UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS EXATAS, NATURAIS E DA SAÚDE

DEPARTAMENTO DE COMPUTAÇÃO
SISTEMAS DE INFORMAÇÃO

ALEF BIANO DOS SANTOS

ESTUDO DA FERRAMENTA IPED NA ANÁLISE DE EVIDÊNCIAS DIGITAIS

ALEGRE - ES
DEZEMBRO DE 2023

ESTUDO DA FERRAMENTA IPED NA ANÁLISE DE EVIDÊNCIAS DIGITAIS

Trabalho de conclusão de curso apresentado ao Departamento de Computação do Centro de Ciências Exatas, Naturais e da Saúde da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

por

ALEF BIANO DOS SANTOS

Orientador
PAULO ROBERTO NUNES DE SOUZA

Universidade Federal do Espírito Santo

ALEGRE - ES

DEZEMBRO DE 2023

ALEF BIANO DOS SANTOS

Estudo da ferramenta IPED na análise de evidências digitais

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação do Centro de Ciências Exatas, Naturais e da Saúde da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovado em 14 de dezembro de 2023.

COMISSÃO EXAMINADORA

Documento assinado digitalmente
PAULO ROBERTO NUNES DE SOUZA
Data: 21/12/2023 10:57:41-0300
Verifique em https://validar.iti.gov.br

Prof. PhD Paulo Roberto Nunes de Souza
Universidade Federal do Espírito Santo
Orientador

Documento assinado digitalmente
JACSON RODRIGUES CORREIA DA SILVA
Data: 21/12/2023 13:40:29-0300
Verifique em https://validar.iti.gov.br

Prof. Dr Jacson Rodrigues Correia da Silva
Universidade Federal do Espírito Santo

Documento assinado digitalmente
MARCELO OTONE AGUIAR
Data: 21/12/2023 11:17:48-0300
Verifique em https://validar.iti.gov.br

Prof. Dr Marcelo Otone Aguiar
Universidade Federal do Espírito Santo

SUMÁRIO

1 Introdução **11**

1.1 O problema e sua importância 12

1.2 Objetivos 13

1.2.1 Objetivo Geral 13

1.2.2 Objetivos Específicos 14

2 Referencial Teórico **15**

2.1 Perícia Forense Computacional 16

2.1.1 Coleta 16

2.1.2 Extração 16

2.1.2.1 Cópia Forense 17

2.1.2.2 *Hash* 18

2.1.3 Análise 20

2.1.4 Apresentação 20

2.2 Antiforense 21

2.2.1 Sobrescrita de Dados 22

2.2.2 Impacto da Sobrescrita de Dados em Investigação Forense 22

3 Metodologia **24**

3.1 Massa de Dados 24

3.2 Cenários de Teste 24

3.3 Realização da Cópia Forense 25

3.3.1 Processo de Cópia Forense 25

3.3.1.1 Hashs das Cópias Forenses 29

3.4 Sobrescrita dos Dados 30

4 Metodologia Experimental 32

4.1 IPED 33

4.2 FTK Imager 34

4.3 AutoPsy 37

5 Resultados 41

6 Conclusão 46

6.1 Trabalhos Futuros 46

Referências 47

LISTA DE FIGURAS

Figura 1 Evolução do número de usuários ativos de Internet 11

Figura 2 Etapas da perícia forense 16

Figura 3 *Write Blocker* 18

Figura 4 Acesso à opção de criação de imagem de disco 26

Figura 5 Seleção do tipo de fonte da evidência 26

Figura 6 Seleção da fonte da evidência 27

Figura 7 Seleção do tipo de imagem 27

Figura 8 Informações da evidência 28

Figura 9 Seleção do tipo de imagem 28

Figura 10 Cópia Forense Finalizada 29

Figura 11 Tela inicial - EaseUS BitWiper 31

Figura 12 Seleção de disco - EaseUS BitWiper 31

Figura 13 Seleção de método - EaseUS BitWiper 31

Figura 14 Prompt de Comando 33

Figura 15 Processamento da Imagem de Disco 34

Figura 16 Tela Inicial - IPED 34

Figura 17 Adicionar Evidência 35

Figura 18 Selecionar tipo de Evidência 35

Figura 19 Selecionar Evidência 36

Figura 20 Tela Inicial FTK Imager 36

Figura 21 Novo Caso AutoPsy 37

Figura 22 Informações sobre o Caso AutoPsy 37

Figura 23 Selecionar Host AutoPsy 38

Figura 24 Selecionar tipo de Evidência AutoPsy 38

Figura 25 Selecionar Evidência AutoPsy 38

Figura 26 Selecionar Módulos AutoPsy 39

Figura 27 Evidência Adicionada AutoPsy 39

Figura 28 Tela Inicial AutoPsy 40

LISTA DE TABELAS

Tabela 1 Referencial Teórico 15

Tabela 2 Estrutura Laudo Técnico Pericial 21

Tabela 3 Informações sobre as Cópias Forenses 29

Tabela 4 MD5 Hash das Cópias Forenses 30

Tabela 5 SHA1 Hash das Cópias Forenses 30

Tabela 6 Arquivos Recuperados 41

Tabela 7 Ferramentas e Pontos analisados 44

LISTA DE SIGLAS

CAINE	Computer Aided Investigative Environment
IPED	Indexador e Processador de Evidências Digitais
HD	Hard Disk
NIST	National Institute of Standards and Technology
IPED	Indexador e Processador de Evidências Digitais

RESUMO

Devido a facilidade e praticidade que o computador oferece para as pessoas, tornou-se um produto de uso comum e indispensável em várias áreas de atuação. Com isso, os criminosos também passaram a utilizar esses dispositivos em seus delitos, trazendo à tona a necessidade de se criar meios de investigação capazes de analisá-los. A presente pesquisa tem por objetivo realizar um estudo de caso tendo como foco a análise de evidências digitais, utilizando o Indexador e Processador de Evidências Digitais (IPED), contrapondo seus resultados com os obtidos em outros sofwares, sendo eles o AutoPsy e FTK Imager. Com os experimentos realizados, pode-se concluir que a ferramenta IPED oferece recursos avançados para a análise de dados em perícias digitais e facilidade de uso, garantindo a recuperação eficiente de informações relevantes em cenários de perícia digital.

Palavras-chave: Computação Forense. Crimes Cibernéticos. Evidências Digitais. IPED. Perícia Forense Computacional.

ABSTRACT

Due to the convenience and practicality that computers offer, they have become widely used and indispensable tools in various fields of activity. Consequently, criminals have also started utilizing these devices in their illicit activities, highlighting the necessity to establish investigative methods capable of scrutinizing them. The present research aims to conduct a case study focusing on the analysis of digital evidence, employing the Digital Evidence Indexer and Processor (IPED) and comparing its results with those obtained from other software, namely AutoPsy and FTK Imager. Based on the experiments conducted, it can be concluded that the IPED tool provides advanced features for data analysis in digital forensics, coupled with user-friendly interfaces, ensuring the efficient recovery of pertinent information in digital forensic scenarios.

Key-words: Forensic Computing. Cyber Crimes. Digital Evidence. IPED. Computer Forensics.

1 INTRODUÇÃO

Com o passar dos anos, os computadores e a *Internet* tornaram-se recursos indispensáveis para a sociedade (vide Figura 1), tendo em vista a ampla utilização nas mais diversas áreas, como na educação, medicina e no desenvolvimento de novas tecnologias. Dada essa importância, não demorou para que essa tecnologia passasse a ser utilizada, também, na realização de atividades ilegais ou criminosas.

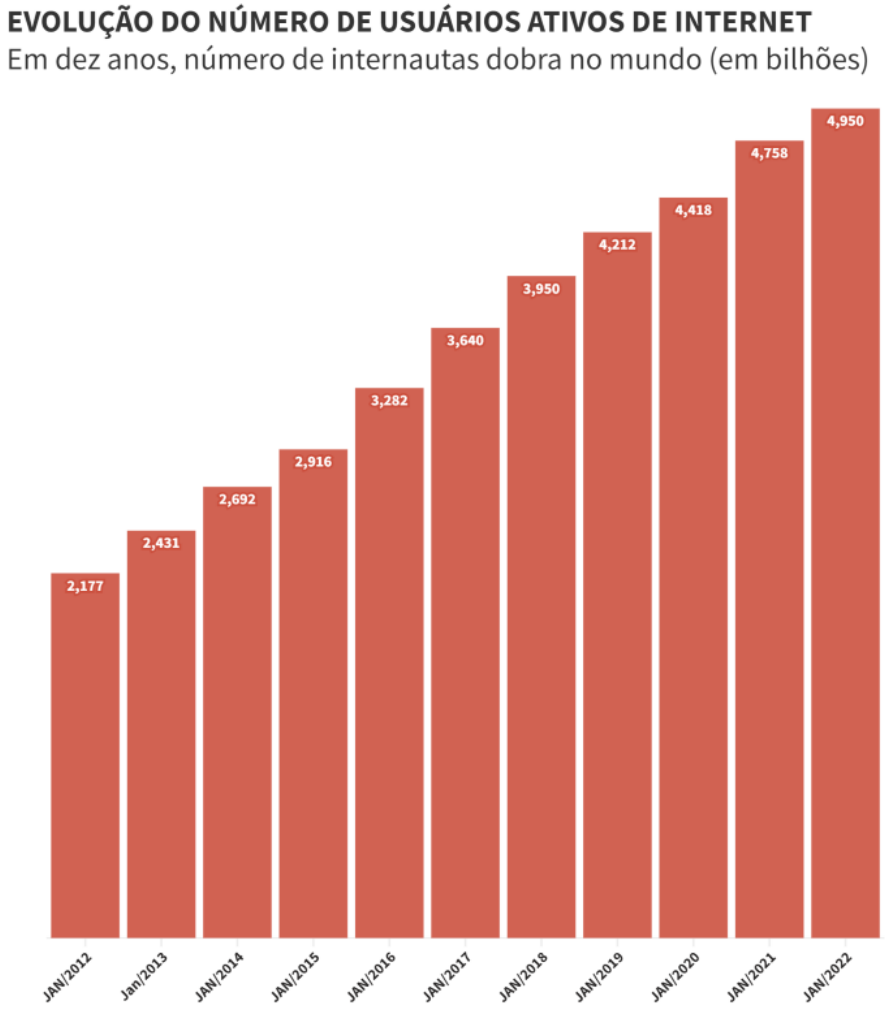

Figura 1: Evolução do número de usuários ativos de Internet
Fonte: (KEMP, 2022)

Almeida et al. (2015) afirma que o aparecimento dos primeiros casos de crimes informáticos ocorreram na década de 1960, nos quais o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas. Porém, esses crimes foram evoluindo ao longo do tempo, juntamente com o poder de processamento dos computadores, trazendo à tona a necessidade de se criar meios de investigação capazes de analisar esses delitos.

Medeiros (2020) ratifica essa hipótese, afirmando que, com o aumento da complexidade dos delitos cibernéticos, criou-se a necessidade de utilização de ferramentas que reúnam recursos para diversas aplicações em um sistema integrado de análise forense.

Segundo Souza (2015), os vestígios deixados por um crime cibernético estão na forma digital (armazenados em um disco, por exemplo). Assim, a perícia forense computacional tem como questão principal a identificação e o processamento de tais vestígios, através de procedimentos, técnicas e ferramentas adequadas.

De acordo com Queiroz e Vargas (2010), a forense computacional é um conjunto de procedimentos e metodologias, cuja função é investigar e armazenar evidências que possam responder se houve ou não um crime, tendo como base de análise equipamentos de processamento de dados (computadores pessoais, laptops, servidores, estações de trabalho ou outras mídias eletrônicas).

Dentre as ferramentas disponíveis atualmente, que têm por objetivo auxiliar na análise dos peritos, pode-se citar o FTK *Imager*[1], *Computer Aided Investigative Environment* (CAINE)[2], *ExifTool*[3], *AutoPsy*[4] e o Indexador e Processador de Evidências Digitais (IPED)[5], sendo este último o objeto de estudo escolhido para esta pesquisa.

1.1 O problema e sua importância

Marques (2013) afirma que os sistemas informáticos podem estar relacionados com a atividade criminosa de três formas: como armas para os cometer; como as próprias vítimas de um ataque; ou como arquivo de indícios ou prova de crimes. Este último cenário é o que mais se conecta com o objeto de estudo dessa pesquisa, pois,

[1]Mais informações em <https://www.exterro.com/ftk-imager>.
[2]Mais informações em <https://www.caine-live.net/>.
[3]Mais informações em <https://exiftool.org/>.
[4]Mais informações em <https://www.autopsy.com/>.
[5]Mais informações em <https://github.com/sepinf-inc/IPED>.

conforme citado anteriormente, existe uma grande probabilidade de serem encontrados vestígios no meio digital, ainda de acordo com Marques (2013).

> Após a ocorrência de um ato ilícito num sistema informático e pelas suas características intrínsecas, ficam registados uma série de indícios e provas, que importa saber recolher, preservar e apresentar para que, tal como já referido, se possam identificar os autores dos factos praticados, de forma inequívoca e legalmente admissível (MARQUES, 2013).

A presente pesquisa tem como foco a análise desses indícios, mas faz-se necessária a execução introdutória de outros procedimentos de igual importância no processo de uma perícia forense, a serem abordados posteriormente, no Capítulo 2.

> Sendo uma certeza que um sistema informático vai mais tarde ou mais cedo estar envolvido numa atividade ilícita, é imprescindível que quem seja responsável por estes ativos saiba dar uma resposta adequada, não só para minimizar o impacto no negócio como também, para maximizar a possibilidade de vir a imputar responsabilidades aos autores dos atos praticados, para em sede de responsabilidade civil, poderem vir a ser recuperados parte ou a totalidade dos prejuízos provocados (MARQUES, 2013).

Portanto, a correta utilização da ferramenta IPED aqui apresentada pode impactar positivamente em uma perícia computacional, ampliando as chances de encontrar evidências que auxiliem na tomada de decisão para elaboração do laudo pericial, com o objetivo de esclarecer os fatos ocorridos e responsabilizar os envolvidos.

1.2 Objetivos

A seguir são apresentados os objetivos gerais e específicos relacionados à esta pesquisa.

1.2.1 Objetivo Geral

Tendo elucidado o problema acima referido, o objetivo da presente pesquisa é realizar um estudo de caso da ferramenta IPED, levando em consideração os seus pontos positivos e passíveis de melhora, a fim de contribuir para a sua disseminação no campo da pesquisa.

1.2.2 Objetivos Específicos

- Identificar e caracterizar os recursos oferecidos pela ferramenta;
- Submeter a ferramenta à testes, através da utilização de uma base de dados;
- Analisar os resultados obtidos, contrapondo com outros softwares.

2 REFERENCIAL TEÓRICO

Foi realizada uma investigação científica de obras já publicadas com o objetivo de fundamentar esta pesquisa e aprofundar o conhecimento do contexto em que a ferramenta IPED está inserida. Essa busca foi realizada através de artigos, livros e revistas científicas encontrados na plataforma Google Scholar, utilizando como parâmetros de busca as palavras-chaves: “Computação Forense”, "Crimes Cibernéticos", “Evidências Digitais”, “IPED” e "Perícia Forense Computacional". Também foram selecionados artigos através de referência cruzada.

Com os resultados obtidos pela busca individual de cada paravra-chave, foi realizada a análise dos títulos dos artigos encontrados, a fim de efetuar uma pré-seleção de obras relevantes e concordantes com o tema da presente pesquisa. Após essa triagem, foi realizada a leitura dos resumos das obras pré-selecionadas, para então decidir quais iriam compor o corpus da revisão bibliográfica (vide Tabela 1).

Após a seleção e estudo da literatura, foram agregados conhecimentos obtidos através de buscas na internet, com o intuito de atingir os objetivos estabelecidos.

Palavra-chave	**Resultados encontrados**	**Selecionados**
Computação Forense	11.100	3
Crimes Cibernéticos	12.800	1
Evidências Digitais	105.000	0
IPED	583	1
Perícia Forense Computacional	2.140	1
Referência Cruzada	-	4

Tabela 1: Referencial Teórico
Fonte: o autor (2022)

A seguir, serão apresentados alguns dos principais tópicos que embasam a metodologia a ser adotada nesta pesquisa.

2.1 Perícia Forense Computacional

Segundo Souza (2015), a necessidade de compreender determinado evento, encontrando e analisando outros fatos e eventos relacionados ao objeto de análise é o que motiva a realização de uma perícia forense. Com esse intuito, Kent, Chevalier e Grance (2006) sugere que a perícia siga um processo forense composto por quatro etapas: coleta, extração, análise e apresentação, ilustradas na Figura 2.

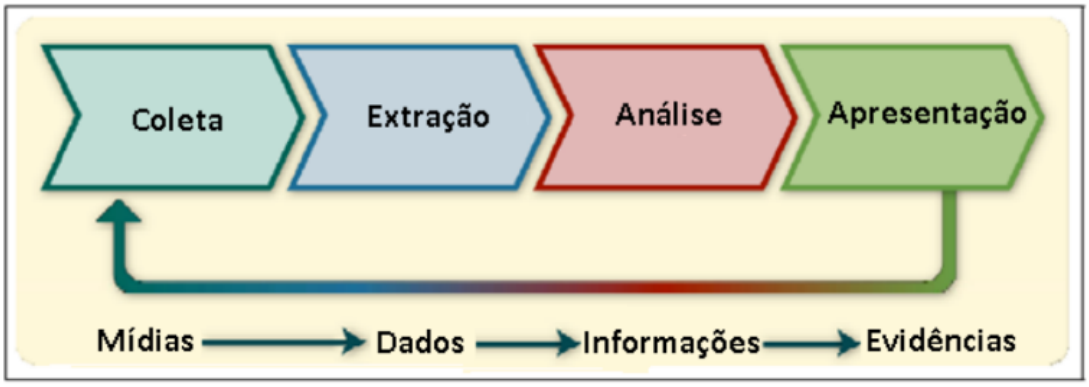

Figura 2: Etapas da perícia forense
Fonte: Adaptado de Kent, Chevalier e Grance (2006)

No intuito de fornecer uma compreensão mais detalhada do processo, as subseções seguintes abordarão individualmente cada uma dessas etapas, discutindo suas características, metodologias e a importância de sua aplicação no contexto da perícia forense.

2.1.1 Coleta

Etapa inicial do processo de perícia, na qual serão coletados as fontes de dados que podem conter evidências do fato a ser investigado. Essas fontes podem ser *Hard Disk's* (HD's) - ou discos rígidos-, computadores, celulares ou *Pen Drive's*, por exemplo. Souza (2015) afirma que é de fundamental importância que esta etapa ocorra de maneira rápida – se possível, logo após o conhecimento do incidente – e que siga procedimentos que preservem a integridade do material coletado.

2.1.2 Extração

Na segunda etapa, depois de coletadas as fontes de dados que serão periciadas, deve-se fazer a cópia forense dessas fontes, também chamada de cópia segura,

o que irá assegurar que nenhum dado seja perdido ou modificado. É importante ressaltar que as etapas a seguir nunca devem ser realizadas nas fontes originais.

> A próxima etapa é recuperar toda a informação contida nas cópias e extrair dados úteis para a investigação. As cópias seguras – realizadas na etapa de coleta – são cópias integrais, ou seja, contêm todos os arquivos, dados e configurações do material original que foi apreendido. Assim, é natural que ao início da etapa de extração, exista uma grande quantidade de arquivos e dados – às vezes ocultos ou até corrompidos – para serem analisados pelo perito. Identificar e recuperar arquivos que possam conter informações relevantes para a investigação é o objetivo da etapa de extração (SOUZA, 2015).

A subseção a seguir abordará de forma mais aprofundada a técnica de cópia forense.

2.1.2.1 Cópia Forense

De acordo com Eleutério e Machado (2019), a realização dos exames forenses deve ser sobre cópias fiéis obtidas a partir do material original. Para isso, deverão ser utilizadas técnicas e ferramentas que realizem uma duplicação fidedigna dos dados e preservem a integridade do material apreendido.

Quando se tratam de evidências digitais, devem ser tomadas precauções especiais, pois

> ...até operações simples podem modificar as evidências armazenadas. Ligar o computador, por exemplo, altera alguns arquivos, datas de último acesso e criam arquivos temporários, mesmo que o usuário não execute nenhuma ação. Até a trivial conexão de um pen drive na porta USB, pode gerar gravação de dados no dispositivo. Em vista disso, toda e qualquer atividade deve ser realizada com a garantia de que as informações armazenadas não sofram alterações (ALMEIDA, 2011).

Segundo Almeida (2011), para realizar a cópia forense, geralmente os peritos utilizam as técnicas de espelhamento (que consiste na cópia exata e fiel dos dados contidos em um dispositivo de armazenamento computacional para outro, ou seja, a duplicação é feita bit a bit) e imagem, que também gera uma cópia fidedigna, porém, ao invés de copiar os dados de um dispositivo para outro, eles são copiados para arquivos de imagem.

De acordo com Eleutério e Machado (2019), a técnica de imagem normalmente é a escolhida para a duplicação dos dados, pois possui algumas vantagens se comparada com o espelhamento. Dentre essas vantagens, pode-se citar:

- um dispositivo de destino pode armazenar diversas imagens de disco, se houver capacidade;
- possibilidade de compactação dos arquivos de imagem;
- facilidade de replicação das imagens de disco.

Ainda de acordo com Eleutério e Machado (2019), independentemente da técnica escolhida, é importante que, no ato da duplicação, seja garantido que as informações contidas no dispositivo original não sejam alteradas. Uma forma de certificar isso é através da utilização de um *Write Blocker*, ou bloqueador de escrita, que é um dispositivo simples conectado entre o computador e o dispositivo, que tem por objetivo assegurar que toda a informação existente permaneça inalterada durante o processo de cópia ou de acesso. Essa garantia é dada através do *hardware*, bloqueando operações de escrita no material submetido à cópia.

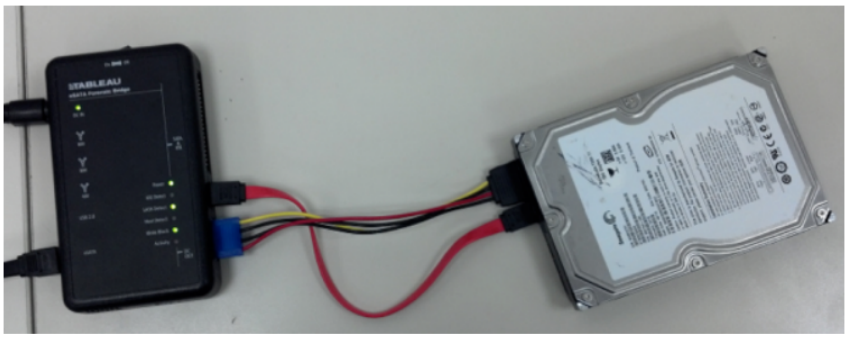

Figura 3: *Write Blocker*
Fonte: Aranha (2015)

Como citado no início dessa subseção, é necessário que a duplicação dos dados seja executada de forma fidedigna, não promovendo alterações nos arquivos originais, para que não se inviabilize a utilização de possíveis evidências encontradas. Uma forma de garantir a legitimidade da informação duplicada é confrontar os *hash's*.

2.1.2.2 *Hash*

De acordo com Martins et al. (2017), o *hash* é uma palavra de tamanho fixo que pode ser usado para representar qualquer arquivo digital, como uma foto, um vídeo ou um documento PDF. Consiste em gerar, a partir da sequência de bits do arquivo original (que pode ser extremamente longa), um código de tamanho padronizado, de acordo com o método utilizado para gerá-lo. O *hash* é específico para cada arquivo

existente e qualquer alteração nesse arquivo, seja uma simples vírgula em um texto, por exemplo, irá gerar uma sequência totalmente diferente, o que garante a confiabilidade em uma evidência, provando que a mesma não foi aduterada. A partir do código gerado, é impossível chegar ao conteúdo original, ou seja, o *hash* não fornece qualquer informação sobre a sequência de bits que o representa.

> Um exemplo da importância dessa propriedade é no armazenamento das senhas dos usuários em um provedor de serviços. Para evitar o armazenamento das senhas em claro, o servidor não armazena as senhas dos usuários, mas sim os *hashes* das senhas. Para se autenticar, o usuário envia sua senha para o servidor. Este determina o hash da senha e compara com o hash da senha previamente armazenado no tabela de senhas do servidor. Se for o mesmo hash, trata-se portanto da mesma senha e o servidor considera o usuário autenticado. O armazenamento do hash das senhas evita que seja possível obter a senha dos usuários a partir da tabela contendo os hashes das senhas. (MARTINS et al., 2017).

Segundo Queiroz e Vargas (2010), um dos algoritmos de *hash* amplamente utilizados na área de informática forense ao longo do tempo é o MD5 *Hash*, que foi desenvolvido pelo Professor Ronald L. Rivest em 1994 e é um resumo digital de 128-bit (16 bytes) relativamente rápido e simples de implementar.

Caso o algoritmo MD5 seja aplicado em um arquivo de texto contendo a sequência "abc", será retornado o código "900150983CD24FB0D6963F7D28E17F72". Se o mesmo arquivo contiver a sequência "abd", obteremos um valor de *hash* totalmente diferente, como "4911E516E5AA21D327512E0C8B197616".

Queiroz e Vargas (2010) afirmam também que a probabilidade de duas mensagens terem o mesmo valor de *hash* é de aproximadamente $1/2^{64}$, enquanto a probabilidade de encontrar uma mensagem com um código específico é da ordem de $1/2^{128}$. É extremamente improvável, embora não impossível, que duas mensagens diferentes tenham o mesmo valor de hash, dadas as grandes dimensões do espaço de hash disponível.

Ainda de acordo com Queiroz e Vargas (2010), outro algoritmo *hash* bastante utilizado é o SHA1, que por sua vez é um resumo de 160 bit desenvolvido pelo NIST (NIST). Esse algoritmo produz um código de 20 bytes, em comparação com os 16 bytes gerados pelo algoritmo MD5. Embora o SHA1 seja mais lento em relação ao MD5, o tamanho do código gerado torna o SHA1 mais forte em termos de vulnerabilidade a ataques.

Aplicando o algoritmo SHA1 ao mesmo arquivo com a sequência "abc", o re-

sultado obtido é "A9993E364706816ABA3E25717850C26C9CD0D89D".

Existindo a possibilidade, mesmo que remota, de esse código *hash* se repetir, devido à limitação de caracteres do método *hash* utilizado, é interessante adotar um algoritmo capaz de gerar sequências maiores, como o SHA-512, que gera códigos com 512 caracteres.

2.1.3 Análise

A terceira etapa é a responsável por analisar os dados e informações obtidos através da etapa de extração, utilizando técnicas e métodos legalmente justificáveis, a fim de obter informações relevantes para a investigação. Segundo Eleutério e Machado (2019), a análise consiste em um exame realizado sobre as informações extraídas, buscando a identificação de evidências digitais (como por exemplo a identificação de pessoas, locais, fotos ou vídeos, e a correlação entre esses elementos com o objeto de investigação). Nessa etapa, um dos maiores desafios é a quantidade de arquivos, o que faz com que o processo de análise demore mais do que o desejado.

2.1.4 Apresentação

É a última etapa do processo forense, que tem como objetivo documentar as evidências encontradas a fim de apresentá-las às autoridades competentes. Segundo Kent, Chevalier e Grance (2006), serão inseridos dados referentes às etapas anteriores, como: método de coleta e extração, análise dos fatos e o valor técnico do conteúdo analisado.

> O laudo técnico pericial deve ser conciso; apresentar uma leitura adequada ao público não ligado à área da informática; descrever de forma objetiva e clara os métodos, ferramentas e exames realizados durante o processo forense (SOUZA, 2015).

Segundo Eleutério e Machado (2019), a estrutura do laudo pericial geralmente possui: preâmbulo; histórico; material; objetivo, considerações técnicas ou periciais; exames e respostas aos quesitos formulados ou conclusões, conforme descrito na Tabela 2.

Preâmbulo	Identificação do laudo
Histórico	Fatos anteriores e de interesse ao laudo / Quesitos concisos e objetivos
Material	Descrição do material examinado
Objetivo	Principais objetivos da perícia
Considerações técnicas / periciais	Conceitos e informações que podem ser úteis para o entendimento do laudo
Exames	Parte descritiva e experimental do laudo
Respostas aos quesitos/-conclusões	Resumo objetivo dos resultados obtidos

Tabela 2: Estrutura Laudo Técnico Pericial
Fonte: Adaptado de Eleutério e Machado (2019)

2.2 Antiforense

Divergindo das abordagens e princípios anteriormente apresentados, a Antiforense constitui um conjunto de estratégias e técnicas para comprometer, dificultar ou até mesmo impedir o acesso a informações cruciais para o desenrolar de uma investigação.

> Durante todo o processo investigatório, desde a etapa de recolhimento dos equipamentos para exames até a fase de análise dos dados encontrados, o perito depara-se com diversos desafios que podem atrapalhar ou impossibilitar a apuração dos fatos. Essas dificuldades, quando impostas explicitamente pelos usuários, são conhecidas comumente na área pelo termo Anti Forense e consistem em métodos de remoção, ocultação ou subversão de evidências com o objetivo de mitigar os resultados de uma análise forense computacional.(ALMEIDA, 2011).

Com a utilização dessas técnicas, as evidências podem ser submetidas a processos de destruição, assegurando que não sejam identificadas ou, quando identificadas, inviabilizando sua aplicação. Alternativamente, as evidências podem ser ocultadas, demandando um esforço prolongado por parte do perito forense para sua localização. Além disso, existe a possibilidade de manipulação e alteração das evidências, com o intuito de distribuir a responsabilidade ou corromper sua validade, tornando-as inutilizáveis em um contexto jurídico.

No desenvolvimento desta pesquisa, exploraremos especificamente a técnica antiforense de sobrescrita de dados, que objetiva eliminar qualquer vestígio de evidência que possa ser identificado em uma mídia digital. Este método representa uma estratégia de alto impacto no contexto da Antiforense, buscando minar a eficácia das técnicas tradicionais de recuperação e análise forense digital.

2.2.1 Sobrescrita de Dados

Para garantir que os dados armazenados em dispositivos de armazenamento removíveis, como *PenDrives*, sejam apagados de forma segura e permanente antes de serem descartados ou repassados, recomenda-se o uso de ferramentas de sobrescrita de dados, como o programa *EaseUS BitWiper (2023)*, que foi escolhido para o desenvolvimento dessa pesquisa.

Este software utiliza o método de preenchimento com zeros, também conhecido como *Write Zero* ou *One Pass Zeros*, para sobrescrever os dados armazenados no *PenDrive*. Esse método consiste em escrever zeros em todos os setores do dispositivo, o que impede a recuperação dos dados originalmente armazenados.

É importante destacar que o uso de ferramentas de sobrescrita de dados é essencial para garantir a privacidade dos dados e evitar a exposição de informações sensíveis.

Além da importância da segurança e privacidade dos dados, a aplicação desse método também se faz necessária nessa pesquisa devido à quantidade de vezes que os dados foram gravados para testes nos dispositivos, visando garantir a fidelidade dos resultados.

2.2.2 Impacto da Sobrescrita de Dados em Investigação Forense

A utilização dessa técnica pode impactar de diversas formas em uma investigação forense, de acordo com o seu objetivo e principalmente por quem a está utilizando. A sobrescrita adequada dos dados em dispositivos utilizados como parte da pesquisa é de extrema importância para garantir a fidelidade dos resultados obtidos. Como mencionado anteriormente, os dados desta pesquisa foram gravados múltiplas vezes para testes, e a utilização dessa técnica permitiu que o ambiente experimental fosse resetado com confiabilidade antes de cada nova análise, assegurando a consistência dos resultados e a não contaminação dos dados entre testes.

Neste primeiro cenário, a técnica ajuda o investigador a conhecer melhor as ferramentas que está utilizando, procurar falhas e entender os limites de recuperação de dados que o software utilizado lhe proporcionará.

Em contextos nos quais os objetivos principais incluem a proteção da privacidade e a eliminação segura de dados sensíveis, o uso de ferramentas de sobrescrita,

como o EaseUS BitWiper aqui apresentado, também possui impacto positivo, sendo, portanto, uma prática importante para prevenir violações de dados e proteger a reputação e a confiança das organizações e indivíduos envolvidos.

Todavia, a sobrescrita de dados também pode apresentar desafios em investigações forenses, especialmente quando se trata de recuperar dados de dispositivos utilizados em atividades criminosas ou em outras situações legais, dificultando ou até mesmo inviabilizando a recuperação de dados relevantes para a investigação. Nesses cenários, é de suma importância que os peritos sejam cuidadosos ao abordar dispositivos que possam ter sido submetidos a processos de sobrescrita de dados e adotem estratégias adequadas para lidar com essa limitação. Isso inclui o uso de técnicas mais avançadas de recuperação de dados e a busca por outras fontes de evidências, como dados residuais em outras mídias ou dispositivos conectados ao sistema em questão.

Vale ressaltar que a sobrescrita de dados não é o único método de eliminação segura de informações, e a escolha do método adequado depende do contexto específico em que está sendo aplicado. Outras técnicas, como criptografia ou a destruição física dos dispositivos de armazenamento, também podem ser consideradas dependendo dos requisitos de segurança e das leis e regulamentações aplicáveis.

Portanto, a sobrescrita de dados é uma prática essencial para garantir a privacidade e a segurança dos dados, especialmente quando se trata do descarte ou reutilização de dispositivos de armazenamento. Porém, em investigações forenses, é importante estar ciente do impacto dessa prática, pois pode apresentar desafios significativos na recuperação de evidências.

3 METODOLOGIA

Para iniciar a análise, é necessário realizar uma cópia forense da mídia contendo os dados a serem analisados, utilizando a técnica de geração de imagem do disco. Idealmente, essa cópia deve ser feita utilizando um *Write Blocker*, dispositivo utilizado para impedir a escrita ou alteração dos dados originais. No entanto, devido ao alto custo de aquisição desse dispositivo e a pesquisa ter como foco as etapas de análise e apresentação, esta pesquisa não contará com sua utilização.

3.1 Massa de Dados

Para realizar os testes, foi montado um dispositivo de armazenamento externo (*PenDrive*) contendo uma variedade de tipos de dados mais comuns de serem utilizados, incluindo cinquenta imagens, dez vídeos e três arquivos PDF. Estes arquivos incluem informações como números de telefone e CPF, com o objetivo de testar tanto recursos específicos do IPED quanto aqueles comuns aos outros softwares de análise de dados.

3.2 Cenários de Teste

Foram escolhidos quatro cenários para teste que buscam contemplar alguns dos possíveis casos encontrados ao se realizar uma perícia, sendo eles:

1. PenDrive montado normalmente com os dados descritos na seção anterior;
2. PenDrive montado normalmente com os dados descritos na seção anterior e posteriormente excluídos manualmente;
3. PenDrive montado normalmente com os dados descritos na seção anterior e posteriormente formatado;

4. PenDrive montado normalmente com os dados descritos na seção anterior e posteriormente sobrescrito com zeros.

3.3 Realização da Cópia Forense

Para o desenvolvimento da presente pesquisa, foi utilizada a versão 3.15.6 do IPED, a qual não contém o recurso de cópia forense. Dessa forma, foi utilizado o *software* FTK *Imager* como ferramenta para a geração das mesmas no formato *Raw* (dd).

Após a obtenção da imagem forense, esta será submetida à análise por meio da ferramenta IPED. A fim de garantir a confiabilidade e avaliar a consistência e a precisão dos resultados obtidos pelo objeto de pesquisa aqui apresentado, foi realizada uma comparação com as informações coletadas pelos *softwares AutoPsy* e FTK *Imager*.

Essa comparação tem por objetivo identificar possíveis discrepâncias ou similaridades entre os resultados gerados pelas diferentes ferramentas forenses, proporcionando uma forma de comparação capaz de prover conclusões a serem apresentadas nesta pesquisa.

3.3.1 Processo de Cópia Forense

Para prosseguir com a criação de uma imagem de disco utilizando o FTK *Imager*, é necessário seguir alguns passos cuidadosamente. O primeiro passo é acessar o menu File e selecionar a opção *Create Disk Image* (Figura 4). Isso irá abrir uma nova aba, onde é necessário escolher o tipo de fonte da evidência (Figura 5).

Dentre as opções disponíveis, utilizaremos a Physical Drive, que representa o hardware de armazenamento real presente em um dispositivo, mas também estão disponíveis outras opções, como a Logical Drive, e a Image File.

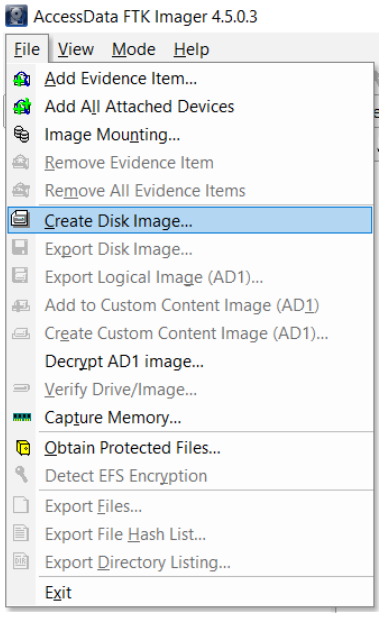

Figura 4: Acesso à opção de criação de imagem de disco
Fonte: O autor (2023)

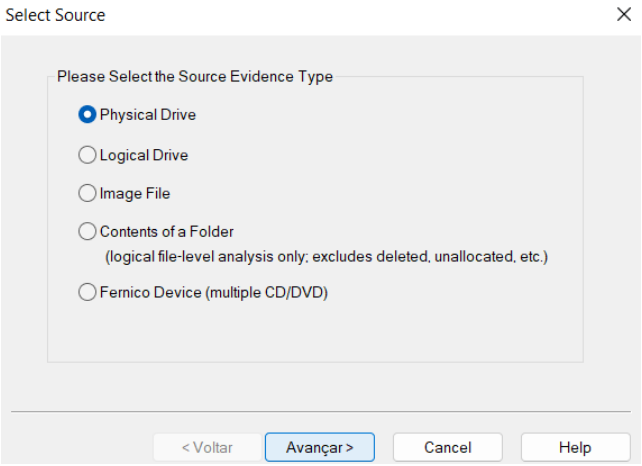

Figura 5: Seleção do tipo de fonte da evidência
Fonte: O autor (2023)

Em seguida, é necessário selecionar a fonte dos dados (Figura 6) e o tipo de imagem a ser gerada (Figura 7). Utilizaremos a imagem Raw (dd), que consiste em uma cópia bit a bit de todo o conteúdo do dispositivo, incluindo dados, estrutura de arquivos e espaço não alocado, por exemplo.

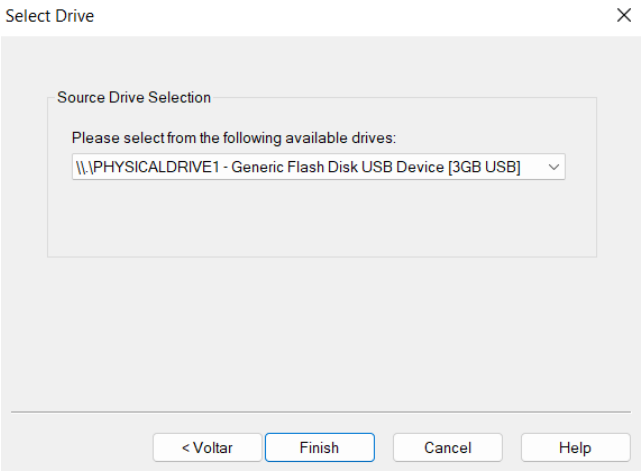

Figura 6: Seleção da fonte da evidência
Fonte: O autor (2023)

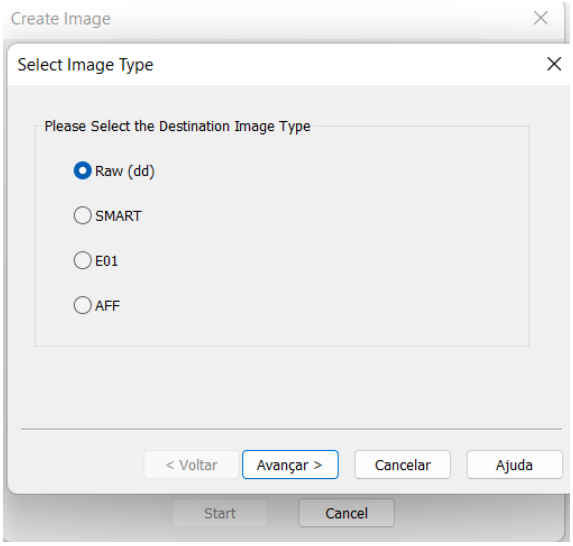

Figura 7: Seleção do tipo de imagem
Fonte: O autor (2023)

É necessário documentar a evidência coletada através das informações fornecidas (Figura 8), para que ela possa ser facilmente identificada em meio a outras evidências que possam existir no processo. Por fim, é necessário selecionar o destino da imagem criada e o nome referente (Figura 9). Dessa forma, a imagem de disco será criada de forma segura e completa, permitindo que sejam realizadas análises detalhadas.

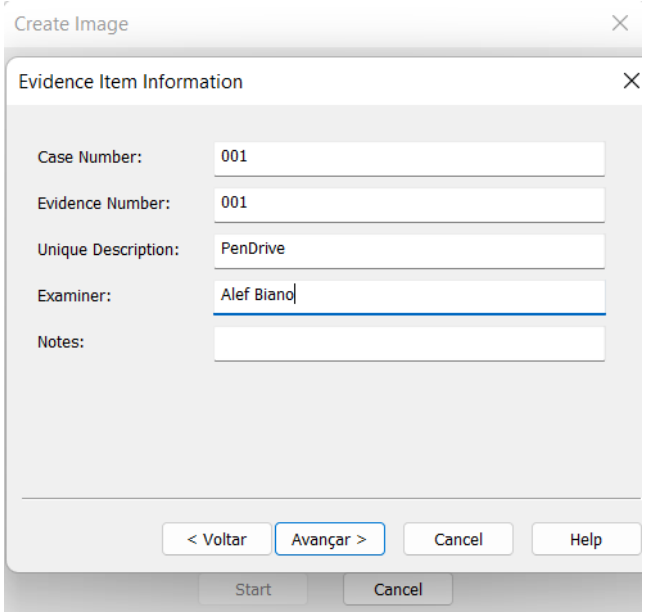

Figura 8: Informações da evidência
Fonte: O autor (2023)

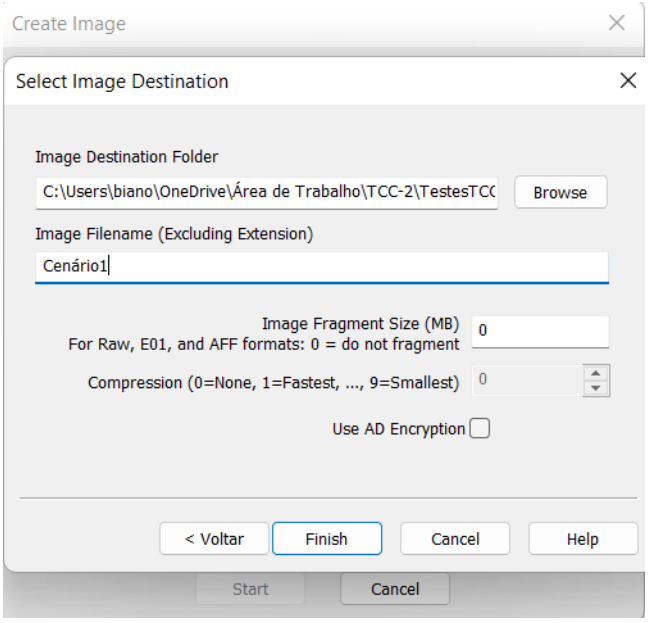

Figura 9: Seleção do tipo de imagem
Fonte: O autor (2023)

Após seguir as etapas de configuração, inicia-se a Cópia Forense. Durante o processo, é possível acompanhar o progresso e o tempo estimado para a finalização. Em testes realizados, o processo levou uma média de 12 minutos para ser concluído, levando em consideração a mídia de 3.599.232 KB, como ilustrado na Figura 10. É importante destacar que o tempo de cópia pode variar de acordo com o tamanho do dispositivo e sua velocidade de leitura.

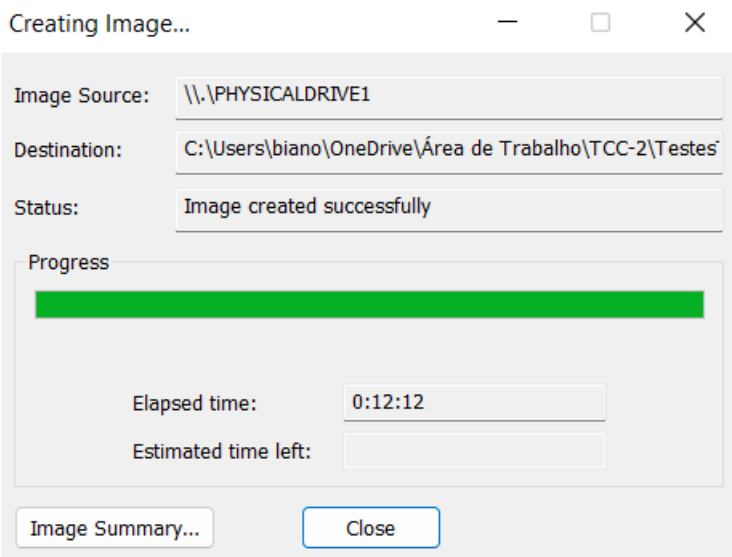

Figura 10: Cópia Forense Finalizada
Fonte: O autor (2023)

O tempo transcorrido para a produção das réplicas de cada cenário analisado, juntamente com o formato empregado e o tamanho final, é apresentado na Tabela 3. Vale ressaltar que o tamanho final refere-se à capacidade total da mídia utilizada para a criação das cópias, independentemente do número de arquivos contidos.

Cenário	**Tempo**	**Tamanho**	**Formato**
Cenário1	12:28	3.599.232 KB	Raw (DD)
Cenário2	12:28	3.599.232 KB	Raw (DD)
Cenário3	12:34	3.599.232 KB	Raw (DD)
Cenário4	12:33	3.599.232 KB	Raw (DD)

Tabela 3: Informações sobre as Cópias Forenses
Fonte: O autor (2023)

3.3.1.1 Hashs das Cópias Forenses

Após a conclusão do processo de cópia forense, é possível obter informações detalhadas sobre o arquivo gerado, incluindo o valor de *Hash*, mencionado anteriormente na subseção 2.1.2.2. Essas informações são de extrema importância para garantir a integridade dos dados coletados, pois o valor de hash permite verificar se a imagem gerada é idêntica ao dispositivo original, assegurando assim a confiabilidade dos dados coletados para fins de investigação.

Nas cópias forenses geradas através do FTK *Imager*, são retornados dois tipos

de *Hash*: o MD5 e o SHA1, a fim de fortalecer a confiabilidade das análises que serão conduzidas posteriormente, garantindo a integridade e autenticidade dos dados.

Os valores de *hash* gerados por esses algoritmos para as cópias forenses analisadas estão detalhados nas Tabelas 4 e 5:

Cenário	**MD5**
Cenário1	AFDC237BF16768035614F26A4DB14D7E
Cenário2	83F980AB520C763F9A03F7D19E6E1C48
Cenário3	FA633F9C130605C3056F000C78CE2C8F
Cenário4	62CE4715BE96BB9799F78CB8E84A23E1

Tabela 4: MD5 Hash das Cópias Forenses
Fonte: O autor (2023)

Cenário	**SHA1**
Cenário1	B8600DC5E6CA877954952508A3208013F2F43FB3
Cenário2	9C35ED3D75532B1562806D91A1D2245E2ED4933C
Cenário3	7F1B539E4E01F95EB9AAF6C27FE7E0F2391BC5BA
Cenário4	64D2F77545A9A7E970FA0CC1409A9A72C1C7F8CD

Tabela 5: SHA1 Hash das Cópias Forenses
Fonte: O autor (2023)

3.4 Sobrescrita dos Dados

Como mencionado anteriormente na seção 2.2.1, será utilizada a técnica antiforense de sobrescrita de dados, através do *software EaseUS BitWiper*, aplicando o método de preenchimento com zeros, objetivando a exclusão permanente dos dados contidos nas mídias analisadas, inviabilizando tentativas de recuperação por parte do perito encarregado da investigação.

Após a instalação do *software*, é necessário iniciá-lo e selecionar a opção Limpar Disco (Figura 11), escolher o disco a ser limpo (Figura 12) e informar o método a ser utilizado (Figura 13), no caso o de preenchimento com zeros. Uma vez que as configurações sejam realizadas, basta aguardar o processo ser finalizado, o que pode demorar algum tempo dependendo do tamanho do dispositivo. Nos testes realizados, o processo durou uma média de 25 minutos.

Figura 11: Tela inicial - EaseUS BitWiper
Fonte: O autor (2023)

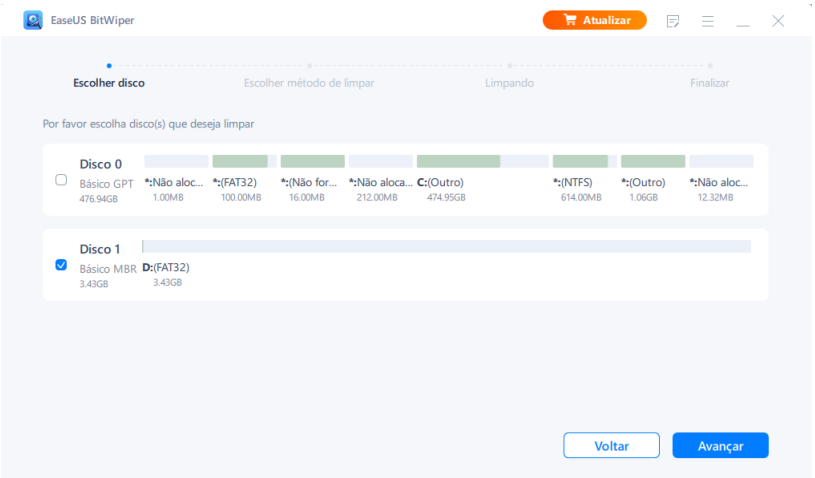

Figura 12: Seleção de disco - EaseUS BitWiper
Fonte: O autor (2023)

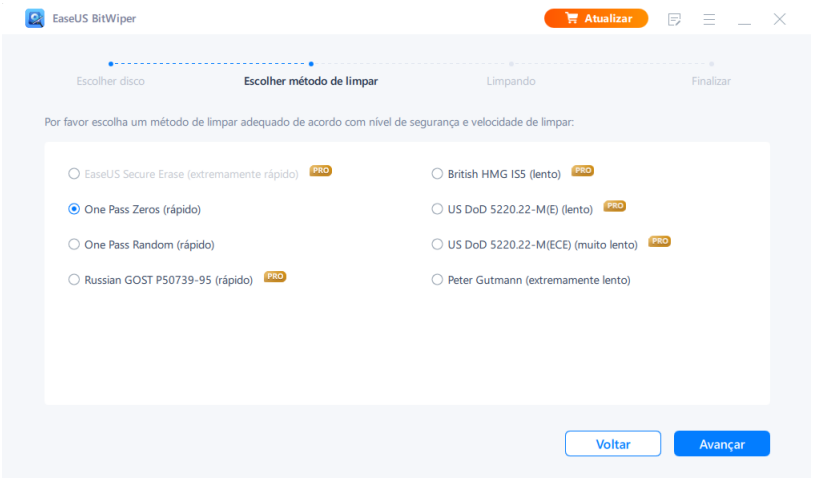

Figura 13: Seleção de método - EaseUS BitWiper
Fonte: O autor (2023)

4 METODOLOGIA EXPERIMENTAL

Após o processo de cópia forense ter sido concluído, é possível iniciar a análise das imagens geradas a partir dos cenários propostos. O equipamento utilizado para esses experimentos foi um *notebook* Dell modelo G15, equipado com um processador Intel I5 11400H, 24GB de memória RAM e uma GPU RTX3050 Laptop com 4GB de memória dedicada. É importante destacar a importância de contar com um equipamento de alta performance para essa etapa, pois a análise de imagens de disco pode ser bastante demorada e exigir altos recursos computacionais.

O objeto de estudo desta pesquisa concentra-se no sistema IPED. No entanto, como parte da metodologia adotada, os experimentos computacionais propostos também serão conduzidos nos softwares AutoPsy e FTK Imager, com o objetivo de realizar uma análise comparativa dos resultados obtidos por meio de cada uma dessas ferramentas.

Segundo SEPINF (2023), o IPED, aqui utilizado na versão 3.15.6, foi desenvolvido de forma colaborativa pelos peritos forenses digitais da Polícia Federal do Brasil. O projeto teve seu início em 2012, mas somente em 2019 o código-fonte foi oficialmente publicado, tornando-o disponível para a comunidade de peritos e pesquisadores através de um repositório no GitHub.

O software *AutoPsy (2023)*, utilizado na versão 4.20, foi desenvolvido pela empresa norte-americana Basis Technology. Assim como o IPED, o AutoPsy é uma ferramenta gratuita e de código aberto. Por fim, o *FTK Imager (2023)*, utilizado na versão 4.5.0.3, é uma criação da empresa *AccessData*.

A condução de experimentos computacionais nas três ferramentas mencionadas – IPED, *AutoPsy* e FTK *Imager* – possibilitará uma análise abrangente e comparativa dos resultados obtidos por cada uma delas. Isso contribuirá para uma compreensão mais profunda das capacidades e limitações de cada ferramenta, permitindo a identificação das circunstâncias nas quais cada uma se destaca ou apresenta desafios. Essa análise comparativa é essencial para a condução de investigações foren-

ses precisas e eficazes, fornecendo um panorama abrangente das opções disponíveis para os peritos.

4.1 IPED

Para iniciar a análise utilizando o IPED, é necessário seguir alguns passos importantes. O primeiro passo é acessar o terminal ou prompt de comando e digitar o seguinte comando: **"java -jar iped.jar -d [caminho para a imagem de disco] -o [caminho de destino]"** (Figura 14). Esse comando irá executar o IPED e indicar ao programa qual é a imagem de disco que será analisada e onde os resultados da análise serão armazenados. É necessário ter o Java[1] instalado e configurado corretamente no sistema para que o comando possa ser executado com sucesso. Além disso, é importante verificar se o caminho para a imagem de disco e o caminho de destino estão corretamente especificados para garantir que a análise ocorra sem problemas.

Figura 14: Prompt de Comando
Fonte: O autor (2023)

Após a execução deste comando, o IPED irá começar a processar a imagem de disco (Figura 15) e criará um diretório no local especificado no comando, contendo um arquivo executável para o perito verificar os arquivos encontrados na evidência.

Uma vez que o processamento foi concluído, o arquivo gerado pode ser acessado e a análise pode ser iniciada. A tela inicial do IPED (Figura 16) é simples e intuitiva, com diversas opções de ferramentas de análise disponíveis para ajudar a investigar e analisar a imagem de disco.

[1]Mais informações em <https://www.java.com/pt-BR/>.

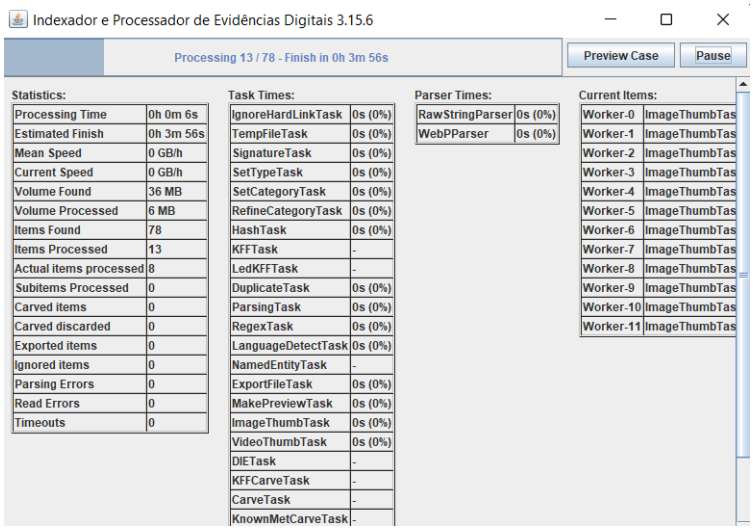

Figura 15: Processamento da Imagem de Disco
Fonte: O autor (2023)

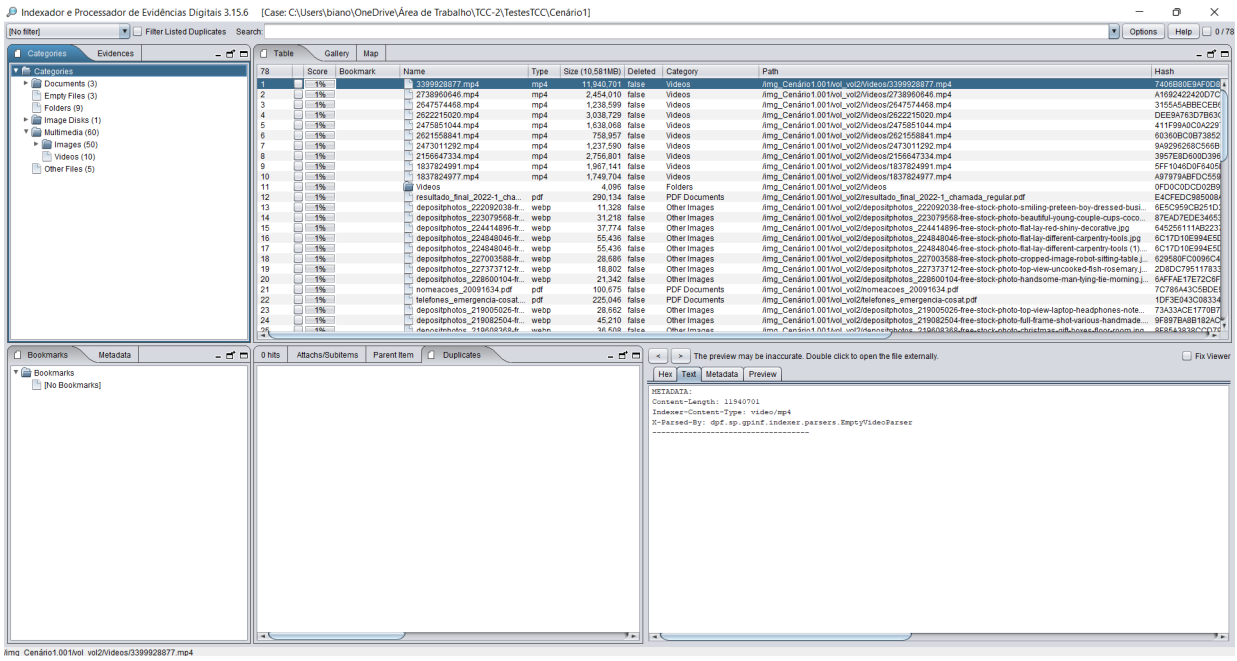

Figura 16: Tela Inicial - IPED
Fonte: O autor (2023)

4.2 FTK Imager

A execução da análise por meio do FTK *Imager* é caracterizada por uma inicialização mais ágil, proporcionando uma análise integralmente conduzida através de uma interface gráfica. Inicialmente, é necessário acessar o menu File e selecionar a opção *Add Evidence Item* (Figura 17). A seguir, o usuário deve escolher o tipo de fonte da evidência (Figura 18) e especificar a origem dos dados (Figura 19).

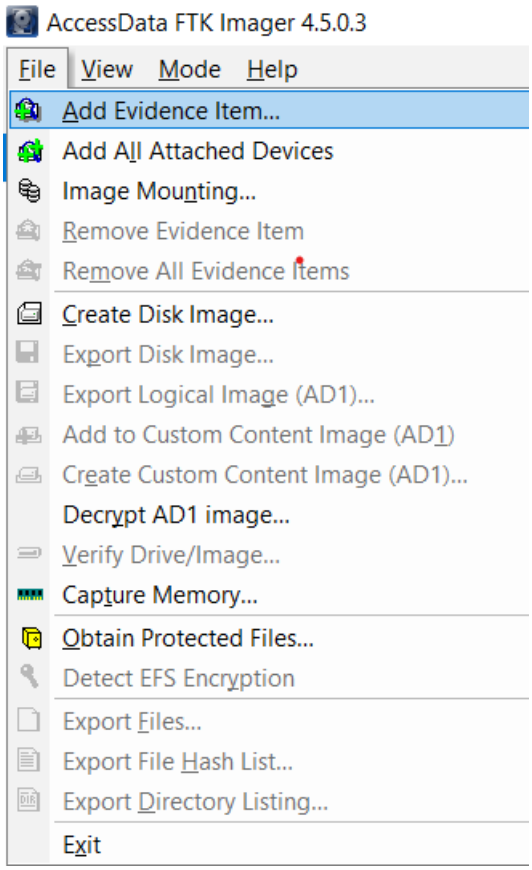

Figura 17: Adicionar Evidência
Fonte: O autor (2023)

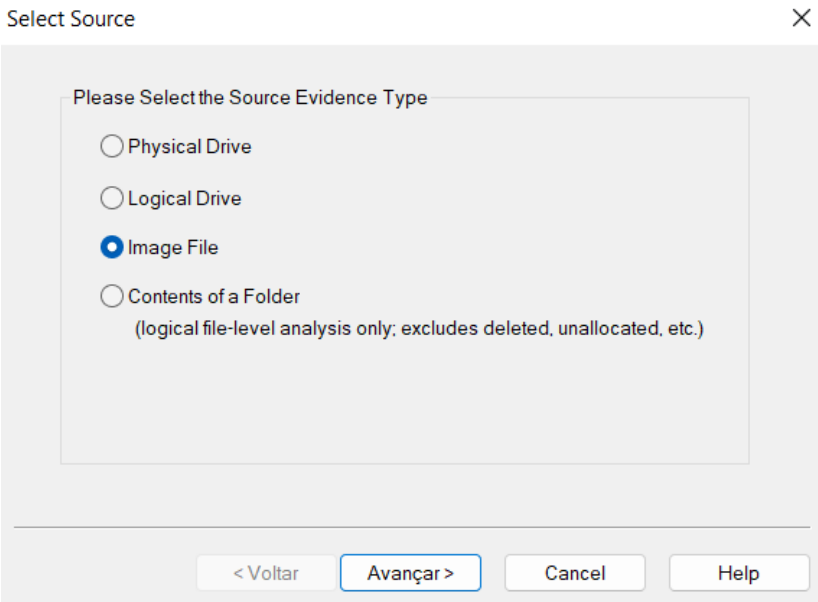

Figura 18: Selecionar tipo de Evidência
Fonte: O autor (2023)

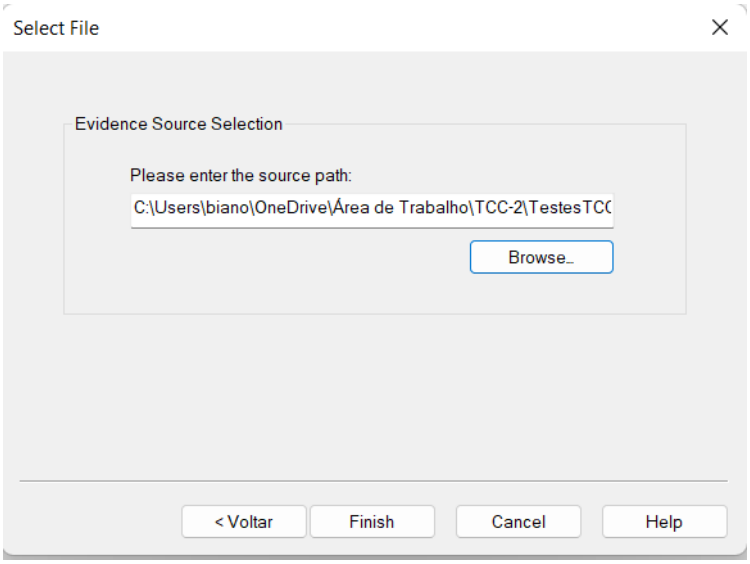

Figura 19: Selecionar Evidência
Fonte: O autor (2023)

Após a importação da evidência, basta dar início à análise, através da tela inicial do FTK *Imager* (Figura 20).

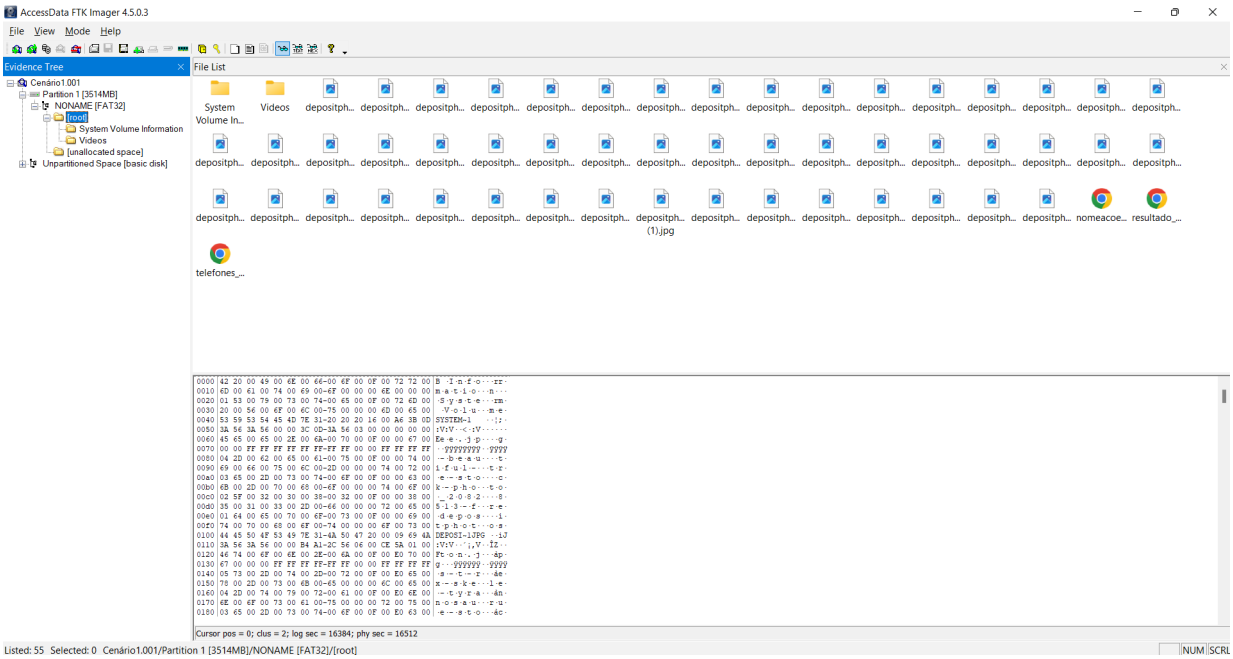

Figura 20: Tela Inicial FTK Imager
Fonte: O autor (2023)

4.3 AutoPsy

Ao iniciar o *software AutoPsy*, uma aba é apresentada. É necessário acessar a opção *New Case* (Figura 21), onde será possível informar dados importantes sobre o caso em questão, como o nome do caso e a pasta de destino onde os dados da análise serão armazenados (Figura 22).

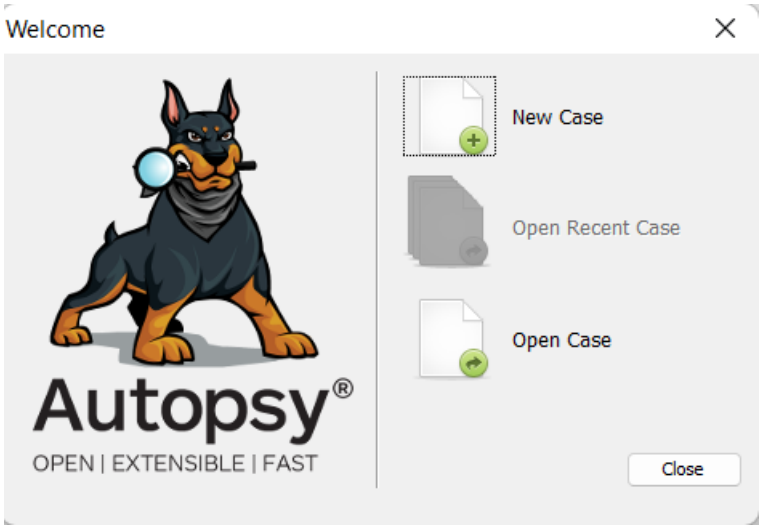

Figura 21: Novo Caso AutoPsy
Fonte: O autor (2023)

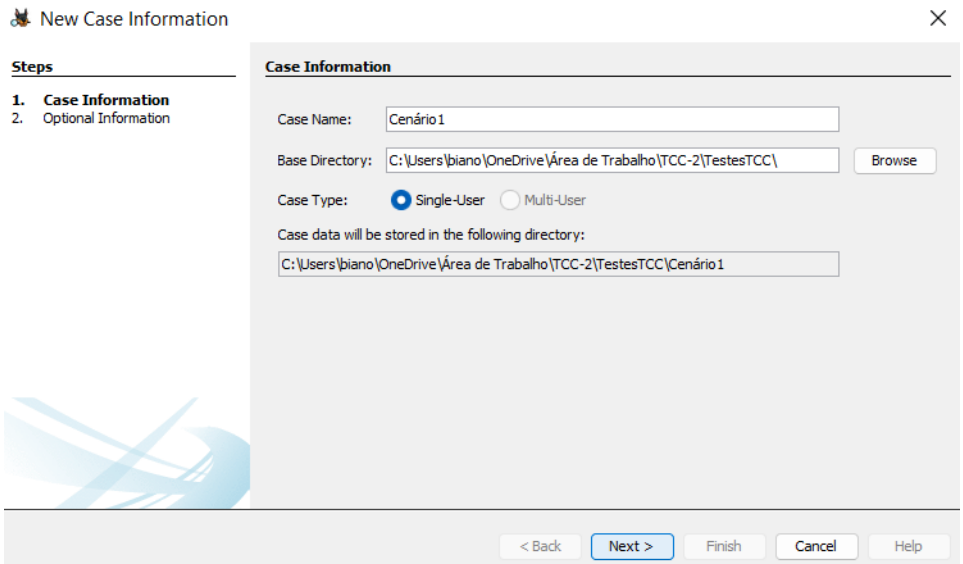

Figura 22: Informações sobre o Caso AutoPsy
Fonte: O autor (2023)

Em seguida, será necessário informar um host (Figura 23), escolher o tipo de fonte da evidência (Figura 24) e a fonte dos dados (Figura 25).

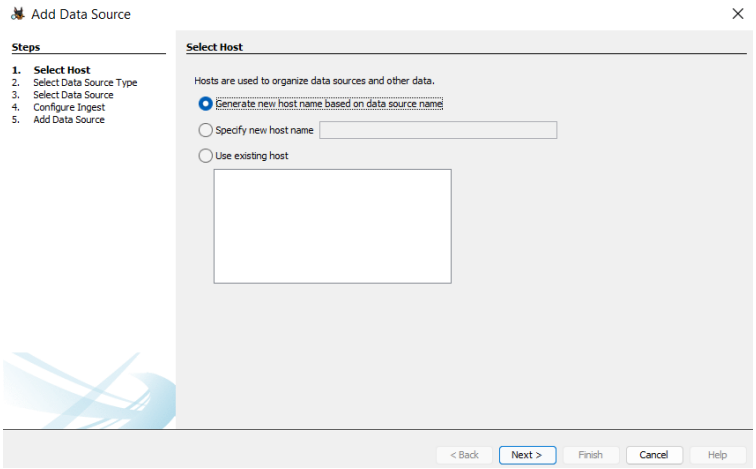

Figura 23: Selecionar Host AutoPsy
Fonte: O autor (2023)

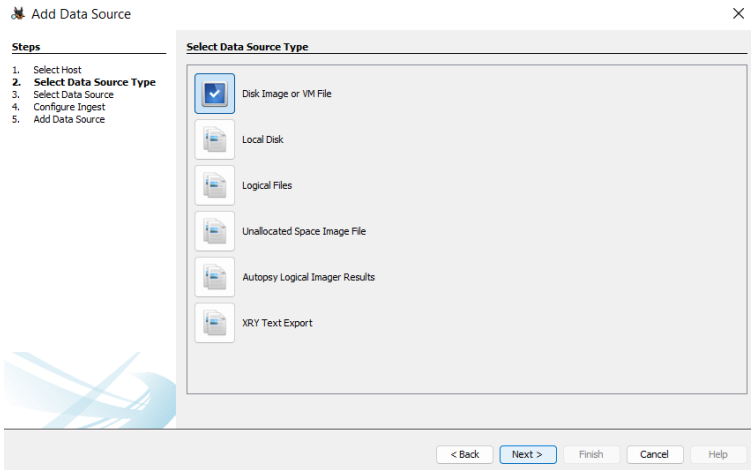

Figura 24: Selecionar tipo de Evidência AutoPsy
Fonte: O autor (2023)

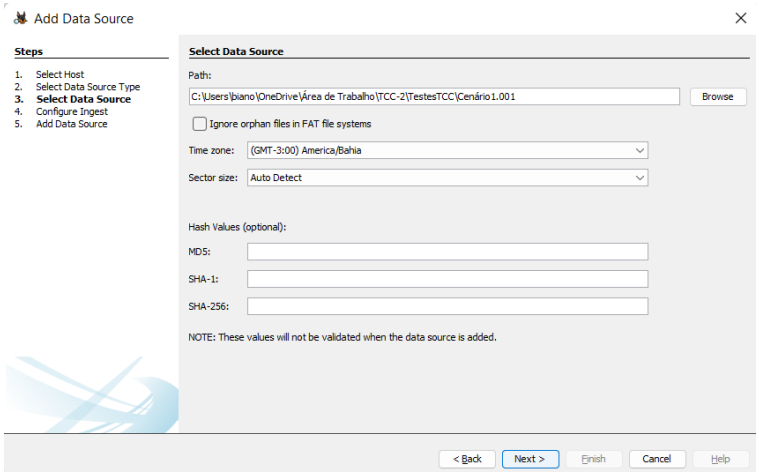

Figura 25: Selecionar Evidência AutoPsy
Fonte: O autor (2023)

Uma vez que a evidência foi incluída, é possível selecionar os módulos a serem utilizados na análise, como a detecção de criptografia e a geração de *hash* (Figura 26). Após a seleção dos módulos, o sistema informa que a evidência foi incluída com sucesso (Figura 27).

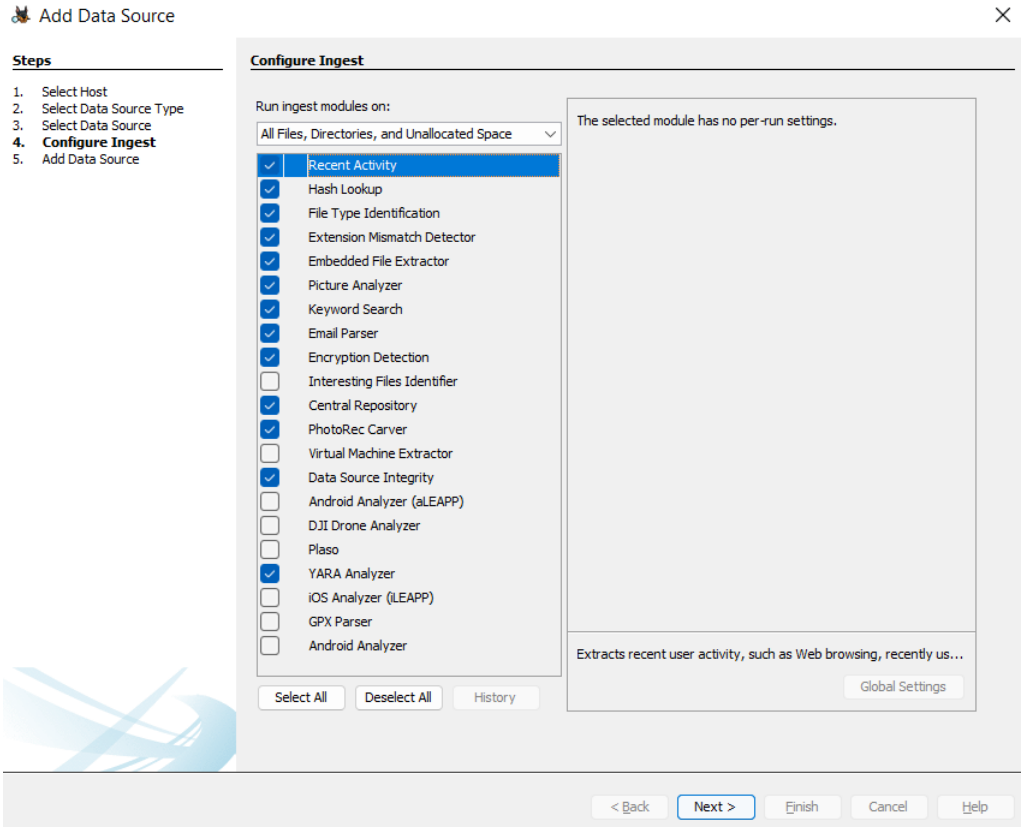

Figura 26: Selecionar Módulos AutoPsy
Fonte: O autor (2023)

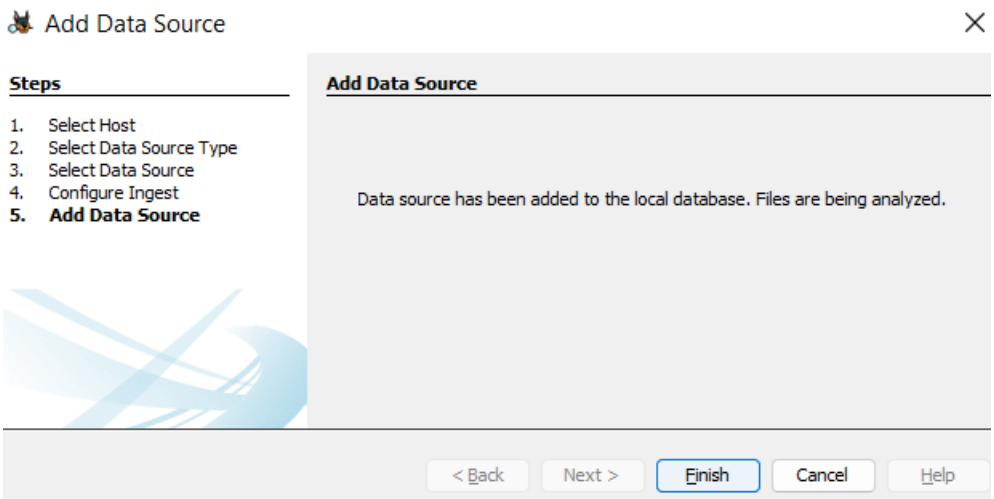

Figura 27: Evidência Adicionada AutoPsy
Fonte: O autor (2023)

Finalmente, para iniciar a análise, basta navegar pelas ferramentas e informações contidas na tela inicial do *software* (Figura 28), acessando as informações relevantes para o caso em questão e utilizando as ferramentas disponíveis para a investigação.

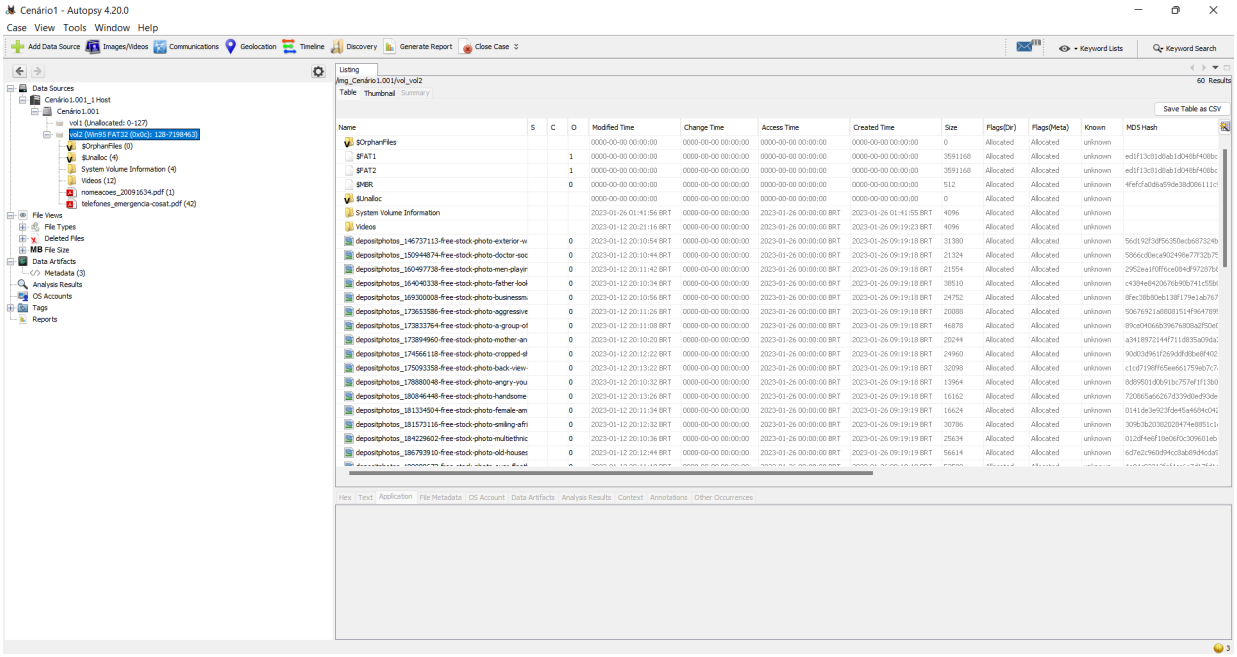

Figura 28: Tela Inicial AutoPsy
Fonte: O autor (2023)

5 RESULTADOS

Tendo realizado os experimentos descritos na seção 4, que consistiram na análise forense das mídias nas três ferramentas citadas, a capacidade de recuperação de arquivos foi analisada de acordo com os cenários propostos na seção 3.2. A Tabela 6 apresenta os resultados obtidos, mostrando a eficiência dos softwares IPED, FTK *Imager* e *AutoPsy* na recuperação de arquivos.

A fim de contextualizar, o primeiro cenário envolve um *Pendrive* montado de maneira convencional, contendo os dados selecionados para os testes. No segundo cenário, os dados foram adicionados e posteriormente excluídos manualmente. Já no terceiro cenário, os dados foram inicialmente incorporados ao dispositivo e, posteriormente, o *Pendrive* foi submetido a um processo de formatação. Por fim, no quarto cenário, os dados foram adicionados e, em seguida, o *Pendrive* foi submetido à sobrescrita completa com zeros, utilizando a técnica descrita na seção 2.2.1.

Arquivos Recuperados			
	Sistema		
Cenário	IPED	FTK Imager	AutoPsy
1	100%	100%	100%
2	100%	100%	100%
3	74,60%	0%	74,60%
4	0%	0%	0%

Tabela 6: Arquivos Recuperados
Fonte: O autor (2023)

No primeiro cenário investigado, que englobava uma mídia com arquivos previamente adicionados, constatou-se que as ferramentas IPED, FTK Imager e AutoPsy exibiram um desempenho equitativo no que tange à capacidade de recuperação dos dados. As três ferramentas demonstraram um bom desempenho ao recuperar a totalidade dos arquivos previamente inseridos, que consistiam em um conjunto de 50 imagens, 10 vídeos e 3 documentos.

No segundo cenário, no qual os arquivos foram excluídos manualmente, as três ferramentas mencionadas também se equipararam, recuperando todo o conteúdo presente na mídia submetida à análise.

Entretanto, a dinâmica mudou significativamente no terceiro cenário, no qual a mídia foi submetida a um processo de formatação. Nesse contexto, o FTK Imager mostrou-se incapaz de recuperar qualquer um dos 63 arquivos originais presentes na mídia, enquanto as ferramentas concorrentes, IPED e AutoPsy, permaneceram equiparados, conseguindo recuperar 34 imagens, 10 vídeos e 3 documentos, totalizando 47 arquivos do total original de 63.

Por fim, no quarto cenário, no qual a mídia foi submetida a um processo de sobrescrita, nenhuma das ferramentas conseguiu recuperar qualquer arquivo, o que evidencia a eficácia da técnica de sobrescrita descrita nesta pesquisa em tornar os dados anteriormente presentes na mídia irrecuperáveis por meio das ferramentas de recuperação de dados utilizadas.

Além da capacidade de recuperação de dados, a análise das ferramentas existentes e dos aspectos que podem auxiliar ou dificultar o trabalho do perito também foi avaliada, levando em consideração os critérios:

1. Boa usabilidade: Facilidade de uso e interface amigável, proporcionando uma experiência positiva ao usuário.

2. Bom desempenho: O desempenho das ferramentas foi levado em conta, verificando sua eficiência e velocidade na realização das tarefas de análise forense.

3. Bom sistema de indexamento: Capacidade das ferramentas em indexar e organizar os dados de forma eficiente, permitindo uma busca rápida e precisa.

4. Busca por expressão regular: Funcionalidade de realizar buscas utilizando expressões regulares, ampliando as opções de pesquisa e análise de dados.

5. Busca por palavra-chave: Funcionalidade de realizar buscas por palavras-chave, facilitando a identificação de informações relevantes nos dados analisados.

6. Cálculo de hash dos arquivos automaticamente ao gerar análise: Capacidade de calcular automaticamente o hash dos arquivos durante o processo de análise, garantindo a integridade dos dados.

7. Criação de coleções de evidências marcadas: Possibilidade de criação de coleções de evidências, permitindo a marcação e organização dos dados relevantes para a investigação.

8. Filtro por metadados: Funcionalidade de filtrar os dados com base em metadados, facilitando a identificação e análise de informações específicas.

9. Filtro por tipo de arquivo: Funcionalidade de filtrar os dados com base no tipo de arquivo, possibilitando uma análise mais direcionada e precisa.

10. Geração de relatório: Funcionalidade de gerar relatórios completos e detalhados das análises realizadas, facilitando a documentação e apresentação dos resultados.

11. Geração de imagem de disco: Funcionalidade de criar imagens de disco a partir dos dispositivos analisados, preservando a integridade dos dados e permitindo análises forenses mais aprofundadas.

12. Marcação de evidências: Possibilidade de marcar e destacar evidências encontradas durante a análise, facilitando a identificação posterior.

13. Pré-visualização dos arquivos: Funcionalidade de fornecer uma pré-visualização dos arquivos analisados, permitindo uma rápida visualização do conteúdo sem a necessidade de abrir cada arquivo individualmente.

14. Realização de todas as funções por interface gráfica: Foi verificado se todas as funções e recursos das ferramentas poderiam ser acessados e executados por meio de uma interface gráfica intuitiva.

15. Recuperação de arquivos apagados manualmente: Eficiência das ferramentas na recuperação de arquivos que foram apagados manualmente, verificando sua capacidade de restaurar dados deletados.

16. Recuperação de arquivos após formatação: Eficiência das ferramentas em recuperar arquivos após formatação dos dispositivos.

O resultado dessa análise de forma sintetizada está apresentada na Tabela 7, demonstrando a facilidade de uso, a precisão e a eficiência das ferramentas presentes em cada software.

Comparação			
	Sistema		
Funcionalidade	**IPED**	**FTK**	**AutoPsy**
Boa usabilidade	Sim	Não	Sim
Bom desempenho	Sim	Sim	Sim
Bom sistema de Indexamento	Sim	Não	Sim
Busca por expressão regular	Sim	Não	Sim
Busca por palavra-chave	Sim	Não	Sim
Calcula hash dos arquivos automaticamente ao gerar análise	Sim	Não	Sim
Criar coleções de evidências marcadas	Sim	Não	Não
Filtro por metadados	Sim	Não	Não
Filtro por tipo de arquivo	Sim	Não	Sim
Gera Relatório	Sim	Não	Sim
Geração de imagem de disco	Não	Sim	Não
Interface amigável	Sim	Não	Sim
Marcar evidências	Sim	Não	Sim
Preview dos arquivos	Sim	Não	Sim
Realiza todas as funções por interface gráfica	Não	Sim	Sim
Recupera arquivos apagados manualmente	Sim	Sim	Sim
Recupera arquivos após formatação	Em parte	Não	Em parte

Tabela 7: Ferramentas e Pontos analisados
Fonte: O autor (2023)

Com base nos resultados obtidos, podemos concluir que o IPED oferece uma experiência de usuário altamente amigável, tornando-o acessível a investigadores com diferentes níveis de habilidade. Além disso, possui ferramentas que podem ser o diferencial entre os sistemas apresentados, como o filtro por metadados, a busca por palavra-chave e a geração automática de hashes que são funcionalidades úteis para a identificação de evidências relevantes. Entre as três opções aqui analisadas, é a que possui o melhor sistema de indexamento. No entanto, o IPED apresenta desvantagens, como a ausência de geração de imagem de disco, o que pode ser problemático em cenários que requerem essa funcionalidade, forçando ao examinador a utilizar uma outra ferramenta para esse fim, e depois submeter a análise ao IPED.

O FTK Imager tem uma vantagem em cima das demais ferramentas apresentadas devido a funcionalidade de geração de imagem de disco, um dos pontos cruciais para se iniciar a análise das evidências, além do fato de realizar todas as funções por meio de uma interface gráfica, que pode ser benéfico para investigadores menos experientes. Entretanto, sua interface pode ser complexa para iniciantes, seu sistema de indexamento dificulta a navegação entre as evidências encontradas e a falta de

suporte para recuperação de dados após formatação pode ser uma desvantagem em determinados cenários.

Por fim, o AutoPsy também possui uma usabilidade amigável e oferece um bom sistema de indexamento para facilitar a busca de evidências. Bem como o IPED, o AutoPsy também carece de funcionalidades críticas, como a geração de imagem de disco.

6 CONCLUSÃO

Ao longo desta pesquisa, foi possível avaliar a eficácia da ferramenta IPED na recuperação de informações relevantes e sua capacidade de identificar e recuperar dados específicos. Através da comparação com outras ferramentas, como o FTK *Imager* e o *AutoPsy*, foi possível constatar que a ferramenta IPED se destaca pelos recursos disponíveis, como a capacidade de processamento de imagens, categorização de arquivos, *data carving*, detecção de arquivos criptografados, cálculo e consulta a base de hashes, detecção de expressões regulares e indexação de conteúdo. Apenas o FTK *Imager* obteve um menor desempenho. O *AutoPsy* apresentou resultados técnicos bem similares, diferindo em aspectos mais simples como estética, filtros e indexação de arquivos, pontos nos quais o IPED se sobressai.

É importante mencionar que esses resultados foram obtidos em um ambiente controlado, e podem variar dependendo do cenário específico da perícia.

Conclui-se, portanto, que a ferramenta IPED oferece recursos avançados para a análise de dados em perícias digitais e facilidade de uso, garantindo a recuperação eficiente de informações relevantes em cenários de perícia digital.

6.1 Trabalhos Futuros

Como trabalhos futuros, sugere-se ampliar a escala dos experimentos realizados, utilizando massas de dados mais complexas e diversificadas, a fim de avaliar a capacidade da ferramenta IPED em lidar com cenários mais desafiadores. Além disso, é importante realizar testes em diferentes ambientes e dispositivos, a fim de avaliar a robustez e eficácia da ferramenta em diferentes situações. Outra sugestão é realizar comparações com outras ferramentas de análise de dados existentes no mercado que não foram abordadas nesta pesquisa. Também seria interessante explorar as possibilidades de automatização dos processos de análise, utilizando técnicas de inteligência artificial e machine learning, para otimizar a eficiência e precisão dos resultados.

REFERÊNCIAS

ALMEIDA, J. de J. et al. Crimes cibernéticos. *Caderno de Graduação-Ciências Humanas e Sociais-UNIT-SERGIPE*, v. 2, n. 3, p. 215–236, 2015. Citado na página 12.

ALMEIDA, R. Perícia forense computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais. *Trabalho de Conclusão de Curso, FATEC/SP*, 2011. Citado 2 vezes nas páginas 17 e 21.

ARANHA, O. *Queira o Sr. Perito detalhar o procedimento de cópia forense*. 2015. Disponível em: <https://qperito.wordpress.com/2015/08/05/queira-o-sr-perito-detalhar-o-procedimento-tecnico-para-realizacao-de-uma-copia-forense/>. Acesso em: 03 ago. 2022. Citado na página 18.

AUTOPSY. *AutoPsy - Digital Forensics*. 2023. Disponível em: <https://www.autopsy.com/>. Acesso em: 25 nov. 2023. Citado na página 32.

EaseUS BitWiper. *EaseUS BitWiper*. 2023. Disponível em: <https://br.easeus.com/bitwiper/>. Acesso em: 25 nov. 2023. Citado na página 22.

ELEUTÉRIO, P. M. da S.; MACHADO, M. P. *Desvendando a computação forense*. [S.l.]: Novatec Editora, 2019. Citado 4 vezes nas páginas 17, 18, 20 e 21.

FTK Imager. *FTK Imager*. 2023. Disponível em: <https://www.exterro.com/ftk-imager>. Acesso em: 25 nov. 2023. Citado na página 32.

KEMP, S. *Digital 2022: Global Overview Report*. 2022. Disponível em: <https://datareportal.com/reports/digital-2022-global-overview-report>. Acesso em: 03 ago. 2022. Citado na página 11.

KENT, K.; CHEVALIER, S.; GRANCE, T. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86*, 2006. Citado 2 vezes nas páginas 16 e 20.

MARQUES, P. P. L. d. C. *Informática forense: recolha e preservação da prova digital*. Tese (Doutorado), 2013. Citado 2 vezes nas páginas 12 e 13.

MARTINS, D. M. B. et al. Algoritmos de hash camaleão. Florianópolis, SC., 2017. Citado 2 vezes nas páginas 18 e 19.

MEDEIROS, L. d. O. Análise de ferramentas open source utilizadas para a perícia forense computacional. 2020. Citado na página 12.

QUEIROZ, C.; VARGAS, R. *Investigação e perícia forense computacional*. [S.l.]: Brasport, 2010. Citado 2 vezes nas páginas 12 e 19.

SEPINF, S. *IPED*. 2023. Disponível em: <https://github.com/sepinf-inc/IPED>. Acesso em: 25 nov. 2023. Citado na página 32.

SOUZA, P. de. Perícia forense computacional: procedimentos, ferramentas disponíveis e estudo de caso. *Santa Maria: UFSM*, 2015. Citado 4 vezes nas páginas 12, 16, 17 e 20.