forensics in crime investigation, especially in the fight against child pornography. Digital forensics allows experts to lists collect, preserve and analyze electronic evidence, which is essential for both conventional and virtual crimes, and acts as an essential support in the investigation of cases of online child exploitation, which is widely prioritized due to its severity. To conduct these investigations, the article highlights the use of specialized tools, such as FTK (Forensic Toolkit), which offers agility in data analysis, enables password recovery and performs data block recovery. Encase is widely used for duplicating device content, analyzing emails and recovering encrypted files. Another essential tool is Autopsy, a free and intuitive option that operates on Linux systems and supports analysis of multiple file systems. These tools allow users to

rites access and thoroughly examine suspicious files, track activities and collect digital evidence in a reliable and preserved manner, facilitating the judicial process in child pornography crimes and other digital crimes.

Salih and Ibrahim (2023) analyze digital forensics tools used in the collection and analysis of electronic evidence for legal purposes, covering categories such as computer, network, active, operating system, database, and email forensics. Among the main tools, they highlight Stellar and the Forensic Tool Kit (FTK) for data recovery and disk imaging, Nmap for network analysis, OSF-Mount for active analysis of RAM and logs, and Autopsy, an open source tool useful for data recovery. The application of Artificial Intelligence (AI) is also explored, especially for analyzing data from IoT devices, with algorithms such as Decision Stump and Bayes Net, the latter effective in detecting suspicious patterns in networks. Challenges such as the increase in data volume, IoT and cloud environments, and the need for advanced tools for big data are also highlighted. The article suggests the need to improve AI techniques for complex environments and develop metrics to validate the effectiveness of digital forensics tools, contributing to the understanding of the crucial role of AI in modern criminal investigation.

Andrade (2024) reviews the application of computer forensics in combating cybercrimes, highlighting the role of free tools, such as Autopsy, in combating illicit online activities, including child pornography. The study contextualizes computer forensics as essential in the collection and analysis of electronic evidence, with an emphasis on adapting to emerging technologies and legal integration to ensure digital security. In addition, the article explores the complexity of cybercrimes, addressing child pornography as one of the most serious types. This crime involves the production, sharing, and storage of images of child sexual exploitation, requiring meticulous investigations to identify the perpetrators and contain the distribution of these images. Andrade (2024) also emphasizes the need for constant updating of forensic tools and methods to ensure integrity and effectiveness in the collection of digital evidence, in addition to addressing the legal and ethical challenges that arise in conducting cyber investigations.

Gangwar*et al.,*(2021) discuss the use of computer forensics in combating cybercrime, focusing on tools to identify child sexual abuse material (*Child Sexual Abuse Material-CSAM*). It highlights the AttM-CNN model, based on deep learning, which identifies pornographic content and classifies the age of individuals, helping to detect CSAM. This model is trained with large databases, such as Pornography-2M and Juvenile-80k, to improve accuracy in identifying new or modified content. It also highlights the challenge of the large volume of digital data in investigations and the limitations of traditional approaches, such as hash detection. The application of deep neural networks is highlighted as an effective solution to speed up CSAM detection in large databases, combining pornography detection and age classification for more accurate results.

Westlake and Guerra (2023) address the application of file and folder organization and naming practices to improve the automated detection of child sexual abuse material (CSAM) on the Dark Web. The study analyzes 162 known CSAM images and their 7,289 displays on 988 sites on the Dark Web, highlighting that organization prevails over attempts at concealment, with files often organized to facilitate user access. This analysis reveals that, instead of using advanced security, operators prioritize explicit terms and structuring that facilitates the search for this material, with common patterns in URLs and file names that explicitly indicate child abuse content. They further suggest that these structuring practices could complement already used automated detection tools, such as PhotoDNA, which is based on hashing. By incorporating file and folder naming and organization patterns, the detection of previously unknown CSAM can be improved, aiding investigations. The analysis also notes that many sites mirror their content on alternative domains to maintain distance.

availability of materials in case of removal, a practice that makes it difficult to effectively combat the spread of CSAM on the Dark Web.

Okutan and Çebi (2019) propose a framework for investigating cybercrimes, especially those involving child pornography. It addresses the collection and preservation of digital evidence, data analysis, and reporting, detailing tools such as EnCase for forensic data collection and Guidance Software for monitoring and responding to threats. It also discusses the importance of security methods, such as firewalls and intrusion prevention systems, to reduce cybercrimes. The study also highlights the need for clear laws and international cooperation in combating online child pornography, as well as the updating of detection technologies. It also advocates the creation of specialized centers

and training to strengthen investigations and protect against digital crimes.

Sanchez*et al.,*(2019) explore the use of forensic tools and technologies, such as artificial intelligence (AI), to investigate child abuse material (CSAM). A survey of professionals assessed the effectiveness of these tools, which include technologies for filtering images and estimating age, facilitating the triage of large volumes of data. The study also addresses challenges, such as workload and exposure to traumatic content, and the need for more accurate tools. Autopsy is mentioned as an open-source forensic tool, but commercial options such as Magnet Forensics and Cellebrite are more common. Technologies that limit exposure to CSAM are seen as essential, although they still need to improve in accuracy and speed. The use of AI to automate detection, such as in the iCOP kit, is highlighted as increasing efficiency and reducing professional exposure. The survey concludes that continued development and collaboration between agencies are vital to address the challenges of CSAM investigations.

Sarkar and Shukla (2023) analyze the behavior of cybercrimes and effective policing strategies, highlighting everything from the definition of typologies to the creation of a framework for investigations. The study addresses the use of digital artifacts as crucial evidence to track and dismantle online crimes, including child pornography. The study emphasizes that effective digital investigations depend on appropriate methods and tools to collect, analyze, and preserve evidence, considering the complexities of crimes that cross legal boundaries. Regarding child pornography, the article highlights the challenges in identifying and processing illicit content, highlighting the need for accurate filtering tools and protection for investigators. The research reinforces the importance of advanced technologies to efficiently detect digital crimes, in addition to promoting collaboration between public and private sectors in combating these crimes.

FINAL CONSIDERATIONS

Forensic computing is a crucial area in the fight against digital crimes, especially in a scenario where cyberspace has become a stage for illicit practices, such as the dissemination of child abuse and exploitation content. In order to collect, preserve and analyze digital evidence, forensic professionals depend on technological tools that enable accurate and efficient investigations. However, the high cost of many advanced solutions limits their access, especially for organizations with budgetary constraints. In this scenario, free forensic tools emerge as important alternatives, allowing investigations to be conducted even in the face of financial limitations.

These tools, such as Autopsy, FTK, NuDetective and others, have demonstrated potential to assist in the detection, analysis and combat of criminal practices involving the production and dissemination of child abuse images. In addition, reviewed studies highlight the effectiveness of some of these tools in extracting and preserving digital evidence, which is essential for conducting investigations.

Despite the significant contributions of free tools, it is important to consider that, in many cases, they have limitations compared to paid tools, especially in terms of advanced features, technical support and updates. However, when used well and combined with good investigation practices, these tools can play a crucial role in tackling this type of crime.

Therefore, it is concluded that the adoption of free forensic tools, combined with the technical training of professionals and the development of public policies to combat child exploitation, represents a viable and necessary strategy in the current scenario. In future research, it is suggested that a practical and comparative analysis of these tools be carried out, as well as studies that evaluate their applicability in different legal and investigative contexts.

REFERENCES

ALMEIDA, Jessica*et al.***Cyber crimes.**Undergraduate Notebook - Human and Social Sciences - UNIT – SERGIPE, Aracaju, v. 2, n. 3, March, 2015. Available at: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013/1217. Accessed on: June 8, 2024.

ANDRADE, Ingrid Lima de.**Digital forensics applied to combating cybercrimes:**a review.*Focus Magazine, Belo Horizonte*, v. 17, n. 7, p. 1-27, Jul. 2024. DOI: 10.54751/revistafoco.v17n7-152. Available at: http://dx.doi.org/10.54751/revistafoco.v17n7-152. Accessed on: Nov. 15, 2024.

AUTOPSY - THE SLEUTH KIT.**Autopsy.**2003. Available at: https://www.sleuthkit.org/autopsy/. Accessed on May 8, 2024.

BRAZIL.**Constitution of the Federative Republic of Brazil of 1988.**Promulgated on October 5, 1988. Official Gazette of the Union, Brasília, DF, October 5, 1988. Available at: < https://www.planalto.gov.br/ccivil_03/constitucao/constituicaocompilado.htm >. Accessed on: June 1, 2024.

BRAZIL. Law 10,406, of January 10, 2002. Institutes the Civil Code.**Official Gazette of the Union**, Brasília, DF, January 11, 2002. Available at: < https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada. htm?ref=blog.suitebras.com >. Accessed on: May 28, 2024.

BRAZIL. Law 11,829, of November 25, 2008. Provides for the Statute of Children and Adolescents and other measures.**Official Gazette of the Union**, Brasília, DF, November 26, 2008. Available at: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Accessed on: May 25, 2024.

BRAZIL. Law 8,069 of July 13, 1990. Provides for the Statute of Children and Adolescents and other measures. Amended by Law 11,829 of November 25, 2008.**Official Gazette of the Union**, Brasília, DF, July 16, 1990. Available at: < https://www.planalto.gov.br/ccivil_03/leis/l8069compilado.htm >. Accessed on: June 1, 2024.

BRAZIL. Law No. 13,709, of August 14, 2018. General Personal Data Protection Law (LGPD).**Official Gazette of the Union**, Brasília, DF, July 6, 2020. Available at: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm>. Accessed on: June 3, 2024.

BRAZIL. Ministry of Health. Secretariat for Women's Policies. Technical Standard: Humanized Care for People in Situations of Sexual Violence with Information Recording and Evidence Collection.**Official Gazette of the Union** , Brasília, DF, 2015. Available at: <https://bvsms.saude.gov.br/bvs/publicacoes/atencao_humanizada_pessoas_violencia_sexual_norma_tecnica.pdf>. Accessed on: June 8, 2024.

CASARIN, Helen de Castro Silva; CASARIN, Samuel José.**Scientific research:**from theory to practice. Curitiba: Intersaberes, 2012.*E-book*. Available at: https://plataforma.bvirtual.com.br. Accessed on: April 19, 2024.

CHAWKI, Mohamed; DARWISH, Ashraf; KHAN, Mohammad.**Cybercrime, Digital Forensics and Jurisdiction**. London: Springer, 2015. v. 593.

ELEUTÉRIO, Pedro Monteiro da Silva;**Unraveling Computer Forensics**. New York: Routledge, 2011.

EVARIST, Thomas. **THE cybersecurity applied node scope of the SMEs.**Santarém, 2022/2023 Dissertation (Master in Web Technology and Systems Engineering) - Higher Institute of Management and Administration of Santarém. Available at: https://comum.rcaap.pt/bitstream/10400.26/49385/1/Dissertacao_tomas_evaristo.pdf. Accessed on: May 16, 2024.

RICARTE, Ivan Luiz.**SYSTEMATIC LITERATURE REVIEW:** CONCEPTUALIZATION, PRODUCTION AND PUBLICATION. Logeion: Philosophy of Information, Rio de Janeiro, RJ, v. 6, n. 1, p. 57–73, 2019. DOI 10.21728/logeion.2019v6n1.p57-73. Available at: https://revista.ibict.br/fiinf/article/view/4835. Accessed on: Apr 24, 2024.

GANGWAR, Abhishek,*et al.***AttM-CNN:**Attention and metric learning based CNN for pornography, age and Child Sexual Abuse (CSA) Detection in images.*Neurocomputing*, v. 445, p. 81–104, 2021. DOI: 10.1016/j.neucom.2021.02.056. Available at: https://doi.org/10.1016/j.neucom.2021.02.056. Accessed on: November 5, 2024.

GARCIA, Gustavo; MAZUI, Guilherme; PARREIRA, Marcelo.**Brazil recorded 202,900 cases of sexual violence against children and adolescents from 2015 to 2021, says bulletin**. Portal G1,Brasilia, May 18, 2023. Available at: < https://g1.globo.com/politica/noticia/2023/05/18/brasil-registrou-2029-mil-

cases-of-sexual-violence-against-children-and-adolescents-from-2015-to-2021-says-bulletin.ghtml>. Access on: May 13, 2024.

KOOPS, Bert-Jaap,*et al.***A typology of identity-related crime:**Information, Communication and Society. 2009. v. 12, p.1-24. Taylor & Francis Online, 2009. Available at: https://www.academia.edu/3327927/A_typology_of_identity_related_crime_conceptual_technical_and_legal_issues. Accessed on: 05 Jun. 2024.

LION, Lourdes Meireles.**Study and research methodology:**making life easier for students, teachers and researchers. 1st ed. São Paulo: Vozes, 2016.*E-book.*Available at: https://plataforma.bvirtual.com.br. Accessed on: April 19, 2024.

MARAS, Marie.**Computer forensics:**cybercriminals, laws, and evidence. 2nd ed. Burlington: Jones Bartlett Learning, 2015.

MELO, Laerte Peotta de*et al.***Minicourses of the XI Brazilian Symposium on Information Security and Computer Systems.**Brasilia: Brazilian Computer Society – SBC, 2011.*E-book.*Available at: https://books-sol.sbc.org.br/index.php/sbc/catalog/view/95/424/695. Accessed on: May 10, 2024.

MELO, Sandro.**Forensic Computing with Free Software - Concepts, Techniques, Tools and Case Studies.**New York: Routledge, 2009.

MERCURY, Rebecca.**Challenges in Forensic Computing.**Communications of the ACM, ACM, v. 48, p. 17- 21, 01 Dec. 2005. Available at: https://dl.acm.org/doi/10.1145/1101779.1101796. Accessed on: 20 Apr. 2024. OLIVO, Cleber Kiel.**Feature evaluation for email phishing detection**. Curitiba, 2010 Dissertation (Master's in Computer Science) - Pontifical Catholic University of Paraná. Available at: https://www.inf.ufpr.br/lesoliveira/download/CleberOlivoMSC.pdf. Accessed on: May 10, 2024.

OKUTAN, Ayşe; ÇEBİ, Yalçın.**A Framework for Cyber Crime Investigation**.*Procedia Computer Science*, Izmir, v. 158, p. 287-294, 2019. DOI: 10.1016/j.procs.2019.09.054. Available at: https://doi.org/10.1016/j.procs.2019.09.054. Accessed on: November 1, 2024.

PARIZOTTO, Lucas Serafim; NEVES, Antonio Lucas; PINHEIRO, Nicolli Rinaldi.**The importance of computer forensics in crime investigation.***In: II FatecSeg Congress - Fatec Information Security Congress*, November 17 and 18, 2022. DOI: 123456789/12551. Available at: https://ric.cps.sp.gov.br/handle/123456789/12551. Accessed: November 10, 2024.

PINHEIRO, Patricia Peck.**Protection of Personal Data:**comments on Law No. 13,709/2018. 2nd ed. São Paulo: Saraiva, 2020.

PINTO, A.**Ransomware:**a rising cyber threat.*In:*BRAZILIAN CONGRESS ON INFORMATION SECURITY AND COMPUTATIONAL SYSTEMS, 1., 2018, Santa Maria.**Proceedings of the Brazilian Congress on Information Security and Computer Systems.**Santa Maria: UFSM, 2018.

COLLINS, Matthew;**NuDetective:**A forensic tool to help combat child pornography through automatic nudity detection.*In*: Workshops on Database and Expert Systems Applications, 2010, p. 349–353. Available at: https://doi.org/10.1109/DEXA.2010.74. Accessed on: 10 May 2024.

FEDERAL POLICE.**IPED Project**. Brasília, 2019. Available at: https://github.com/sepinf-inc/IPED. Accessed on: May 16, 2024.

SAFERNET.**Safernet receives historic record of new reports of images of child sexual abuse and exploitation on the internet.**SAFERNET, 2024. Available at: https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual. Accessed on: May 8, 2024.

SALIH, Karam Muhammed Mahdi; IBRAHIM, Najla Badi.**Digital forensic tools:**a literature review.*Journal of Education and Science, Mosul*, v. 32, n. 1, p. 109-124, Mar. 2023. DOI: 10.33899/edusj.2023.137420.1304. Available at: http://dx.doi.org/10.13140/RG.2.2.10098.48321. Accessed on: Nov. 15, 2024.

SANCHEZ, Laura,*et al.***A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)**.*Digital Investigation*, v. 29, p. S124-S142, 2019. DOI: 10.1016/j.diin.2019.04.005. Available at: https://doi.org/10.1016/j. diin.2019.04.005. Accessed on: November 1, 2024.

SARKAR, Gargi; SHUKLA, Sandeep K.**Behavioral analysis of cybercrime:**Paving the way for effective policing strategies.*Journal of Economic Criminology*, v. 2, 2023. DOI: 10.1016/j.jeconc.2023.100034. Available at: https://doi.org/10.1016/j.jeconc.2023.100034. Accessed on: November 3, 2024.

SILVA FILHO, Wilson.**Cybercrimes and Computer Forensics**. *In:*XVI BRAZILIAN SYMPOSIUM ON INFORMATION AND COMPUTATION SYSTEMS SECURITY, n. 1. 2016. Proceedings [...] Niterói: Brazilian Computer Society, 2016, p. 44-81. Available at: https://sbseg2016.ic.uff.br/pt/files/ MC2-SBSeg2016.pdf. Accessed on: May 2, 2024.

WESTLAKE, Bryce; WAR, Enrique.**Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the Dark Web**.*Forensic Science International: Digital Investigation*, v. 47, p. 301620, 2023. DOI: 10.1016/j.fsidi.2023.301620. Available at: https://doi. org/10.1016/j.fsidi.2023.301620. Accessed on: November 8, 2024.