v. 13, n. 1, p. 156-167, 2024
ISSN 2237-9223

REVISTA BRASILEIRA DE CRIMINALÍSTICA

DOI: http://dx.doi.org/10.15260/rbc.v13i1.759

Princípios de Localidade de Referência: proposta de redução do escopo de análise pericial em casos envolvendo violência contra menores no ambiente de cibernético

G.P. Vilar [a], A.G. Souza [a], M. Bushatsky [a], R.I.C. Campello [a], E.P. Soriano [a], A.C. Almeida [a], A.A. Antunes [a], G.G.P. Petraki [a,*]

[a] *Mestrado de Pericias Forenses, Universidade de Pernambuco, PE, Brasil.*

**Endereço de e-mail para correspondência: gabriela.porto@upe.br. Tel.: +55-819923-23241.*

Recebido em 12/07/2023; Revisado em 20/02/2024; Aceito em 20/02/2024

Resumo

Na análise forense de dispositivos computacionais, os profissionais enfrentam um volume cada vez maior de dados para examinar. As unidades de armazenamento são os principais repositórios permanentes utilizados nessas análises e estão ficando cada vez maiores, armazenando uma quantidade igualmente grande de informações. Uma opção para lidar com essa situação é a utilização dos princípios de localidade de referência, que se baseiam nos fundamentos de recentidade, frequência e agrupamento de recursos, com o objetivo de reduzir o tempo necessário ou o escopo espacial dos exames periciais. Para este trabalho, foram utilizados os legados do cientista da computação Peter Denning, que percebeu uma tendência de concentração temporal em áreas de memória menores, o que possibilitou a construção de uma hierarquia de memórias combinando várias tecnologias distintas para melhorar o desempenho global do sistema a um custo relativamente baixo. Para aplicar a técnica proposta, foram usadas mídias de armazenamento com estruturas do sistema operacional Windows e artefatos consolidadores de registros de recentidade e frequência de acessos a arquivos, pastas e programas. Os resultados obtidos mostram-se promissores para a redução do acúmulo de equipamentos computacionais à espera de análises periciais nas centrais de custódia brasileiras, promovendo, após a aplicação do método reducionista proposto neste trabalho, um decremento de 759.161 arquivos ou pastas para analisar para 12.597 pastas ou arquivos inicialmente analisados. Analisando um subconjunto representativo dos dados originais, foi possível concluir sobre a materialidade, autoria e dinâmica das condutas previstas no Estatuto da Criança e do Adolescente, o que permitiu reduzir o tempo de análise pericial e consequente entrega do laudo pericial.

Palavras-Chave: Redução de escopo; Localidade de referência; Encurtamento temporal.

Abstract

In the forensic analysis of computer devices, professionals are facing an increasingly large volume of data to examine. Storage units are the main permanent repositories used in these analyses and are becoming larger and storing an equally large amount of information. One option for dealing with this situation is the use of the principles of reference locality, which are based on the fundamentals of recency, frequency and grouping of resources, with the aim of reducing the time required or spatial scope of forensic examinations. For this research, the legacies of the computer scientist Peter Denning were used, who noticed a trend of temporal concentration in smaller memory areas, which enabled the construction of a memory hierarchy combing several distinct technologies to improve the overall performance of the system at a relatively cost. To apply the proposed technique, storage media with Windows operating system structures and consolidating artifacts of recency and frequency of access to files, folders and programs were used. The results obtained are promising for reducing the accumulation of computer equipment awaiting forensic analysis in Brazilian custody warehouses, promoting, after applying the reductionist method proposed in this work, a reduction from 759,161 files or folders to analyze to 12,597 folders. By analyzing a representative subset of the original data, it was possible to conclude about the materiality, authorship, and dynamics of the conducts provided for in the Statute of the Child and Adolescent, which made it possible to reduce the time of expert analysis and consequent delivery of the expert report.

Keywords: Scope reduction. Reference locality. Time reduction.

1. INTRODUÇÃO

A formação de peritos é fundamental para o combate à violência infantojuvenil no ambiente cibernético, especialmente em relação a crimes relacionados com pornografia infanto-juvenil. Um trabalho acadêmico que aborde esse tema pode trazer contribuições valiosas para a formação de peritos, fornecendo informações relevantes sobre a natureza e complexidade desses crimes, bem como as técnicas e ferramentas utilizadas para investigá-los. Além disso, este trabalho acadêmico aborda aspectos legais e éticos envolvidos na investigação de crimes de violência sexual contra o esse público, destacando a importância da atuação dos peritos dentro dos limites legais e garantindo a preservação da privacidade e dos direitos das vítimas e dos acusados.

O termo "pedofilia" é frequentemente utilizado de forma incorreta e imprecisa em contextos legais. Na verdade, a pedofilia é considerada uma parafilia, que se caracteriza pela atração sexual por crianças e adolescentes.

Entretanto, do ponto de vista jurídico, o termo "pedofilia" não é utilizado para descrever um crime em si, mas sim para descrever uma característica psicológica do agressor. O crime em questão é a exploração sexual do público menor de 18 anos, que pode envolver diferentes tipos de condutas, tais como a produção, distribuição, posse ou consumo de material pornográfico envolvendo crianças.

Portanto, embora o termo "pedofilia" possa ser utilizado para descrever a motivação ou a atração sexual do agressor, ele não é um termo jurídico preciso e não deve ser confundido com o próprio crime de exploração sexual de menores. É importante que profissionais do direito e da justiça criminal utilizem terminologia precisa e adequada para descrever esses crimes, a fim de garantir uma adequada investigação, acusação e punição dos responsáveis.

Existem diversas críticas internacionais em relação ao enfrentamento dos crimes de violência no ambiente cibernético brasileiro. Uma das principais críticas promovidas pelo relatório do Departamento de Estado dos Estados Unidos sobre o Tráfico de Pessoas em 2021 [1] é a falta de investimento em tecnologia e recursos humanos para combater esse tipo de crime. Segundo esse relatório, "o Brasil continua a enfrentar desafios significativos no combate ao tráfico de pessoas e à exploração sexual de vulneráveis, incluindo o tráfico sexual online". O relatório também aponta a falta de recursos e de pessoal treinado como um problema para a efetividade das operações policiais e para a proteção das vítimas.

Outra crítica é em relação à falta de cooperação internacional. O relatório da Organização dos Estados Americanos (OEA) [2] sobre a exploração sexual de crianças e adolescentes na América Latina e no Caribe em 2019 aponta que "a cooperação regional e internacional é limitada, resultando em lacunas na capacidade de identificar, investigar e processar os autores de crimes sexuais online".

Além disso, a legislação brasileira tem sido criticada por especialistas por não ser suficientemente abrangente e por não contemplar todas as formas de exploração sexual no ambiente cibernético. De acordo com um estudo da organização Safernet Brasil em parceria com a Childhood Brasil [3], a falta de uma lei específica para criminalizar a produção, distribuição e posse de material de exploração sexual do público infantojuvenil na internet dificulta a identificação e punição dos autores desses crimes. No Brasil, temos o Estatuto da Criança e do Adolescente [4] que define as crianças e os adolescentes como sujeitos de direitos, em condição peculiar de desenvolvimento, que demandam proteção integral e prioritária por parte da família, sociedade e do Estado.

Os exames periciais em sistemas operacionais podem ser fundamentais para investigações de crimes relacionados à violência contra crianças e adolescentes no ambiente cibernético. Por meio desses exames, é possível recuperar e analisar informações contidas em dispositivos eletrônicos, como computadores e celulares, que possam comprovar a prática desses crimes.

Os peritos podem utilizar técnicas específicas de análise forense para encontrar evidências de acesso a conteúdo ilegal envolvendo o público infantojuvenil, como imagens e vídeos de pornografia. Além disso, é possível identificar comunicações entre suspeitos e vítimas, como conversas em redes sociais ou aplicativos de mensagens, que possam indicar a prática de crimes como aliciamento e exploração sexual.

A redução de escopo de trabalho em análises periciais de informática é uma técnica que visa a obtenção de resultados mais céleres, sem prejudicar a qualidade e confiabilidade das análises periciais. O objetivo é concentrar os esforços do perito nos pontos mais relevantes para a investigação, excluindo itens menos importantes ou que não apresentam informações úteis para a apuração do fato. Com isso, é possível reduzir o tempo necessário para realizar a análise, tornando o processo mais eficiente e ágil.

Essa metodologia é especialmente importante no contexto de investigações de crimes no ambiente cibernético, uma vez que o grande volume de informações e a complexidade dos sistemas computacionais podem tornar a análise pericial muito demorada e onerosa.

Ao utilizar a redução de escopo, o perito pode se concentrar nos pontos mais críticos e relevantes, como arquivos de imagem e vídeo, registros de navegação na

internet, conversas em aplicativos de mensagens, entre outros. Dessa forma, é possível obter resultados mais rapidamente e contribuir para o sucesso das investigações.

No entanto, é importante ressaltar que a redução de escopo não deve ser aplicada de forma indiscriminada, e sim de maneira criteriosa e embasada em conhecimentos técnicos sólidos. O perito deve avaliar cuidadosamente quais itens podem ser excluídos sem prejudicar a investigação, e quais são essenciais para a análise pericial.

Além disso, é importante destacar que a redução de escopo não substitui a necessidade de uma análise pericial completa e detalhada em casos mais complexos e que exijam uma investigação mais aprofundada. Nesses casos, a aplicação da técnica pode ser útil para agilizar o processo, mas é importante que o perito esteja preparado para realizar análises mais extensas e detalhadas quando necessário.

Diante do exposto, o objetivo desse trabalho foi aplicar os princípios da localidade de referência espacial e temporal em análises periciais que envolvam artefatos tecnológicos em ambientes regidos pelo Sistema Operacional Windows, mensurando ganhos e perdas na confecção de análise forense.

2. MATERIAIS E MÉTODOS

A investigação forense é uma área crucial para a justiça, especialmente em casos que envolvem crimes cibernéticos. Para garantir a efetividade dos processos de investigação, é fundamental que se utilize *hardware* e *software* especializados em análises forenses.

O *hardware* utilizado em análises forenses geralmente inclui ferramentas como dispositivos de armazenamento externo, adaptadores de interface, duplicadores de disco rígido e ferramentas de imagem de disco.

Por outro lado, o *software* especializado em análises forenses é responsável por extrair, analisar e interpretar os dados coletados pelo hardware. Esses *softwares* são projetados para identificar e extrair dados de arquivos, bancos de dados, registros de sistema, dispositivos móveis e outras fontes, permitindo que os peritos identifiquem rapidamente informações relevantes para o caso em questão. Além disso, os *softwares* de análise forense geralmente incluem recursos de visualização de dados e ferramentas de relatório, permitindo que os peritos apresentem suas descobertas de forma clara e concisa aos tribunais.

2.1. MATERIAIS

2.1.1 Unidades de armazenamento

Os testes de aplicabilidade das técnicas tradicional e reducionista recaíram sobre 09 (nove) cópias forenses de unidades de armazenamento que possuíam o sistema operacional Windows, obtidas a partir de buscas e apreensões promovidas pela Polícia Federal brasileira, cuja autorização de acesso e respeito aos preceitos internos da instituição Polícia Federal, bem como o respeito ao Estatuto da Criança e do Adolescente e à Lei Geral de Proteção de Dados [5] foram respeitados.

2.1.2 Hardware

Para processamento foi utilizado um computador modelo Z2 da marca HP com as seguintes especificações de armazenamento e memória:

- Processador: Intel Xeon E-2100 ou E-2200 de 9ª geração dotado de 48 núcleos.
- Memória RAM: 96 GB DDR4 ECC (Erro de Correção de Código) de 2666 MHz.
- Armazenamento: Disco rígido (HDD) de 9 TB e unidade SSD de 2 TB.
- Sistema operacional: Windows 11.

2.1.3. Software

Para a criação de cópias forenses, montagem de arquivos de imagem e exportação de conteúdo, foi utilizada a ferramenta AccessData® FTK® Imager, disponível em https://www.exterro.com/ftk-imager. Já para a indexação e processamento das unidades de armazenamento, foi utilizada a versão 4.1 da ferramenta IPED, disponível para download na rede social GitHub do Serviço de Perícias em Informática do Instituto Nacional de Criminalística, disponível em https://github.com/sepinf-inc/IPED.

2.2. MÉTODOS

2.2.1 Método Tradicional

Adotando a metodologia tradicional, os trabalhos se iniciaram com a confecção de cópia forense das 09 (nove) unidades questionadas para 09 (nove) arquivos imagens que formaram as cópias exatas em formato bruto ou RAW das unidades forenses sobre as quais residiam as suspeitas de ocorrência de atividades criminosas.

Uma cópia forense de dados é uma réplica exata e bit a bit de um dispositivo de armazenamento de dados, como um disco rígido, um pendrive ou um cartão de memória. Essa cópia é realizada de forma a garantir a preservação das informações contidas no dispositivo original, sem modificá-las ou apagá-las. Ela é importante em investigações criminais que envolvem a análise de dispositivos de armazenamento de dados, pois permite que os peritos possam trabalhar com uma cópia do dispositivo, sem comprometer a integridade das informações originais.

Tabela 1. Ferramentas utilizadas no processamento das provas obtidas para produção da prova pericial em crimes cibernéticos contra a criança e adolescente no Grupo de Perícias de Informática do Setor Técnico Científico da Superintendência Regional da Polícia Federal no Estado da Paraíba.

Ferramenta	Funcionalidade	Distribuidor	Disponibilização
FTK Imager 4.3.1.1	Produção de cópias forenses de unidades de armazenamento de dados	Exterro	https://www.exterro.com/ftk-imager
IPED 4.0.4	Indexação e processamento de evidências digitais	SEPINF-INC, Luís Nassif	https://github.com/sepinf-inc/IPED
ShellBagsViewer 1.30	Interpretação do Registro do sistema operacional Windows na funcionalidade de personalização de visualização de pastas.	Nir Sofer	https://www.nirsoft.net/
JumpListsViewer 1.16	Interpretação da funcionalidade de menus acessíveis através dos ícones dos aplicativos contidos na barra de tarefas do sistema operacional Windows, principalmente na recentidade e frequência de acessos.	Nir Sofer	https://www.nirsoft.net/
UserAssistViewer 1.02	Interpretação do Registro do sistema operacional Windows nas regiões relacionadas ao registro dos softwares mais recentemente executados.	Nir Sofer	https://www.nirsoft.net/
ThumbCacheViewer	Acesso e visualização dos bancos de dados de miniaturas de arquivos visualizados no explorador de arquivos do sistema operacional Windows.	Eric Kutcher	https://erickutcher.github.io/

A cópia forense foi realizada utilizando o software FTK Imager, já descrito na Tabela 1. O processo visou à garantia de integridade dos dados originais. Nesse processo de cópia, houve duplicação exata de todos os bits do dispositivo, incluindo as informações que foram apagadas ou que não são acessíveis por meio do sistema operacional. Após o término dessa cópia forense, todo o trabalho se desenvolveu sobre as cópias, buscando por informações relevantes que possam ajudar na investigação e preservando-se as unidades de armazenamento questionadas/originais.

O processamento e análise dessa cópia forense de uma unidade de armazenamento de dados é uma das etapas mais importantes em um exame pericial de informática, pois é a partir dessa cópia que o perito poderá identificar e analisar as informações contidas na unidade de armazenamento, sem correr o risco de modificar ou apagar dados originais. Essa análise pode ser dividida em algumas etapas básicas, como:

Verificação da integridade da cópia: Aqui verificamos se a cópia forense foi feita corretamente e se é uma réplica exata da unidade de armazenamento questionada. Isso é importante para garantir que as informações contidas na cópia são confiáveis e não foram modificadas durante o processo de cópia.

Identificação dos sistemas de arquivos: a próxima etapa é identificar os sistemas de arquivos presentes na unidade de armazenamento. Isso permite que o perito possa entender como os dados estão organizados na unidade de armazenamento e possa recuperar informações importantes.

Busca por dados relevantes: o perito realiza buscas em todo o conteúdo da cópia forense para encontrar informações relevantes para a investigação. Isso pode incluir busca por palavras-chave, endereços de e-mail, nomes de arquivos, metadados[1], entre outros.

Análise de metadados: os metadados contidos nos arquivos podem fornecer informações valiosas, como data e hora da criação, modificação e acesso de um arquivo. A análise desses metadados pode ajudar o perito a reconstituir a sequência de eventos que levaram à criação ou modificação de um arquivo.

Recuperação de dados apagados: em muitos casos, o perito pode recuperar dados que foram apagados da unidade de armazenamento. Isso pode incluir arquivos inteiros ou partes de arquivos que foram apagados, mas que ainda podem ser encontrados nos setores desalocados da unidade de armazenamento.

Análise de artefatos: artefatos são informações que ficam armazenadas no dispositivo devido à sua utilização, e que podem fornecer informações importantes, como histórico de navegação na internet, lista de programas instalados, pastas acessadas,

[1] Informações descritivas e estruturais que fornecem detalhes sobre um arquivo, como seu nome, tipo, tamanho, data de criação e modificações, autor, localização, entre outros dados

programas executados, entre outros. A análise desses artefatos pode ajudar a compreender como o dispositivo foi utilizado e quais foram as ações realizadas pelo usuário.

Na etapa de busca por dados relevantes acima descrita, esbarramos em um problema crescente que é o aumento do número de pastas e arquivos contidos nas unidades de armazenamento.

É difícil fornecer um número exato de arquivos e pastas contidos em uma instalação padrão do Windows 10 ou Windows 11, pois o número pode variar dependendo de muitos fatores, como a edição do sistema operacional instalada, as atualizações instaladas e os programas adicionais instalados. No entanto, estima-se que uma instalação padrão do Windows 10 possa conter mais de 100.000 arquivos e pastas em sua unidade de armazenamento, enquanto uma instalação padrão do Windows 11 pode ter um número similar ou um pouco maior, já que o sistema operacional é uma atualização do Windows 10 e tende a manter uma estrutura de arquivos semelhante. Esse número pode aumentar consideravelmente quando se adicionam programas, drivers e outros softwares.

2.2.2. Método Reducionista

Como já dito, Peter Denning [5] é um renomado cientista da computação que contribuiu significativamente para o campo da arquitetura de computadores. Em seus estudos, ele desenvolveu os princípios da localidade de referência temporal e espacial, que se tornaram fundamentais para o design de *caches* - uma memória de alta velocidade que fica localizada entre a memória principal (RAM) e a unidade central de processamento (CPU) em um computador. Sua função é armazenar temporariamente os dados mais utilizados pelo processador, para que possam ser acessados com mais rapidez e eficiência - e sistemas de memória em computadores. Esses princípios serão considerados na aplicação da metodologia reducionista proposta neste trabalho.

O conceito de Localidade Temporal destaca que, quando uma determinada região da memória foi acessada recentemente, é altamente provável que ela seja acessada novamente em um futuro próximo. Isso significa que há uma tendência dos programas em revisitar locais específicos da memória em curtos intervalos de tempo. Esse princípio é crucial para a eficácia de estruturas de cache. Por exemplo, se um programa está iterando por um conjunto de dados, os elementos desse conjunto podem ser armazenados no cache após o primeiro acesso. Assim, se o programa precisar acessar esses dados novamente em breve, a recuperação será mais rápida devido à presença deles no cache.

Já a Localidade Espacial refere-se à observação de que, uma vez que um determinado endereço de memória foi referenciado, é provável que as localidades de memória próximas a esse endereço também sejam referenciadas em um futuro próximo. Em outras palavras, há uma tendência de acessar dados em blocos contíguos de memória. Um exemplo prático da Localidade Espacial é quando um programa acessa um elemento de um vetor. Se, por exemplo, o programa acessa o elemento na posição 100 do vetor, é provável que ele também acesse os elementos adjacentes, como os das posições 101, 102 e assim por diante. Estratégias de pré-busca (pre-fetching) de dados adjacentes podem ser implementadas para otimizar esse padrão de acesso e melhorar a eficiência do sistema de memória.

Ao estabelecer esses princípios, Peter Denning [6] preconizou que os sistemas de memória e *caches* deveriam ser projetados para aproveitar a localidade de referência temporal e espacial. Isso pode ser feito por meio de técnicas como o pré carregamento de dados em *caches* e a utilização de algoritmos de substituição de *cache* que levam em conta a localidade de referência.

Com a utilização desses princípios, é possível melhorar significativamente o desempenho dos sistemas de computação, reduzindo o tempo necessário para acessar dados em memória e caches e aumentando a eficiência no uso de recursos de hardware.

O processo de redução de escopo em Sistemas Operacionais Windows, baseado nos princípios da localidade de referência, pode ser aplicado a objetos de exame e abrange principalmente quatro áreas.

1. A recentidade e a frequência de acesso às pastas do sistema através do artefato *Shellbags*.
2. A recentidade e a frequência de leitura ou escrita de arquivos de usuário através do artefato *Jump Lists*.
3. A recentidade e a frequência de execução de programas através do artefato *User Assists*.
4. Acesso ao acervo de miniaturas de arquivos de imagem geradas pelo próprio Sistema operacional Windows através do software *ThumbCacheViewer*.

Essas áreas foram examinadas pelas ferramentas contidas na Tabela 1 aplicadas sobre os artefatos contidos na Tabela 2.

Em complemento à descrição sucinta contida nno parágrafo acima, segue uma ampliação narrativa das funcionalidades descritas na Tabela 2.

Tabela 2. Relação de artefatos presentes nos sistemas operacionais Windows analisados no método reducionista e respectivas finalidades.

Artefato	Finalidade
Shellbags	Informações armazenadas pelo sistema operacional Microsoft Windows sobre as pastas acessadas pelo usuário através do Windows Explorer.
Jump Lists	Recurso do sistema operacional Microsoft Windows que fornece um menu de atalhos para os arquivos usados recentemente/frequentemente pelos aplicativos.
User Assists	Recurso do sistema operacional Microsoft Windows que fornece informações sobre os aplicativos que foram executados pelo usuário em um determinado sistema.
Thumbs	Pasta oculta do sistema operacional Microsoft Windows que armazena miniaturas de imagens, vídeos e outros tipos de arquivos multimídia.

Shellbags é um termo utilizado para se referir a uma funcionalidade do sistema operacional Windows que armazena informações sobre pastas abertas pelo usuário, incluindo sua localização, tamanho e configurações de visualização. Essas informações são armazenadas no registro do Windows e são usadas pelo sistema operacional para restaurar a aparência e a posição das pastas quando elas são abertas novamente. Se mostram parte importante da interface do usuário desse sistema operacional, pois permitem que os usuários personalizem a aparência e o comportamento das pastas em seus computadores. No entanto, essas informações também podem ser usadas por profissionais de segurança cibernética para entender melhor a atividade do usuário e determinar se houve alguma atividade suspeita ou maliciosa em um determinado sistema.

Por esse motivo, as *Shellbags* também são consideradas uma fonte valiosa de evidências digitais em investigações forenses de computadores que envolvem a análise da atividade do usuário. Os examinadores forenses podem usar as informações das *Shellbags* para reconstruir a atividade do usuário e determinar quais pastas foram acessadas e quando. Um dos maiores benefícios é a redução de escopo de pastas a serem analisadas: em vez de analisar todas as pastas do sistema, que são dezenas de milhares, passa a analisar algumas dezenas ou centenas.

Seguindo adiante no processo de redução de escopo, procedeu-se a uma busca pelos últimos arquivos e pastas acessados pelo usuário. Os artefatos que nos oferece esse conjunto de informações são as *Jump Lists*.

Jump Lists são uma funcionalidade do sistema operacional Windows que fornecem um atalho conveniente para arquivos e pastas frequentemente acessados. Eles aparecem como lista de itens quando um usuário clica com o botão direito do mouse em um ícone na barra de tarefas ou no menu Iniciar – Figura 1.

As *Jump Lists* geralmente exibem os arquivos e pastas mais recentemente ou frequentemente acessados pelo usuário, bem como opções para abrir um item com um programa específico ou fixar um item na lista para facilitar o acesso posterior. São uma ferramenta útil para aumentar a produtividade do usuário, permitindo que eles acessem facilmente os arquivos e pastas usados.

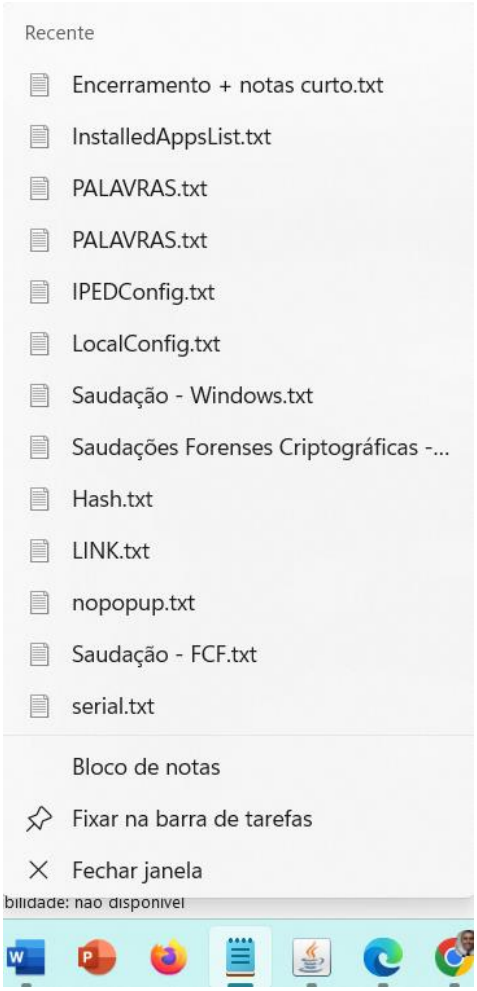

Figura 1. Visualização de uma Jump List relacionada com o Bloco de Notas, com exibição dos itens mais recentes acessados pelo programa.

No entanto, assim como as *Shellbags*, as *Jump Lists* também podem fornecer evidências valiosas em investigações forenses de computadores, permitindo que os examinadores identifiquem quais arquivos e pastas foram acessados pelo usuário e em que momento. Um dos maiores benefícios é a redução de escopo de arquivos, endereços de internet e pastas a serem analisadas: em vez de analisar todos os arquivos, endereços de internet ou pastas contidos no sistema, analisa-se apenas um subconjunto desse montante.

No tocante aos programas em execução, o *User Assist* é um recurso do sistema operacional que rastreia a execução de programas por parte dos usuários. Ele registra as informações sobre os programas que foram executados, a frequência de uso e a data da última

execução. Essas informações são usadas pelo sistema operacional para exibir os programas mais frequentemente usados no menu Iniciar e em outras áreas do sistema, e para personalizar o comportamento do sistema de acordo com as preferências do usuário.

O acesso ao acervo de miniaturas de arquivos de imagem geradas pelo próprio Sistema operacional Windows pode ser obtido pelo artefato *Thumbnails*, que são pequenas imagens em miniatura, armazenadas em bancos de dados específicos, que representam o conteúdo de arquivos de imagem, vídeo ou outros tipos de arquivos suportados pelo sistema operacional.

As miniaturas são geradas automaticamente pelo Windows para permitir que o usuário visualize o conteúdo de um arquivo sem precisar abri-lo. As miniaturas são armazenadas em bancos de dados ocultos do sistema. No entanto, é importante notar que as miniaturas podem conter informações que podem ser usadas em investigações forenses para recuperar informações sobre arquivos que foram visualizados pelo usuário, mesmo que estes já tenham sido apagados ou resida em unidades de armazenamento removíveis.

3. RESULTADOS

3.1. Aplicação do Método Tradicional

Inicialmente foram realizados o levantamento e a identificação de 09 (nove) unidades de armazenamento, obtidas através de cumprimentos de mandados de busca e apreensão e enviadas para exame no setor técnico-científico da Superintendência Regional de Polícia Federal no Estado da Paraíba nos anos de 2022 e 2023.

Em seguida, por meio de técnicas forenses apropriadas, essas unidades foram duplicadas. Esse processo de duplicação consiste na realização de cópia integral das unidades de armazenamento originais para outras mídias de armazenamento. Como medida de segurança, os exames foram realizados sobre as cópias, preservando-se o original.

Procedeu-se então ao processamento e à indexação dos arquivos com o software Indexador e Processador de Evidências Digitais (IPED), permitindo buscas, em todo o conteúdo recuperado e extraído, por palavras-chave, tipos e formatos de arquivo, dentre outros. Cabe salientar que esse processo atingiu não apenas os arquivos diretamente acessíveis, mas também aqueles previamente apagados que puderam ser recuperados, total ou parcialmente, através de técnicas de *data carving*[2] - Figura 2.

Algumas das técnicas mais comuns de data *carving* incluem:

Análise de cabeçalho: essa técnica envolve a análise do cabeçalho do arquivo para identificar o tipo e o formato do arquivo. Essa informação é usada para ajudar a recuperar os dados.

Assinatura de arquivo: essa técnica envolve a busca por assinaturas únicas de arquivos que indicam o início ou o final de um determinado arquivo. Essas assinaturas são usadas para ajudar a identificar e recuperar arquivos específicos.

Entropia: essa técnica envolve a análise de padrões de entropia dentro do dispositivo de armazenamento. Os dados com alta entropia são mais difíceis de recuperar, enquanto dados com baixa entropia são mais fáceis de identificar e recuperar.

Análise de fragmentos: essa técnica envolve a análise de fragmentos de arquivos que foram danificados ou excluídos. Os fragmentos são reunidos para ajudar a recuperar o arquivo original.

Análise de setores: essa técnica envolve a análise de cada setor do dispositivo de armazenamento em busca de dados que possam ser recuperados. Essa técnica é mais demorada do que as outras técnicas, mas pode ser útil quando outras técnicas não funcionam.

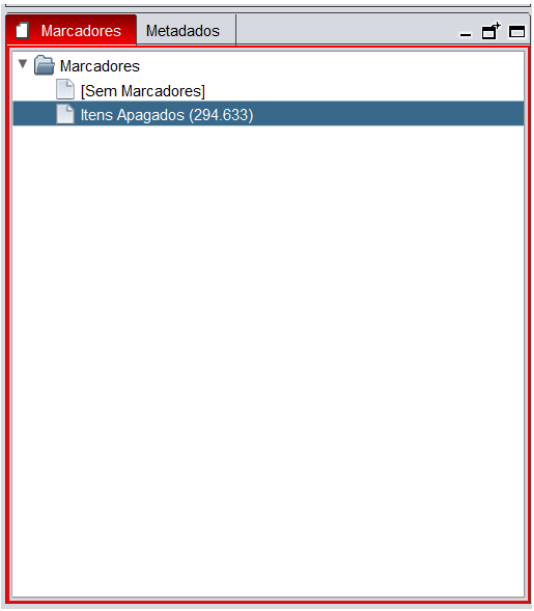

Figura 2. Marcador quantitativo dos arquivos apagados que puderam ser recuperados pelas técnicas de *data carving*, pela ferramenta IPED, totalizando 294.633 arquivos nas 09 (nove) cópias forenses.

Após o processamento, etapa em que foram aplicadas as técnicas de *data carving*, seguimos para a técnica de indexação, onde os conteúdos são agrupados por natureza e funcionalidade. O resultado combinado das etapas de processamento e indexação pode ser visualizado na Figura 3.

[2] Processo de recuperação de dados que envolve a extração de arquivos de um dispositivo de armazenamento que foram excluídos, corrompidos ou danificados através de técnicas de análise de dados.

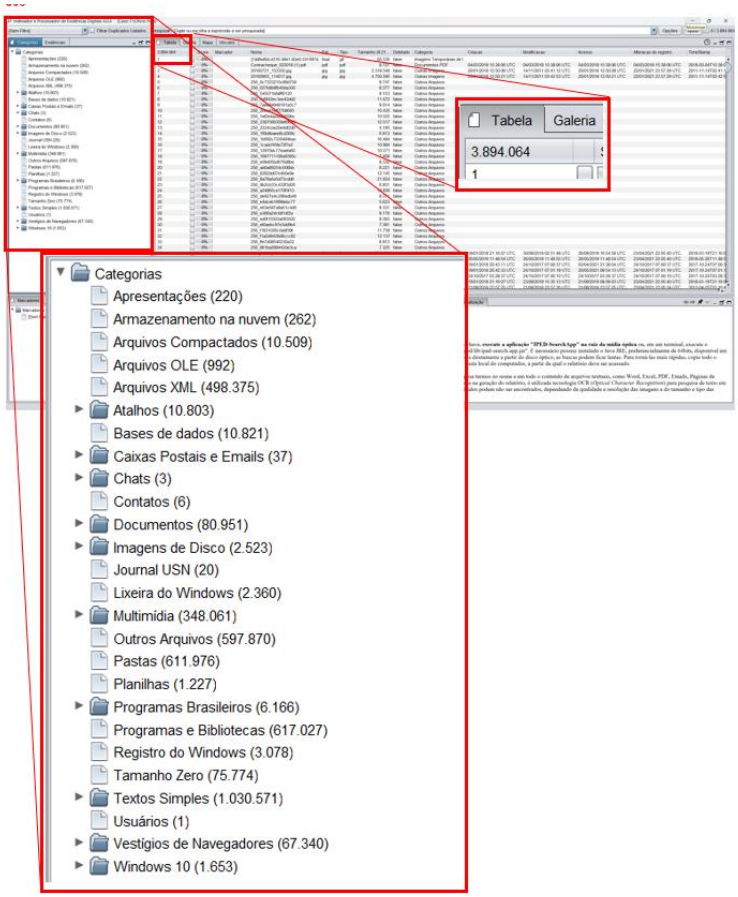

Figura 3. Interface de análise da ferramenta IPED com destaque para o quantitativo de 3.894.064 (três milhões, oitocentos e noventa e quatro mil e sessenta e quatro) objetos com as respectivas categorizações.

Após o processamento e indexação de conteúdo de cópias forenses utilizando ferramentas como o IPED, a análise de evidências digitais geralmente segue uma série de passos tradicionais, requerendo a intervenção humana manual.

Primeiro, foram identificados arquivos relevantes nas cópias forenses considerados úteis para a investigação em questão. Em seguida, a análise se concentrou em examinar os artefatos do sistema, como logs de eventos, registros de atividade, histórico de navegação, histórico de buscas e dados de rede, buscando por evidências de atividade suspeita.

Além disso, foram analisados os arquivos de mídia, como imagens, vídeos e áudios, em busca de evidências de crimes digitais, e exame de metadados associados aos arquivos para obter informações adicionais. Os arquivos excluídos e as áreas não alocadas da cópia forense também foram examinados para recuperar arquivos apagados, mas relevantes para a investigação.

As comunicações presentes na cópia forense, como e-mails, mensagens de texto e conversas em redes sociais, foram analisadas para identificar evidências de crimes digitais, e arquivos criptografados presentes na imagem forense foram examinados na tentativa de recuperar o conteúdo e identificar evidências de crimes digitais, conforme categorizações contidas na Tabela 3.

Tabela 3. Arquivos categorizados por natureza e respectivos quantitativos.

Apresentações (220)
Armazenamento na nuvem (262)
Arquivos Compactados (10.509)
Arquivos OLE (992)
Arquivos XML (498.375)
Atalhos (10.803)
Bases de dados (10.821)
Caixas Postais e E-mails (37)
Chats (3)
Contatos (6)
Documentos (80.951)
Imagens de Disco (2.523)
Journal USN (20)
Lixeira do Windows (2.360)
Multimídia (348.061)
Outros Arquivos (597.870)
Pastas (611.976)
Planilhas (1.227)
Programas Brasileiros (6.166)
Programas e Bibliotecas (617.027)
Registro do Windows (3.078)
Tamanho Zero (75.774)
Textos Simples (1.030.571)
Usuários (1)
Vestígios de Navegadores (67.340)
Windows 10 (1.653)

3.2. Aplicação do Método Reducionista

Atendendo aos preceitos norteadores da cadeia de custódia em dispositivos informáticos, foram repetidos os passos iniciais da aplicação do método tradicional, ou seja, levantamento e identificação das unidades de armazenamento e cópias forenses. Como medida de segurança, os exames foram realizados sobre as cópias, preservando-se o original.

Utilizando software gratuito *ShellBagsView* de interpretação da região do registro do Windows conhecida como *Shellbags*, desenvolvido pelo israelense Nir Sofer, reduziu-se o escopo de pastas a analisar: de 611.976 para 1524 pastas – Figura 4.

Utilizando o *software JumpListsView* de interpretação dos arquivos ou pastas mais recentemente ou frequentemente acessados nos sistemas analisados, também desenvolvido pelo israelense Nir Sofer, reduziu-se o escopo de arquivos lidos ou editados pelo usuário: de 80.951 para 3044 – Figura 5.

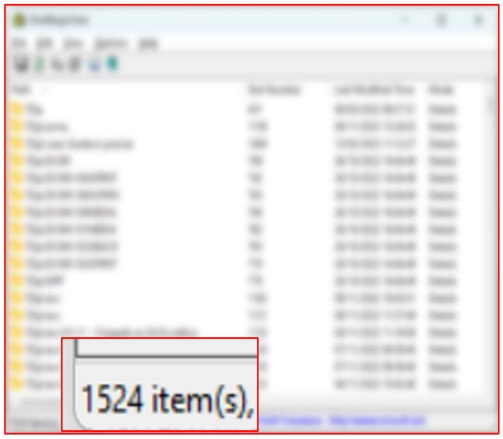

Figura 4. Interface da ferramenta *ShellBagsView* com aplicação de efeito embaçador e foco no quantitativo de pastas acessadas nos sistemas analisados.

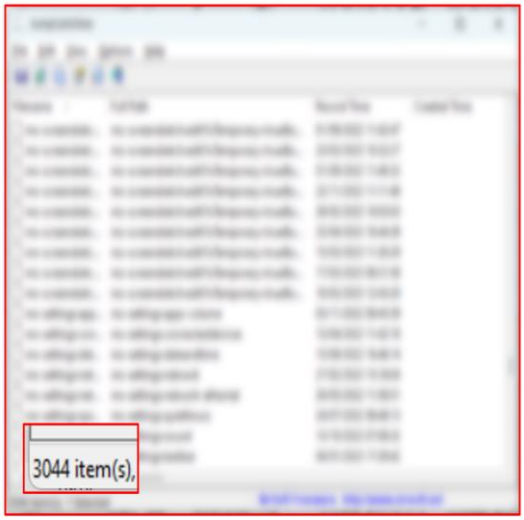

Figura 5. Interface da ferramenta *JumpListsView* com aplicação de efeito embaçador e foco no quantitativo de arquivos mais recentemente ou frequentemente acessados nos sistemas analisados.

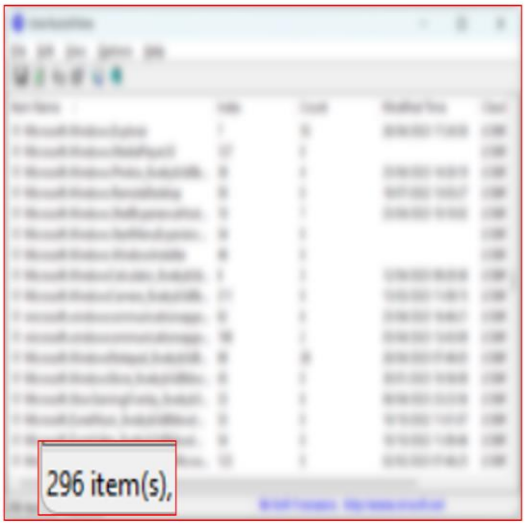

Figura 6. Interface da ferramenta *UserAssisView* com aplicação de efeito embaçador e foco no quantitativo de programas mais recentemente executados nos sistemas analisados.

Utilizando *software* gratuito *UserAssistView* de interpretação dos softwares mais recentemente executados, desenvolvido pelo israelense Nir Sofer, reduziu-se o escopo de processos da seguinte forma: de 6.166 para 296 – Figura 6.

Utilizando software gratuito *ThumbCacheViewer* de interpretação dos bancos de dados armazenadores de miniaturas de imagens, reduziu-se o escopo da seguinte forma: de 64.068 para 7.733 miniaturas – Figura 7.

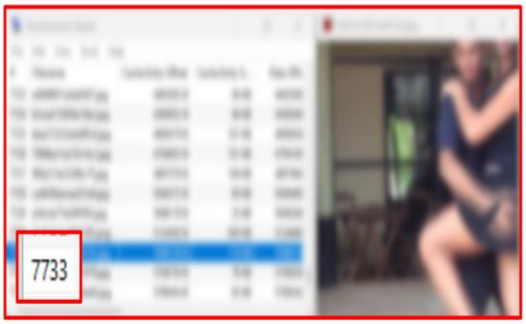

Figura 7. Interface da ferramenta *ThumbCacheViewer* com aplicação de efeito embaçador e foco no quantitativo de miniaturas de imagens encontradas nos sistemas analisados.

Tabela 4. Arquivos categorizados por natureza e respectivos quantitativos após a aplicação do método reducionista.

Pastas navegadas (1524)
Últimos arquivos acessados (3044)
Últimos programas executados (296)
Miniaturas de arquivos de imagens (7733)

Tabela 5. Comparativo quantitativo dos artefatos que se interseccionaram após a aplicação dos métodos tradicional e reducionista.

CASOS	Método Tradicional	Método Reducionista	% Redução
Total	Pastas encontradas (611.976)	Pastas navegadas (1524)	99,75%
	Documentos (80.951)	Últimos arquivos acessados (3044)	96,24%
	Programas Executados (6.166)	Últimos programas executados (296)	95,20%
	Arquivos de Imagens (64.068)	Miniaturas de arquivos de imagens (7733)	87,13%
01	Pastas encontradas (68.917)	Pastas navegadas (178)	99,74%
	Documentos (8.335)	Últimos arquivos acessados (422)	94,94%
	Programas Executados (1.221)	Últimos programas executados (15)	1,23%
	Arquivos de Imagens (6.899)	Miniaturas de arquivos de imagens (922)	13,36%
02	Pastas encontradas (45.022)	Pastas navegadas (174)	98,77%
	Documentos (8.996)	Últimos arquivos acessados (347)	96,14%
	Programas Executados (635)	Últimos programas executados (29)	95,43%
	Arquivos de Imagens (5.887)	Miniaturas de arquivos de imagens (556)	90,56%
03	Pastas encontradas (76.820)	Pastas navegadas (145)	99,81%
	Documentos (8.774)	Últimos arquivos acessados (332)	96,22%
	Programas Executados (333)	Últimos programas executados (36)	89,19%
	Arquivos de Imagens (8.745)	Miniaturas de arquivos de imagens (840)	90,39%
04	Pastas encontradas (102.963)	Pastas navegadas (198)	99,81%
	Documentos (9.444)	Últimos arquivos acessados (347)	96,33%
	Programas Executados (654)	Últimos programas executados (29)	95,57%
	Arquivos de Imagens (6.931)	Miniaturas de arquivos de imagens (655)	90,55%
05	Pastas encontradas (105.222)	Pastas navegadas (144)	99,86%
	Documentos (12.400)	Últimos arquivos acessados (333)	97,31%
	Programas Executados (578)	Últimos programas executados (26)	95,5%
	Arquivos de Imagens (5.553)	Miniaturas de arquivos de imagens (445)	91,99%
06	Pastas encontradas (63.544)	Pastas navegadas (222)	99,65%
	Documentos (6.244)	Últimos arquivos acessados (434)	93,05%
	Programas Executados (455)	Últimos programas executados (29)	93,63%
	Arquivos de Imagens (5.167)	Miniaturas de arquivos de imagens (653)	87,36%
07	Pastas encontradas (15.233)	Pastas navegadas (143)	99,06%
	Documentos (6.010)	Últimos arquivos acessados (326)	94,58%
	Programas Executados (677)	Últimos programas executados (48)	92,91%
	Arquivos de Imagens (7.665)	Miniaturas de arquivos de imagens (791)	89,68%
08	Pastas encontradas (78.622)	Pastas navegadas (101)	99,87%
	Documentos (10.922)	Últimos arquivos acessados (277)	97,46%
	Programas Executados (955)	Últimos programas executados (39)	95,92%
	Arquivos de Imagens (8.333)	Miniaturas de arquivos de imagens (1.659)	80,09%
09	Pastas encontradas (55.633)	Pastas navegadas (219)	99,61%
	Documentos (9.826)	Últimos arquivos acessados (226)	97,7%
	Programas Executados (658)	Últimos programas executados (45)	93,16%
	Arquivos de Imagens (4.888)	Miniaturas de arquivos de imagens (1.212)	75,2%

4. DISCUSSÃO

Um trabalho pericial aplicado em um subconjunto gerado a partir de um conjunto de dados anterior muito maior pode ter diversas finalidades, dependendo do contexto em que é aplicado. Geralmente, o objetivo é analisar o subconjunto em busca de padrões, anomalias ou informações relevantes que possam ser utilizadas para fins de investigação, tomada de decisão ou avaliação de riscos.

Os ganhos em escala de tempo podem ser significativos quando se trabalha com um subconjunto de dados, em comparação com a análise do conjunto de dados completo. Isso ocorre porque a análise do conjunto completo pode ser extremamente demorada e complexa, principalmente quando se trata de grandes volumes de dados. A análise de um subconjunto, por outro lado, pode ser realizada de forma mais rápida e eficiente, permitindo que os resultados sejam obtidos em um prazo menor.

Além disso, o uso de um subconjunto de dados pode reduzir o custo e a complexidade do trabalho pericial, pois é possível realizar análises mais precisas e focadas em áreas específicas de interesse, sem a necessidade de processar todo o conjunto de dados. É importante lembrar que a escolha do subconjunto de dados a ser analisado deve ser cuidadosamente feita para garantir que ele seja representativo do conjunto completo, evitando assim a perda de informações relevantes para o caso em espécie.

A redução de escopo em análises forenses pode ser uma técnica útil para otimizar o processo de análise, economizar tempo e recursos, e concentrar a análise em áreas específicas que são mais relevantes para a investigação. Pode ser uma técnica útil em análises forenses, mas deve ser usada com cuidado e equilíbrio para evitar perda de informações importantes e viés de análise. É importante que os examinadores entendam bem as vantagens e desvantagens da técnica e apliquem critérios objetivos e bem definidos para a seleção do escopo. Apresentaremos alguns pontos vantajosos e desvantajosos que devem ser considerados na seleção e aplicação da técnica reducionista alternativamente à tradicional:

Vantagens:

1 Economia de tempo e recursos: reduzir o escopo de análise permite que os examinadores foquem em áreas mais relevantes e prioritárias para a investigação, economizando tempo e recursos.

2 Agilidade na obtenção de resultados: Ao concentrar a análise em áreas mais relevantes, a obtenção de resultados pode ser mais rápida e eficiente.

3 Análise mais objetiva: A redução de escopo pode ajudar a tornar a análise mais objetiva, pois, as decisões de análise são baseadas em critérios pré-definidos.

Desvantagens:

1- Perda de informações importantes: ao reduzir o escopo de análise, pode haver a perda de informações importantes que podem estar presentes em outras áreas do sistema.
2- Viés de análise: a seleção arbitrária de áreas para análise pode levar a um viés de análise, em que a interpretação dos resultados é influenciada pela seleção dos dados analisados.
3- Falta de contexto: a análise de partes isoladas do sistema pode levar à falta de contexto e dificultar a compreensão da atividade geral do sistema.
4- Risco de perder evidências relevantes: a redução de escopo pode levar à perda de evidências relevantes que podem estar presentes em áreas aparentemente irrelevantes ou inesperadas do sistema.

A redução de escopo em análises forenses apresenta vantagens significativas, como a economia de tempo e recursos, a agilidade na obtenção de resultados e a promoção de uma análise mais objetiva. Ao concentrar-se em áreas relevantes e prioritárias, os examinadores podem direcionar seus esforços de maneira mais eficiente, maximizando a eficácia do processo de análise forense. No entanto, é essencial considerar as desvantagens associadas a essa técnica, como a possibilidade de perda de informações importantes, o risco de viés de análise, a falta de contexto e a potencial perda de evidências relevantes. Portanto, é crucial que os examinadores tenham critérios claros e objetivos na seleção do escopo, a fim de garantir uma abordagem equilibrada e abrangente que minimize esses potenciais problemas.

5. CONCLUSÃO

Ao ponderar cuidadosamente os benefícios e as limitações da redução de escopo em análises forenses, os profissionais podem aproveitar ao máximo essa técnica para obter resultados mais eficientes e relevantes. Ao focar em áreas-chave, é possível otimizar recursos, reduzir o tempo necessário para a análise e tomar decisões embasadas em critérios pré-definidos. No entanto, é essencial considerar as desvantagens, como a possibilidade de perder informações cruciais e o risco de viés de análise. Ao aplicar a redução de escopo, é fundamental equilibrar a seleção das áreas analisadas

com a necessidade de uma visão abrangente e contextualizada do sistema investigado.

AGRADECIMENTOS

APOIO: FACEPE (Edital 05/2022 - PIBIC 2022)

REFERÊNCIAS BIBLIOGRÁFICAS

[1] DEPARTAMENTO DE ESTADO DOS ESTADOS UNIDOS. Trafficking in persons report 2021. Washington, D.C.: Departamento de Estado dos Estados Unidos, 2021.

[2] ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Exploração sexual de crianças e adolescentes na América Latina e no Caribe 2019: relatório regional. Washington, D.C.: OEA, 2019.

[3] Safernet Brasil; Chilhood Brasil. *Cenário da exploração sexual de crianças e adolescentes na internet no Brasil*, Safernet Brasil, Brasil (2018).

[4] Brasil. Estatuto da Criança e do Adolescente. Lei nº 8.069, de 13 de julho de 1990. Retirado em 22/05/2021, de http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

[5] Brasil. Marco Civil da Internet. Lei Nº 12.965, de 23/05/2023, de, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[6] P.J. Denning; H. Craig. *Martell Great Principles of Computing*, MIT Press (2015).