UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

EANDRO CLEITON ARAÚJO BRASIL

IDENTIFICAÇÃO E ANÁLISE DAS FERRAMENTAS DE COMPUTAÇÃO FORENSE APLICADAS EM INVESTIGAÇÕES NO BRASIL

QUIXADÁ

2023

EANDRO CLEITON ARAÚJO BRASIL

IDENTIFICAÇÃO E ANÁLISE DAS FERRAMENTAS DE COMPUTAÇÃO FORENSE APLICADAS EM INVESTIGAÇÕES NO BRASIL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas De Informação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas De Informação.

Orientador: Prof. Me. Roberto Cabral Rabêlo Filho.

QUIXADÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B83i Brasil, Eandro Cleiton Araújo.
Identificação e análise das ferramentas de computação forense aplicadas em investigações no Brasil / Eandro Cleiton Araújo Brasil. – 2023.
79 f. : il.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Sistemas de Informação, Quixadá, 2023.
Orientação: Prof. Me. Roberto Cabral Rabêlo Filho.

1. Computação Forense. 2. Ferramentas Forenses. 3. Norma ABNT ISO/IEC 27037:2013. 4. Processo Forense. I. Título.

CDD 005

EANDRO CLEITON ARAÚJO BRASIL

IDENTIFICAÇÃO E ANÁLISE DAS FERRAMENTAS DE COMPUTAÇÃO FORENSE APLICADAS EM INVESTIGAÇÕES NO BRASIL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas De Informação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas De Informação.

Aprovada em:

BANCA EXAMINADORA

Prof. Me. Roberto Cabral Rabêlo Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Arthur de Castro Callado
Universidade Federal do Ceará (UFC)

Prof. Me. Marcos Dantas Ortiz
Universidade Federal do Ceará (UFC)

À minha família, gostaria de expressar minha sincera gratidão por sempre acreditarem em mim e pelo apoio que me deram ao longo do caminho. Mãe, seu cuidado e dedicação foram especialmente significativos e me deram forças nos momentos mais desafiadores.

AGRADECIMENTOS

Ao Prof. Me. Roberto Cabral Rabêlo Filho, pela excelente orientação.

Aos professores participantes da banca examinadora, Dr. Arthur de Castro Callado e Me. Marcos Dantas Ortiz, expresso minha sincera gratidão pelo tempo dedicado, assim como pelas valiosas colaborações e sugestões oferecidas.

“É um erro grave formular teorias antes de conhecer os fatos. Sem querer, começamos a mudar os fatos para que se adaptem às teorias, em vez de formular teorias que se ajustem aos fatos.” (Arthur Conan Doyle, 1888, A Study in Scarlet ch. 3)

RESUMO

O presente trabalho tem como objetivo central investigar a aplicação e análise das ferramentas de computação forense nas investigações no Brasil, em conformidade com a norma ABNT ISO/IEC 27037:2013. A pesquisa abrangeu as etapas estabelecidas pela norma, que compreendem a identificação, coleta, aquisição e preservação de evidências digitais. Foram selecionadas quatro ferramentas relevantes para cada etapa, com base em critérios como funcionalidades, confiabilidade e conformidade com as práticas forenses aceitas. Por meio de uma revisão bibliográfica abrangente, foram levantadas informações sobre as características e funcionalidades dessas ferramentas, a fim de fornecer um guia útil para profissionais e pesquisadores da área. Os resultados indicam que a aplicação adequada das ferramentas de computação forense, em conformidade com a norma, desempenha um papel fundamental na coleta, análise e preservação das evidências digitais, garantindo sua integridade, autenticidade e admissibilidade nos processos legais. Recomenda-se que os profissionais da área estejam atualizados com as evoluções tecnológicas e as atualizações das normas, a fim de aprimorar constantemente seus conhecimentos e práticas no campo da computação forense. Espera-se que este estudo contribua para o avanço das investigações digitais no Brasil, fornecendo uma visão abrangente das ferramentas efetivas disponíveis e destacando a importância da conformidade com as diretrizes da norma.

Palavras-chave: computação forense; ferramentas forenses; norma ABNT ISO/IEC 27037:2013; processo forense.

ABSTRACT

The present study aims to investigate the application and analysis of computer forensic tools in investigations in Brazil following the ABNT ISO/IEC 27037:2013 standard. The research encompasses the stages established by the standard, which include the identification, collection, acquisition, and preservation of digital evidence. Four relevant tools were selected for each stage based on functionality, reliability, and compliance with accepted forensic practices. A comprehensive literature review gathered information on the characteristics and functionalities of these tools to provide a valuable guide for professionals and researchers in the field. The results indicate that the proper application of computer forensic tools, following the standard, plays a fundamental role in collecting, analyzing, and preserving digital evidence, ensuring its integrity, authenticity, and admissibility in legal proceedings. It is recommended that professionals stay updated with technological advancements and standard updates to improve their knowledge and practices in computer forensics continuously. This study is expected to contribute to the advancement of digital investigations in Brazil by providing a comprehensive overview of practical tools available and highlighting the importance of compliance with the guidelines of the standard.

Keywords: computer forensics; forensic tools; ABNT ISO/IEC 27037:2013 standard; forensic process.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT/CB-21	Comitê Brasileiro de Computadores e Processamento de Dados
ADB	Android Debug Bridge
AF	Anti-forense
API	Application Programming Interface
BSD	Berkeley Software Distribution
CE-21:027.00	Comissão de Estudo de Técnicas de Segurança
COVID-19	Coronavirus Disease 2019
CPP	Código de Processo Penal
DFF	Digital Forensics Framework
DLL	Dynamic-link Library
DNA	Ácido desoxirribonucleico
DNS	Domain Name System
DOS	Disk Operating System
ExTFS	Extended File System
FAT	File Allocation Table
FEX	Forensic Explorer
FTK	Forensic Toolkit
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IPED	Indexador e Processador de Evidência Digital
ISO	International Organization for Standardization
ISO/IEC JTC	Joint Technical Committee Information Technology
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MAC	Macintosh
MMS	Multimedia Message System
NIST	Institute of Standards and Technology
NTFS	New Technology File System

RAM	Random Access Memory
SC 27	Subcommittee IT Security Techniques
SCADA	Supervisory Control And Data Acquisition
SMS	Short Message Service
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TI	Tecnologia da Informação
TSK	The Sleuth Kit
URL	Uniform Resource Locator
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
XML	Extensible Markup Language
XWF	X-Ways Forensics

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, o progresso tecnológico tem dado origem a uma variedade de crimes, entre os quais o cibercrime se destaca. Esse termo abrange uma gama de atividades criminosas perpetradas por meio da internet e de outras tecnologias digitais. Incluem-se nessa categoria invasões de sistemas, roubo de informações pessoais e financeiras, e uma série de outros delitos (MONTEIRO, 2016).

O avanço tecnológico também tem impulsionado o aprimoramento crimes tradicionais. A falsificação de documentos, o tráfico de drogas, o *bullying*, o assédio sexual e a disseminação de discursos de ódio são apenas alguns exemplos dessas modalidades aperfeiçoadas. Além disso, as organizações criminosas têm expandido sua atuação graças às oportunidades oferecidas pela tecnologia.

Em contrapartida, nos últimos cem anos, a ciência tem experimentado um progresso exponencial, fornecendo às investigações criminais um vasto conjunto de ferramentas e técnicas com potencial inestimável (FACHONE; VELHO, 2007). Como resultado, as investigações criminais se tornaram mais desafiadoras e complexas, não se limitando mais somente a confissões e testemunhos.

Atualmente, dispõe-se de métodos avançados e precisos, como análises de Ácido desoxirribonucleico (DNA), reconhecimento facial e análise forense de dispositivos eletrônicos, que ampliam ainda mais as possibilidades de investigação.

Diante desse contexto, surgiu a necessidade de estabelecer técnicas padronizadas de análise e investigação criminal, visando auxiliar na resolução dessas infrações. Esse processo culminou no desenvolvimento da ciência forense. Conforme definido por Saferstein (2018), essa disciplina abrange a aplicação de conhecimentos científicos e tecnológicos no campo jurídico, com o intuito de promover uma execução mais eficiente das leis.

A ciência forense, baseada no princípio da Troca de Locard estabelecido por Locard (1925), sustenta que cada contato deixa uma evidência. Conforme essa premissa, mesmo que essas evidências só possam ser identificadas por meio de análises microscópicas ou com o auxílio de equipamentos altamente precisos, sempre existirão vestígios a serem descobertos.

Com o progresso das tecnologias da informação, a ciência forense viu-se obrigada a ampliar sua compreensão de local de crime, que anteriormente se limitava a um espaço físico contendo vestígios de atividades criminosas (ELEUTéRIO; MACHADO, 2011). Atualmente, o conceito de local de crime abrange também ambientes digitais, nos quais valiosas evidências

eletrônicas podem ser encontradas para a solução de crimes. Muitas vezes, esses ambientes digitais atuam como a principal ferramenta utilizada para cometer transgressões à lei.

Conforme destacado por Pereira e Oliveira (2019), a Perícia Forense Computacional, também conhecida como Análise Digital Forense, tem como objetivo combater os crimes digitais por meio do uso de análises e métodos que visam identificar e coletar evidências de forma válida e eficaz. Durante o processo de análise de vestígios digitais, um perito especializado nessa área deve seguir uma série de diretrizes, a fim de preservar as evidências virtuais e garantir que seu valor jurídico não seja comprometido.

A motivação deste trabalho surge da constante evolução da área de computação forense, que demanda cada vez mais técnicas e procedimentos para combater e identificar infrações cometidas em dispositivos computacionais. Nesse contexto, o domínio de ferramentas e técnicas forenses torna-se fundamental para profissionais especializados em segurança da informação, possibilitando a seleção adequada de dispositivos e a condução de processos de investigação específicos.

Com o objetivo de apresentar as ferramentas de computação forense utilizadas no contexto atual do Brasil, este trabalho organizou essas ferramentas de acordo com cada fase do processo estabelecido pelas diretrizes para identificação, coleta, aquisição e preservação de evidência digital, conforme a norma ISO/IEC 27037 (2013). Em cada etapa, foram apresentadas atividades realizadas em cada uma e ferramentas que podem ser aplicadas durante essas diligências.

1.1 Objetivos

Esta seção tem como objetivo delinear, de forma clara e objetiva, os principais propósitos deste trabalho de conclusão de curso. O estudo tem como meta investigar e apresentar as ferramentas de computação forense em uso no cenário atual brasileiro, além de abordar a norma que busca orientar a prática da computação forense e da perícia criminal no país. Por meio da análise das diretrizes da ISO/IEC 27037 (2013) para a gestão de evidências digitais, foram identificadas as etapas fundamentais do processo de computação forense, assim como as técnicas e ferramentas recomendadas para cada uma delas.

1.1.1 Objetivo Geral

Apresentar e classificar as ferramentas de computação forense utilizadas no cenário atual brasileiro, bem como relacionar a norma que busca auxiliar na computação forense e a perícia criminal no Brasil.

1.1.2 Objetivos Específicos

Foram estabelecidos os seguintes objetivos específicos:

- Analisar as diretrizes para a gestão de evidências digitais estabelecidas pela norma ISO/IEC 27037 (2013) e compreender suas implicações na área da computação forense no Brasil.
- Estabelecer as fases do processo de gestão e identificar as principais técnicas utilizadas em cada uma das fases.
- Apresentar ferramentas, termos e práticas disponíveis dentro de cada fase de uma análise forense computacional.

2 FUNDAMENTAÇÃO TEÓRICA

Este trabalho tem como propósito realizar um estudo abrangente sobre as ferramentas de computação forense utilizadas em investigações criminais no Brasil. Para alcançar esse objetivo, é fundamental possuir um conhecimento sobre os termos técnicos utilizados no campo pericial e sua relevância para o processo investigativo.

2.1 Ciência Forense

O conceito de "ciência" abrange uma série de abordagens sistemáticas voltadas para a compreensão do mundo físico. Por outro lado, o adjetivo "forense" atribui-se à aplicação dessas abordagens a questões de interesse público ou jurídico. Quando unidos, esses termos formam a expressão "ciência forense", que é adequada para descrever a ocupação dos cientistas que utilizam essas abordagens metodológicas para responder a questionamentos apresentados em contextos judiciais, oferecendo relatórios e testemunhos (HOUCK; SIEGEL, 2015).

A ciência forense desempenha um papel fundamental no contexto do direito civil e penal, fornecendo uma técnica aplicada que traz benefícios significativos. À medida que a sociedade se tornou mais complexa, a dependência das regras legais para regular as ações individuais na coletividade aumentou consideravelmente (SAFERSTEIN, 2018). Por meio de uma abordagem científica sistemática, a ciência forense desvenda casos de alta complexidade, contribuindo assim para preservar a integridade do sistema legal e garantir sua eficácia.

Além disso, segundo Saferstein (2018), essa ciência é incumbida de fornecer informações precisas e objetivas sobre os eventos ocorridos em uma cena de crime. Desse modo, a ciência forense é a aplicação de técnicas e métodos científicos às leis criminais e civis, conduzida por agências policiais em colaboração com especialistas de diversas áreas.

Trata-se da utilização de métodos científicos e técnicas em questões de interesse jurídico-policiais. Dessa forma, todas as áreas científicas podem ser manipuladas com o intuito de responder a questionamentos de ordem legal e criminal, o que faz com que a ciência forense esteja inserida em todas as áreas do conhecimento (VELHO *et al.*, 2011).

Para Rodrigues *et al.* (2011), são estabelecidas conexões vitais com diversos grupos nesse processo: juízes, promotores, delegados de polícia, médicos legistas, papiloscopistas, universidades, fornecedores de tecnologia, policiais, vítimas, suspeitos, testemunhas, organizações de direitos humanos, mídia e presidentes de comissões de inquérito. Essas conexões são

essenciais para a busca da verdade e promoção da justiça pela ciência forense.

Dessa forma, é necessário compreender os seus princípios fundamentais e os diversos públicos que a ciência forense precisa lidar, visto que eles moldam a maneira como os cientistas forenses devem conduzir suas investigações.

2.2 Computação Forense

A área da computação forense é especializada em investigar crimes e evidências relacionados a dispositivos computacionais. Essa expertise pericial não se limita apenas a computadores, mas engloba também dispositivos móveis, assistentes digitais pessoais, redes e outros dispositivos que armazenam ou processam informações digitais. Conforme destacado por Maras (2015), a computação forense abrange todo o processo de coleta, análise, processamento, inspeção e armazenamento de dados digitais, com o propósito de utilizá-los como prova em processos criminais, casos civis e administrativos.

De acordo com a visão de Nelson *et al.* (2019), a computação forense, também conhecida como análise forense digital, é uma área profissional consolidada, embora ainda conte com muitos especialistas autodidatas. Nesse contexto, é crucial adotar uma abordagem metodológica e científica, pois tem havido um aumento significativo no uso de computadores como ferramenta em infrações criminais, incluindo violações de políticas empresariais, apropriação indébita, assédio por e-mail, assassinato, vazamentos de informações proprietárias e até mesmo atos de terrorismo.

Com o aumento da demanda por investigações digitais resultante do crescimento da internet e da disseminação global dos computadores, profissionais como administradores de rede, advogados e investigadores privados têm se beneficiado das habilidades dos especialistas forenses digitais. Esses especialistas são essenciais para investigar casos criminais e civis relacionados ao ciberespaço[1](NELSON *et al.*, 2019).

O objetivo primordial da Computação Forense é estabelecer a dinâmica, materialidade e autoria de delitos no campo da informática, por meio da identificação e análise de evidências digitais. Esse processo é conduzido por meio de métodos técnico-científicos que atribuem validade probatória às evidências materiais dos crimes durante o processo judicial (ELEUTéRIO; MACHADO, 2011).

[1] Ciberespaço: espaço das comunicações por redes de computação.

2.3 Dispositivos computacionais

Os dispositivos computacionais abrangem uma ampla gama de dispositivos eletrônicos capazes de armazenar ou processar dados digitais, como computadores, *smartphones*, *tablets*, dispositivos de armazenamento externo, entre outros. É essencial destacar a importância de identificar todos os dispositivos relevantes para uma investigação e tomar as medidas adequadas para garantir a preservação e a coleta dos dados de maneira aceitável juridicamente, conforme ressaltado por (CARRIER, 2005).

Os dispositivos computacionais podem ser classificados em diferentes tipos, como: computadores pessoais, incluindo *desktops* e *laptops*; dispositivos móveis, como *tablets* e *smartphones*; periféricos, como impressoras, *scanners* e câmeras; dispositivos de armazenamento, como discos rígidos, unidades *flash Universal Serial Bus (USB)* e cartões de memória; dispositivos de rede, incluindo roteadores, *switches* e *modems*; e outros dispositivos conectados a um computador, como *webcams*, microfones e alto-falantes (BIGELOW, 2020).

A variedade de dispositivos mencionada anteriormente acrescenta uma camada de complexidade à investigação forense, demandando habilidades e conhecimentos técnicos específicos para lidar com cada tipo de dispositivo e suas peculiaridades. Portanto, é essencial que os investigadores possuam um amplo conhecimento sobre a extensa gama de dispositivos computacionais disponíveis, incluindo suas configurações, sistemas operacionais, arquiteturas e tecnologias envolvidas. Essa expertise é fundamental para realizar uma análise adequada das evidências digitais.

2.4 Crimes Cibernéticos

Para Eleutério e Machado (2011), os sistemas computacionais e a internet desempenham um papel fundamental em diversas atividades do dia a dia. Essas ferramentas permitem a busca de conhecimento em áreas de interesse, viabilizando também a execução de tarefas relacionadas ao ambiente corporativo. Além disso, proporcionam momentos de lazer, como a prática de jogos e o acesso à música.

Apesar dos benefícios trazidos pela tecnologia, é importante ressaltar que o crescente uso de sistemas computacionais e da internet também resultou no aumento significativo dos crimes cibernéticos, acarretando uma série de transtornos para a sociedade. De acordo com Eleutério e Machado (2011), tais infrações podem se valer dos computadores tanto como

instrumentos auxiliares na prática de delitos convencionais, como também como meios diretos de execução dos crimes em si.

O surgimento de crimes relacionados a computadores não é uma novidade, mas sim uma consequência do crescimento da conectividade global. Com o avanço da tecnologia, o desenvolvimento dos cibercrimes contemporâneos tornou-se praticamente inevitável. Hoje em dia, qualquer atividade criminosa que faça uso de um dispositivo eletrônico como instrumento, alvo ou meio para perpetuar crimes se enquadra no âmbito do crime cibernético, como afirmado por Chawki *et al.* (2015). Essa evolução representa um desafio significativo para a segurança digital e exige uma resposta efetiva por parte das autoridades e das políticas públicas.

De acordo com a visão de Chawki *et al.* (2015), o cibercrime pode ser definido de forma geral como "atos ilegais nos quais o computador é utilizado como ferramenta, alvo ou ambos". Essa abrangente definição engloba uma ampla variedade de crimes, que vão desde ataques a sistemas e redes, passando por fraudes online e violações da propriedade intelectual, até delitos mais graves, como pedofilia, terrorismo e espionagem.

É importante destacar que essa diversidade de crimes cibernéticos demanda uma abordagem abrangente e multidisciplinar para o combate efetivo a essas práticas ilegais.

2.4.1 Computador como apoio aos crimes convencionais

Uma das formas mais frequentes de cibercrime envolve o uso do computador como instrumento para facilitar a prática de crimes já existentes, como sonegação fiscal, compra de votos em eleições, tráfico de drogas e falsificação de documentos, entre outros. Nessas situações, a realização de exames forenses desempenha um papel fundamental na elaboração de laudos técnicos que podem auxiliar na tomada de decisão do juiz (ELEUTéRIO; MACHADO, 2011).

A utilização do computador como instrumento para a prática de atividades criminosas confere um valor significativo às evidências digitais, que desempenham um papel crucial na investigação e produção de provas técnicas. Os exames forenses desempenham um papel de extrema importância nessa área, garantindo a coleta, preservação e análise adequadas das evidências digitais, visando a identificação precisa da autoria e da dinâmica dos crimes em questão. Portanto, o emprego de tecnologias forenses no combate ao crime cibernético desempenha um papel crucial para assegurar a efetividade do sistema de justiça, como ressaltado por (ELEUTéRIO; MACHADO, 2011).

2.4.2 Computador como meio para a realização do crime

Ao contrário do uso do computador como suporte a crimes convencionais, também é possível que o próprio computador seja o meio para a realização do crime cibernético. Essa modalidade de delito envolve uma série de atividades, como ataques a sites, roubo de informações, *phishing*[2] e o uso de *malwares*[3] para a obtenção de senhas. Tais crimes só seriam viáveis com o auxílio de dispositivos computacionais. Vale ressaltar que, com o contínuo avanço tecnológico, novos delitos desse tipo surgem com frequência e sua incidência tem se mostrado em crescimento constante, conforme apontado por Eleutério e Machado (2011). É necessário estar atento a essas ameaças em constante evolução e adotar medidas de segurança apropriadas para mitigar os riscos associados.

2.5 Ferramentas de Computação Forense

No campo da computação forense, existem duas categorias principais de ferramentas: as de *hardware* e as de *software*. As ferramentas de *hardware* abrangem uma ampla gama de componentes, desde dispositivos simples e de propósito único até sistemas e servidores informáticos. Já as ferramentas de *software* são agrupadas em aplicativos de linha de comando e em formulários com *Graphical User Interface (GUI)*[4] (NELSON *et al.*, 2019).

Segundo as informações apresentadas por Johnson (2014), as ferramentas requeridas para uma investigação forense são determinadas pelos dados, arquivos, fontes e sistemas operacionais envolvidos. Cada sistema operacional apresenta características específicas em termos de *drivers*, bibliotecas de *software* e código do kernel, que precisam ser minuciosamente examinados. Dessa forma, o responsável pela equipe de análise forense tem a responsabilidade de garantir que as ferramentas adequadas estejam disponíveis no laboratório, devidamente licenciadas, aprovadas e certificadas para uso. Essa medida visa assegurar a conformidade com os padrões legais e técnicos exigidos durante o processo de investigação.

A fim de garantir a legalidade e a efetividade das investigações, é fundamental que cada ferramenta seja adquirida de forma legítima pela organização, seguindo um sistema de

[2] Phishing: termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online.

[3] Malware: programa malicioso, desenvolvido com a intenção de danificar computadores, servidores, clientes ou redes

[4] GUI: é uma interface visual para interação com dispositivos eletrônicos. Ela utiliza ícones e indicadores visuais, em vez de texto ou comandos digitados, tornando-a mais intuitiva para os usuários (WELLS, 2009)

aquisição regular. Além disso, é essencial que a equipe receba treinamento adequado para utilizar essas ferramentas de maneira eficiente e eficaz.

2.6 Anti-forense

A Anti-forense (AF) é uma técnica que visa comprometer a disponibilidade ou a utilidade das provas durante o processo forense. Seu objetivo é ocultar evidências ou manipular dados de forma a impedir que sejam acessíveis a um investigador posteriormente, conforme mencionado por Harris (2006). São uma série de métodos e técnicas que podem dificultar a recuperação e a análise forense de evidências digitais, tornando o trabalho dos investigadores mais desafiador.

De acordo com o artigo de Stüttgen e Cohen (2013), os ataques AF podem ser classificados em duas categorias principais. A primeira categoria abrange as técnicas que têm como objetivo impedir a obtenção de evidências. Isso pode ser alcançado por meio do uso de ferramentas que apagam ou modificam informações críticas nos sistemas ou dispositivos de armazenamento. O objetivo é dificultar ou impossibilitar a recuperação dessas informações pelos investigadores.

Já a segunda categoria de ataques anti-forenses envolve técnicas que removem dados dos indícios coletados, tornando as provas reunidas incompletas ou inutilizáveis para análise adequada. Essas técnicas podem incluir criptografia, ocultação de dados ou até mesmo a exclusão intencional de informações relevantes. O propósito dessas técnicas é impedir a descoberta de provas e tornar o processo de investigação mais desafiador, tornando a coleta e análise de evidências um processo demorado e complexo (STüTTGEN; COHEN, 2013).

Ambas as categorias de ataques anti-forenses têm em comum o objetivo de dificultar a investigação e evitar a descoberta de evidências sólidas. A compreensão dessas técnicas e o desenvolvimento de contramedidas adequadas são fundamentais para garantir a eficácia da análise forense digital e a obtenção de provas válidas.

2.7 Evidência Digital

De acordo com Maras (2015), o conceito de evidência digital abrange informações obtidas de sistemas de computadores ou dispositivos digitais, cuja finalidade é comprovar ou refutar uma infração ou violação de política, desde que a obtenção tenha ocorrido de maneira

legal. Em suma, a evidência digital engloba objetos ou informações relevantes para a investigação de um crime, extraídos de meios eletrônicos e utilizados em processos judiciais ou investigações. É crucial que a coleta de tais evidências siga as diretrizes legais para assegurar sua admissibilidade em um contexto jurídico.

É imprescindível na investigação forense digital a identificação e coleta das evidências eletrônicas pertinentes ao caso em análise. Segundo Marshall (2008), qualquer dado ou software presentes em um sistema digital podem ser considerados como provas, desde que tenham relevância para a investigação em curso. Nesse contexto, é crucial compreender a maneira pela qual essas informações foram inseridas no sistema, buscando detectar possíveis fontes de contaminação ou adulteração dos dados. Dessa forma, a análise das evidências digitais deve ser conduzida de modo meticuloso, empregando metodologias e técnicas específicas da investigação forense.

Conforme argumentado por Casey (2011), os dados digitais desempenham um papel abrangente em praticamente todos os aspectos de nossa vida diária, tornando sua coleta sistemática essencial em qualquer investigação. É altamente provável que, em algum momento, o suspeito tenha interagido com um computador, dispositivo móvel ou acesso à internet. Portanto, é crucial que todas as investigações corporativas considerem as informações relevantes armazenadas nos sistemas de computadores utilizados por seus funcionários, tanto no ambiente de trabalho quanto em suas residências.

Para evitar a necessidade de uma segunda determinação e a perda de oportunidades, é fundamental incluir a busca por evidências digitais durante o mandado de busca. Mesmo que esses dados não forneçam uma conexão direta entre o crime e a vítima, ou a infração e o perpetrador, eles podem desempenhar um papel valioso em uma investigação. As evidências digitais têm o potencial de revelar detalhes sobre a maneira como um crime foi cometido, fornecer pistas investigativas, corroborar ou refutar as declarações de testemunhas e identificar possíveis suspeitos. Portanto, é crucial considerar as informações armazenadas em dispositivos eletrônicos, que podem ser utilizadas como provas em um processo legal (CASEY, 2011).

2.8 Aspectos técnicos e legais

Conforme observado por Costa (2011), a computação forense abrange uma variedade de aspectos técnicos essenciais para garantir a qualidade e a eficiência das investigações. Esses aspectos abrangem desde a aplicação de padrões científicos na identificação, preservação, análise

e formalização das evidências, até considerações relacionadas à infraestrutura laboratorial, materiais periciais e qualificação dos profissionais envolvidos. Em suma, a perícia forense computacional é um processo complexo que demanda conhecimentos especializados e o uso de ferramentas adequadas para assegurar a integridade e confiabilidade das provas digitais coletadas. Ao analisar e compreender esses elementos, é possível fortalecer a solidez das investigações e facilitar o alcance de resultados conclusivos.

Por outro lado, os aspectos legais envolvidos na investigação forense computacional se referem às leis e normas que regem o processo judicial e a utilização das evidências digitais no contexto legal. Como apontado por Costa (2011), esses preceitos podem ser encontrados em diversas legislações, tais como o Código Penal, o Código de Processo Penal, o Código de Processo Civil, entre outras normas aplicáveis. Nesse sentido, é essencial que os profissionais envolvidos na perícia forense computacional tenham um conhecimento aprofundado das leis e regulamentos pertinentes, a fim de garantir que todo o processo seja conduzido de acordo com os requisitos legais e as normas éticas da profissão.

Conforme apontado por Eleutério e Machado (2011), o artigo 158 do Código de Processo Penal (CPP) estipula a obrigatoriedade de realizar um exame de corpo de delito nos casos em que a infração deixa vestígios, os quais não podem ser substituídos pela mera confissão do acusado, seja o exame direto ou indireto. Portanto, torna-se essencial que um especialista qualificado conduza a investigação forense computacional de maneira criteriosa, com o objetivo de identificar e analisar todos os vestígios digitais relevantes para a apuração do delito em questão. Somente por meio da elaboração de laudos técnicos precisos e confiáveis é possível fornecer à justiça subsídios sólidos no processo de tomada de decisões. Assim, a expertise do profissional responsável pela perícia se torna crucial na busca pela verdade e na garantia de um processo justo e imparcial.

Os artigos 159 e 160 do CPP estabelecem a obrigatoriedade de que o exame de corpo de delito e outras perícias sejam conduzidos por um perito oficial, devidamente habilitado com diploma de curso superior, responsável por elaborar um laudo pericial minucioso e responder aos questionamentos formulados. No âmbito da investigação forense computacional, essa função oficial é desempenhada pelo Perito Criminal em Informática (ELEUTéRIO; MACHADO, 2011). No entanto, é importante destacar que outros profissionais, como peritos particulares, auditores de sistemas, especialistas em Tecnologia da Informação (TI), entre outros, podem ser requisitados para realizar exames de computação em situações específicas. Embora não possuam o status

de peritos oficiais, esses profissionais podem desempenhar um papel relevante no contexto da análise forense digital, trazendo suas competências especializadas para contribuir com o processo de investigação.

Além disso, é relevante ressaltar que não apenas os profissionais técnicos devem possuir conhecimento sobre a correta coleta, análise e apresentação das evidências e provas digitais. Juízes, advogados, delegados, promotores e demais atores do sistema de justiça também devem compreender esses procedimentos, a fim de assegurar a validade e confiabilidade das provas digitais no âmbito jurídico. Conforme destacado por Eleutério e Machado (2011), é essencial que todos os envolvidos nesse processo tenham plena ciência das normas e procedimentos necessários para garantir a integridade e validade das provas digitais em uma investigação forense. Ao possuir esse conhecimento, os profissionais do sistema de justiça podem avaliar de forma adequada as evidências apresentadas, promovendo um julgamento justo e embasado em informações consistentes. Assim, a compreensão coletiva desses procedimentos é fundamental para a correta aplicação da justiça no contexto digital.

A estrutura legal da perícia forense computacional vai além do CPP, que estabelece normas gerais para a condução de perícias forenses. De fato, existem várias outras leis que são fundamentais nesse contexto. Essas regulamentações abrangem diferentes aspectos da investigação forense computacional, incluindo a proteção de dados pessoais, a interceptação de comunicações, a obtenção e análise de evidências digitais, entre outros. Portanto, é crucial que os profissionais envolvidos na perícia forense computacional estejam atualizados e familiarizados com essa complexa estrutura legal, a fim de garantir a conformidade com as regulamentações e a validade das evidências digitais apresentadas no âmbito jurídico.

2.8.1 Lei Geral de Proteção de Dados Pessoais

Lei nº 13.709/2018 entrou em vigor em setembro de 2020, após a prorrogação do início da vigência em função da pandemia da *Coronavirus Disease 2019 (COVID-19)*. A Lei Geral de Proteção de Dados Pessoais (LGPD) tem como propósito a definição de princípios, direitos dos titulares de dados e regras relativas ao tratamento de informações pessoais, bem como a imposição de sanções para o descumprimento de suas disposições. Seu principal objetivo é garantir a salvaguarda dos direitos fundamentais de liberdade e privacidade das pessoas, além de fomentar o livre desenvolvimento de sua personalidade, inclusive em ambientes digitais.(BRASIL, 2018).

Essa regulamentação da LGPD também busca estabelecer um ambiente de segurança jurídica, por meio da implementação de regulamentos e práticas padronizadas, visando à proteção dos dados pessoais de todos os cidadãos brasileiros, alinhada aos padrões internacionais existentes (BRASIL, 2018). Com isso, busca-se criar um ambiente confiável e seguro para o uso e tratamento de dados pessoais, tanto no setor público quanto no privado. Através dessa regulamentação, espera-se garantir a privacidade e a integridade dos dados, promovendo a confiança dos titulares de dados e fortalecendo as relações entre as organizações e os indivíduos.

A utilização de técnicas de perícia forense computacional na investigação de crimes digitais requer o cumprimento da LGPD para garantir a proteção dos dados pessoais das vítimas e suspeitos envolvidos no processo. Para Chaves *et al.* (2020) lei também estabelece a necessidade de consentimento informado dos titulares dos dados para a sua coleta e processamento, o que pode ser um fator relevante para a análise de evidências digitais em investigações criminais.

2.8.2 Marco Civil da Internet

O Marco Civil da Internet, também referido como Lei nº 12.965/2014, desempenha um papel fundamental ao estabelecer um conjunto de normas e diretrizes que regulamentam o uso da internet no Brasil. Promulgada em 23 de abril de 2014, essa legislação tem como objetivo primordial salvaguardar os direitos dos usuários online, assegurando-lhes a liberdade de expressão, a proteção da privacidade e a segurança dos dados na esfera virtual. Adicionalmente, o decreto nº 8.771/2016 foi criado para estabelecer diretrizes complementares e regulamentar alguns aspectos específicos dessa lei (BRASIL, 2014).

No contexto da perícia forense computacional, a legislação estabelece que os provedores de conexão e os provedores de aplicação de internet têm a responsabilidade de manter registros de acesso às aplicações online como uma medida essencial para a segurança e a integridade dos dados. Além disso, a lei prevê a possibilidade de emissão de ordens judiciais para a coleta de informações em ambientes digitais, visando a investigação de crimes cibernéticos (TAVARES, 2020). Em síntese, o Marco Civil da Internet é uma legislação abrangente e de suma importância, cujo objetivo é garantir os direitos e proteger os usuários da internet no Brasil.

2.8.3 Lei Carolina Dieckman

A Lei Carolina Dieckmann, também referida como Lei nº 12.737/2012, foi sancionada em 30 de novembro de 2012 e passou a vigorar em 2 de abril de 2013. Seu principal objetivo

é estabelecer a tipificação penal de delitos informáticos, abrangendo condutas como invasão de dispositivo, obtenção não autorizada, divulgação ou comercialização de dados pessoais (BRASIL, 2012). Essa legislação desempenha um papel fundamental ao oferecer proteção jurídica contra práticas ilícitas no âmbito digital.

Diante desse contexto, a perícia de computação forense tem desempenhado um papel crucial nas investigações de crimes digitais, possibilitando a coleta de evidências e contribuindo significativamente para o desenrolar dos processos judiciais. Essa prática especializada tem sido amplamente empregada para identificar autoria, reconstruir eventos, preservar a integridade das provas digitais e fornecer subsídios técnicos às autoridades competentes.

2.8.4 Lei de Acesso a Informação

A Lei de Acesso à Informação (LAI) ou Lei nº 12.527/2011 é uma legislação brasileira que entrou em vigor em 16 de maio de 2012, tendo como propósito garantir o direito dos cidadãos ao acesso a informações públicas. Essa lei estabelece a obrigatoriedade de todos os órgãos públicos, tanto da União quanto dos Estados, do Distrito Federal e dos Municípios, em fornecer informações de interesse público, com exceção dos casos previstos pela própria legislação. Buscando ainda transparência na gestão pública, garantindo aos cidadãos o acesso às informações como um direito fundamental (BRASIL, 2011).

O acesso às informações pode ser solicitado por qualquer pessoa, de forma gratuita e sem a necessidade de justificar o pedido, e o prazo estipulado para a disponibilização das informações é de até 20 dias. Dessa forma, busca-se fomentar uma maior participação da sociedade na fiscalização do uso dos recursos públicos e na gestão governamental.

Com base na LAI, os peritos em computação forense possuem a prerrogativa de solicitar informações e dados aos órgãos públicos quando estão envolvidos em investigações criminais ou civis, especialmente nos casos relacionados a crimes cibernéticos. Essa lei permite que esses profissionais requisitem informações específicas relevantes para a condução das investigações, facilitando a obtenção de elementos probatórios necessários para o caso em questão.

2.8.5 Lei das Perícias Oficiais

A Lei nº 12.030/2009, que entrou em vigor em 17 de setembro de 2009, estabelece diretrizes gerais sobre a realização de perícias oficiais no Brasil, com o objetivo de assegurar

a qualidade e a imparcialidade dessas investigações. A legislação determina que as perícias sejam conduzidas por profissionais devidamente habilitados e nomeados pelo poder público, estabelecendo critérios para sua nomeação, capacitação e atuação. A lei prevê a criação de instituições especializadas, como os Institutos de Criminalística e os Institutos Médico-Legais, com a finalidade específica de realizar perícias. Além disso, busca enfatizae que as perícias devem ser conduzidas de maneira imparcial, técnica e científica, visando à produção de provas que auxiliem em processos judiciais ou administrativos. Destacando importância da autonomia técnica e científica dos peritos, estabelecendo que eles devem atuar de forma independente e imparcial, sem estarem subordinados hierarquicamente a qualquer autoridade (BRASIL, 2009).

A perícia forense computacional está sujeita às normas dessa lei, pois ela garante que os peritos atuantes nessa área estejam devidamente habilitados e capacitados para desempenhar suas funções de forma técnica e imparcial. Estabelecendo também critérios para a nomeação e atuação dos peritos em computação forense, assegurando a qualidade e eficácia das perícias realizadas nesse campo específico e reforçando a importância da autonomia dos peritos, permitindo que eles exerçam suas atividades de forma independente, sem qualquer forma de subordinação hierárquica a autoridades (BRASIL, 2009). Dessa forma, a legislação contribui para a garantia da integridade e confiabilidade das perícias forenses computacionais, assegurando o cumprimento dos princípios de imparcialidade e competência técnica exigidos nesse tipo de investigação.

2.8.6 Lei do Software

A Lei do *Software*, oficialmente denominada Lei nº 9.609, foi promulgada no Brasil com o propósito de regular os direitos autorais relacionados a programas de computador. Sua entrada em vigor ocorreu em 19 de fevereiro de 1998. Essa legislação reconhece os programas de computador como bens protegidos pela lei de direitos autorais e estabelece diretrizes específicas para a reprodução, distribuição e comercialização desses programas. Em casos de violação dos direitos autorais dos programas de computador, a lei prevê sanções, incluindo a obrigação de pagar indenizações aos detentores desses direitos. Contudo, essa lei também contempla certas exceções, como o direito do usuário realizar cópias de segurança exclusivamente para seu próprio uso, desde que não haja intenção de obter lucro com isso (BRASIL, 1998).

A perícia forense computacional desempenha um papel fundamental na investigação e obtenção de evidências técnicas em situações de violação de direitos autorais de *software*. Além disso, a legislação exige a preservação das informações armazenadas nos sistemas durante

o processo de perícia, assegurando a integridade dos dados cruciais para a investigação. Portanto, esse regulamento desempenha um papel essencial na proteção dos direitos autorais de programas de computador e no suporte à perícia forense computacional em casos relacionados a esses direitos.

2.8.7 Lei do Processo Judicial Eletrônico

A Lei nº 11.419, popularmente conhecida como Lei do Processo Judicial Eletrônico, foi aprovada em 19 de dezembro de 2006 e passou a ser efetiva a partir de 20 de janeiro de 2007. Essa legislação introduziu o uso do processo judicial eletrônico como forma de conduzir os procedimentos legais, estabelecendo diretrizes para a utilização de meios eletrônicos na prática dos atos processuais e na comunicação entre os órgãos do sistema judiciário (BRASIL, 2006).

Está diretamente relacionada com a perícia digital forense, pois prevê a tramitação eletrônica de processos judiciais e a utilização de meios eletrônicos para realização de atos processuais, incluindo a produção de provas digitais (BRASIL, 2006). Com isso, a lei permite que a perícia digital forense seja realizada de forma eletrônica, utilizando técnicas e ferramentas específicas para garantir maior eficiência e celeridade nos processos judiciais que envolvem questões tecnológicas.

3 TRABALHOS RELACIONADOS

Abaixo, são apresentados uma série de estudos dedicados à análise de recursos forenses digitais. Cada artigo selecionado apresenta análises sobre a eficácia de programas computacionais em investigações. Muitas dessas ferramentas são softwares comerciais, ou seja, programas de empresas privadas com manipulação restrita de terceiros, impossibilitando a realização de pesquisas mais aprofundadas e padronizadas, especialmente sobre o código-fonte.

3.1 Can computer forensic tools be trusted in digital investigations?

O estudo de Bhat *et al.* (2021a) avaliou a confiabilidade das ferramentas de computação na extração de evidências digitais, com ênfase em como esses mecanismos lidam com ataques anti-forenses. O artigo também destacou a necessidade de mais pesquisas na área de computação forense para lidar com possíveis problemas que possam afetar a confiabilidade das provas judiciais. Para avaliar as ferramentas de forma padronizada, o estudo utilizou o projeto *Computer Forensics Tool Testing* do *Institute of Standards and Technology (NIST)*, cujo objetivo é estabelecer um conjunto de normas para avaliação de softwares forenses.

Neste estudo, foram avaliadas quatro ferramentas de computação forense - *The Sleuth Kit*, *EnCase*, *Forensic Toolkit* e *OSForensics* - em relação à sua capacidade de lidar com onze tipos de ataques anti-forenses comumente encontrados em sistemas de arquivos. A metodologia utilizada baseou-se nos princípios de teste de caixa preta[1].

Foram preparados casos de teste para avaliar as ferramentas de computação forense, levando em consideração os tipos de ataques anti-forenses e os equipamentos utilizados para executá-los em sistemas operacionais *Windows* e *Linux*.

O artigo buscou reforçar a necessidade de mais esforços de pesquisa na área de computação forense, a fim de lidar com possíveis armadilhas e combater ataques anti-forenses no sistema de arquivos.

3.2 Digital Forensic Tools Used in Analyzing Cybercrime

O estudo de Dweikat *et al.* (2021) enfatizou a importância dos mecanismos de extração de provas digitais em um cenário de rápida evolução da sociedade. O seu objetivo foi fornecer informações detalhadas sobre as ferramentas de computação forense, identificando seus

[1] Teste de caixa preta: teste de software para verificar a saída dos dados usando entradas de vários tipos.

pontos fortes e fracos e sugerindo soluções para os problemas encontrados. O estudo também enfocou todos os aspectos das evidências digitais para ajudar os investigadores a selecionar o melhor programa para suas necessidades.

Este estudo abrangeu um conjunto de ferramentas forenses relacionadas a computadores, redes e dispositivos portáteis, incluindo o *EnCase*, *Digital Forensics Framework*, *Bulk Extractor*, entre outras. Além disso, foram avaliadas ferramentas voltadas para a manipulação da memória volátil[2].

Foi utilizada a análise *Supervisory Control And Data Acquisition (SCADA)*. Consiste em um conjunto de ferramentas usadas para extrair evidências forenses e coletar informações sobre gabinetes e dispositivos em rede. Os dados coletados foram utilizados para determinar a penetração, a porcentagem de invasão no sistema e examinar quais processos funcionais do aparelho foram afetados. Após cada ataque, as evidências foram coletadas e a metodologia e ferramentas foram aplicadas para cada um dos métodos de invasão.

Constatou-se que muitas ferramentas forenses eletrônicas apresentam lacunas que precisam ser preenchidas. É necessário que essas ferramentas sejam atualizadas com mais frequência, a fim de resolver essas lacunas e permitir um trabalho mais eficiente para os investigadores.

3.3 Digital forensic tool verification: An evaluation of options forestablishing trustworthiness

No artigo de Marshall (2021), foram apresentados modelos de análise de ferramentas que levam em consideração os riscos e custos tanto para os usuários quanto para os fornecedores dessas soluções. Além disso, o artigo destacou as dificuldades enfrentadas na avaliação da confiabilidade desses equipamentos devido às suas restrições de direitos autorais. Essas restrições acabam gerando um aumento do trabalho necessário para a validação de métodos que visam atender aos requisitos das normas regulatórias internacionais.

Com o objetivo abordar a necessidade de mecanismos que possibilitem a verificação de ferramentas forenses e a divulgação de evidências, sem expor as partes envolvidas a riscos indevidos de responsabilidade ou de propagação de informações sensíveis.

Além disso, é essencial que haja incentivos para que os desenvolvedores dessas

[2] Memória volátil: que requer corrente elétrica para reter dados. Quando a energia é desligada, todos os dados são apagados.

ferramentas possam adotar atualizações e novos produtos de forma mais ágil, bem como fornecer evidências da confiabilidade de suas funcionalidades e, consequentemente, da credibilidade de suas ferramentas. Dessa forma, é possível garantir que as ferramentas forenses estejam atualizadas e preparadas para lidar com as mais diversas situações, além de aumentar a confiança dos usuários em relação a esses produtos.

3.4 Similaridades e diferenças do estudo

O estudo está relacionado aos artigos de Bhat *et al.* (2021a) e Dweikat *et al.* (2021) no que diz respeito à análise das características de ferramentas estabelecidas no campo da perícia forense digital. O objetivo é abordar suas funções e características.

A relação com o artigo de (MARSHALL, 2021) é que foram abordados a existência de diversos métodos de avaliação de ferramentas devido aos diferentes cenários de cada investigação e às restrições impostas por cada ferramenta. Um exemplo disso são os direitos autorais que muitas ferramentas possuem, o que dificulta a criação de um padrão de análise internacional. O objetivo é examinar essas questões e explorar alternativas para lidar com os desafios associados à uma perícia forense digital.

O principal diferencial do estudo em relação aos artigos citados é o contexto voltado para as funcionalidades de ferramentas forenses que são utilizadas no Brasil. Citando ferramentas consideradas seguras pela lei e por análises especializadas para realização das atividades em que são destinadas.

Ainda são utilizadas as diretrizes da norma ISO/IEC 27037 (2013) responsável por reger todo o processo de uma investigação criminal. Estabelecendo a identificação, coleta, aquisição e preservação como etapas do método de captura de uma evidência digital durante uma investigação no Brasil.

Na Tabela 1 estão listadas todas as similaridades e diferenciais do presente trabalho em relação aos trabalhos relacionados.

Tabela 1 – Comparativo sobre o trabalho proposto

Assunto tratado	Bhat *et al.*	Dweikat *et al.*	Marshall	Presente trabalho
Análise de ferramentas forenses	Sim	Sim	Não	Sim
Dificuldades de avaliação das ferramentas	Não	Não	Sim	Sim
Cenário Brasileiro	Não	Não	Não	Sim
Estudo sobre termos forenses	Não	Não	Sim	Sim
Organização por etapas da investigação	Não	Não	Não	Sim

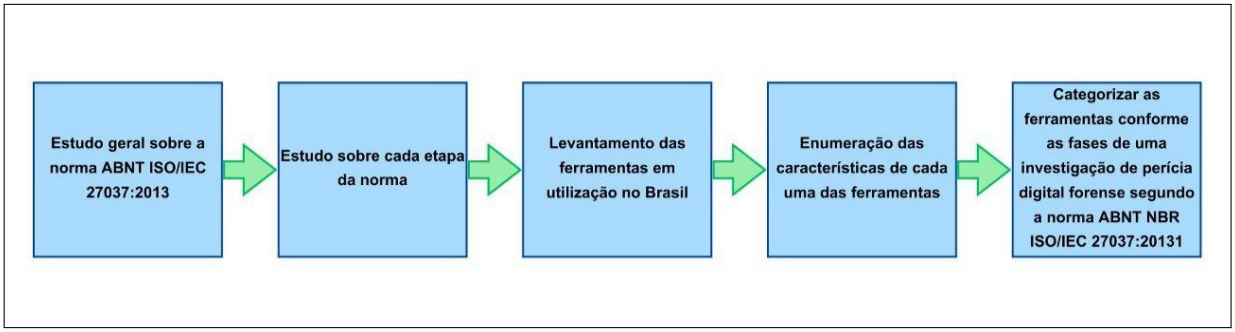
Fonte: elaborado pelo autor (2023).

Dessa maneira, o projeto atual tem o propósito de indicar ferramentas úteis em cada etapa do processo de inquisição que o conjunto de orientações que a norma destacada propõe. Buscando ainda elaborar explicações claras sobre os termos empregados no ramo da perícia digital e da ciência forense.

4 METODOLOGIA

O propósito deste estudo é aprofundar o conhecimento sobre as ferramentas e o campo da computação forense, com ênfase no contexto brasileiro, normas e diretrizes relacionadas à perícia criminal, análise forense digital e manipulação de dados dos usuários. A Figura 1 ilustra a estrutura do processo do projeto estabelecido.

Figura 1 – Etapas do trabalho



Fonte: elaborada pelo autor (2023).

4.1 Estudo sobre a norma ABNT ISO/IEC 27037:2013

Foi realizado um estudo geral sobre a norma ABNT ISO/IEC 27037:2013, que estabelece diretrizes para a aplicação da computação forense e a manipulação de evidências digitais. O objetivo principal desse estudo foi compreender os objetivos e garantias que essa norma busca assegurar, bem como os dispositivos analisados durante uma investigação computacional forense.

4.2 Estudo sobre cada etapa da norma

Ocorreu um estudo detalhado de cada etapa presente na norma: identificação, coleta, aquisição e preservação. Durante esse estudo, foram exploradas as características específicas de cada etapa, bem como os processos envolvidos em cada uma delas.

4.3 Levantamento das ferramentas em utilização no Brasil

Aconteceu uma pesquisa sobre as ferramentas de computação forense que estão em utilização atualmente no Brasil, tanto pelo setor criminal brasileiro como por profissionais autodidatas da área. Para isso foi feita uma pesquisa em catálogos *online*, artigos e *sites* voltados ao assunto da perícia digital. Com base nessa pesquisa, foi possível compreender as tendências

atuais e as opções disponíveis no mercado nacional.

4.4 Categorizar as ferramentas conforme as fases de uma investigação de perícia digital forense segundo a norma ABNT NBR ISO/IEC 27037:20131

Após a categorização de cada uma das etapas da diretriz, ocorreu a seleção de quatro ferramentas para cada etapa da norma. É importante ressaltar que o cumprimento da norma envolve a aplicação de um conjunto abrangente de processos e procedimentos, que vão além do uso de ferramentas específicas. Recomenda-se sempre avaliar a conformidade de uma ferramenta com a norma e adaptar as práticas e métodos conforme necessário para atender aos requisitos estabelecidos.

As ferramentas selecionadas foram consideradas como exemplos representativos das opções disponíveis no mercado e como um guia útil para auxiliar nas investigações no contexto brasileiro. É relevante mencionar que as ferramentas podem se enquadrar em mais de uma etapa, mas para tornar o trabalho mais diverso não será utilizada uma mesma ferramenta em mais de uma etapa. Essa abordagem visa fornecer um panorama mais abrangente das ferramentas efetivas em cada um dos processos de investigação no Brasil.

4.5 Enumeração das características de cada uma das ferramentas

Para levantar as funcionalidades e características das ferramentas selecionadas, ocorreram pesquisa abrangentes em catálogos disponíveis na internet, livros, artigos científicos, sites oficiais e consultas a especialistas no campo da computação forense. Essa pesquisa acabou sendo fundamental para definir de maneira coesa a importância dessas ferramentas em uma investigação digital e sua aplicabilidade nas respectivas etapas para as quais foram selecionadas.

5 RESULTADOS

A seção de resultados deste trabalho traz à tona os achados da pesquisa realizada sobre a identificação e análise das ferramentas de computação forense aplicadas em investigações no Brasil. Aqui são apresentadas as informações coletadas sobre a norma ISO/IEC 27037 (2013), suas etapas e sobre as ferramentas apresentadas em cada estágio.

A pesquisa buscou investigar o panorama atual das soluções tecnológicas disponíveis para apoiar investigações forenses no cenário brasileiro, analisando suas características e funcionalidades. Por meio da coleta de informações junto a artigos especializados, *sites* e instituições relevantes, foram identificadas as ferramentas mais utilizadas e reconhecidas no contexto forense brasileiro.

Os resultados apresentados aqui fornecem uma visão sobre as principais ferramentas de computação forense adotadas no país, destacando seus pontos fortes, possíveis limitações e aplicabilidade.

5.1 ABNT NBR ISO/IEC 27037:2013

A norma ISO/IEC 27037 (2013) foi desenvolvida pelo Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00). O projeto passou por uma Consulta Nacional conforme o Edital nº 08, entre 30/08/2013 e 30/09/2013. Sendo uma implementação completa, em termos técnicos, de estrutura e redação, da ISO/IEC 27037:2012, elaborada pelo *Subcommittee IT Security Techniques (SC 27)* do *Joint Technical Committee Information Technology (ISO/IEC JTC)*[1], seguindo o *ISO/IEC Guide 21-1:2005*[2].

O seu principal propósito é fornecer orientações precisas e abrangentes sobre as atividades específicas relacionadas ao tratamento de evidências digitais, abrangendo assim a identificação, coleta, aquisição e preservação dessas evidências. Adicionalmente, essas diretrizes contribuem para assegurar a admissibilidade das evidências em processos judiciais, disciplinares e outras instâncias relevantes (ISO/IEC 27037, 2013). Esses passos desempenham um papel

[1] ISO/IEC JTC: é um órgão cooperativo da *International Organization for Standardization (ISO)* e da *International Electrotechnical Commission (IEC)*. Seu objetivo é desenvolver, manter e disseminar padrões na área de tecnologia da informação e comunicação.

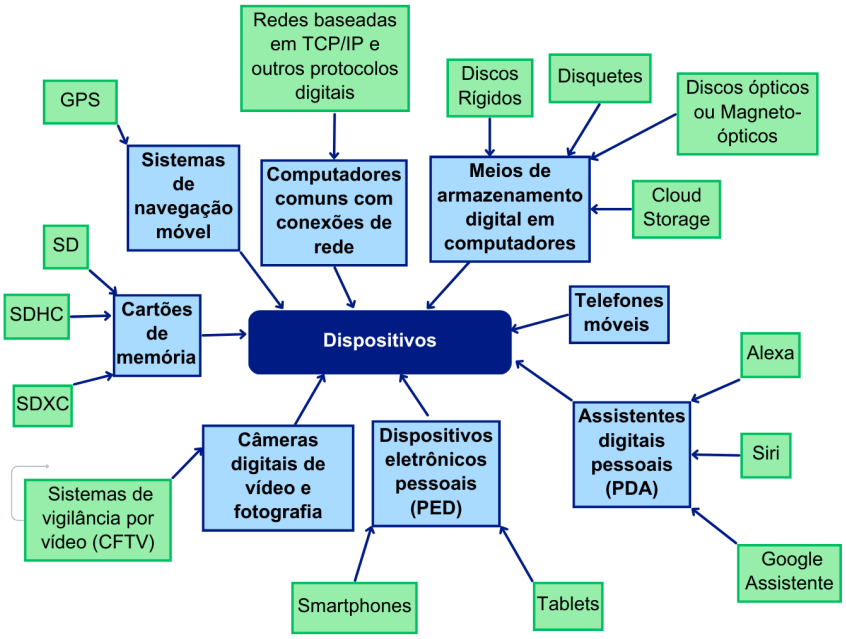
[2] ISO/IEC Guide 21-1:2005: fornece métodos para comparar e adotar normas regionais ou nacionais com as Normas Internacionais relevantes. Ela também ajuda a identificar desvios técnicos e indica o grau de correspondência entre a norma regional ou nacional e a Norma Internacional correspondente. Em resumo, a norma auxilia na harmonização e na utilização consistente de padrões em nível global (ISO, 2005).

fundamental em investigações, pois visam garantir a integridade das evidências digitais, seguindo uma metodologia apropriada para sua obtenção.

De acordo com a afirmação feita por Oliveira (2019), essa diretriz busca assegurar que os indivíduos possam realizar a gestão de evidências digitais de maneira eficiente e universalmente reconhecida. Estabelecendo uma padronização na investigação de dispositivos e/ou provas digitais, de modo imparcial e sistemático, com a finalidade de preservar a integridade e autenticidade dessas provas.

A Figura 2 ilustra uma ampla variedade de dispositivos digitais, para as quais esta norma oferece diretrizes. É importante ressaltar que essa lista de dispositivos é apenas indicativa, ou seja, não abrange todos os dispositivos e funções que podem ser contemplados pela norma.

Figura 2 – Alguns dispositivos comtemplados pela ISO/IEC 27037 (2013)



Fonte: adaptado da norma ISO/IEC 27037 (2013).

Segundo Neto e Santos (2020), apesar da ausência de um reconhecimento legal explícito, a norma em questão foi elaborada por entidades competentes com a finalidade de estabelecer diretrizes padronizadas para o tratamento de evidências digitais. Além disso, sua versão internacional descreve procedimentos adotados em vários países, estabelecendo-se como uma referência global na área de investigação forense digital. Sendo assim, embora não seja obrigatória, ela desempenha um papel significativo na padronização e aprimoramento da qualidade das práticas relacionadas à aquisição de evidências digitais.

É válido lembrar que as circunstâncias envolvendo evidências digitais abrangem

uma ampla variedade de dispositivos e contextos específicos, como sistemas automotivos. Nesse cenário, os veículos podem apresentar componentes como sistemas de navegação móvel, armazenamento de dados e sistemas sensoriais (ISO/IEC 27037, 2013). Essa diversidade de dispositivos requer abordagens especializadas para a aquisição e análise das evidências digitais relevantes.

A seguir serão abordadas as etapas estabelecidas pela norma, juntamente com as ferramentas que podem ser relevantes em cada uma dessas etapas. Serão examinadas as particularidades das distintas fases que compõem o processo de aquisição de evidências digitais, conforme definido por essa norma.

5.1.1 Identificação

Durante a fase de identificação, muitas atividades são realizadas para pesquisar, detectar e documentar possíveis evidências digitais. Uma parte importante desse processo é a identificação de equipamentos de armazenamento e processamento de mídia digital que possam conter evidências relevantes para o incidente em questão. Além disso, priorizar a coleta de provas é fundamental, dada a relevância e urgência da investigação (ISO/IEC 27037, 2013).

Para Neto e Santos (2020), esta etapa desempenha um papel importante na investigação de um incidente. Nesta fase, é importante conduzir uma investigação completa e abrangente para reconhecer fontes com potenciais evidências digitais. É importante considerar o caráter volátil dessas informações, que podem ser facilmente alteradas ou excluídas, exigindo agilidade e eficiência na coleta e registro das evidências.

Além disso, nesta etapa é necessário recuperar, reconhecer e documentar evidências digitais, bem como encontrar dispositivos de armazenamento e processamento que possam conter informações relevantes para uma investigação (OLIVEIRA, 2019). Dependendo das circunstâncias e objetivos da investigação, também pode ser importante considerar o histórico de navegação na internet, *logs*[3] do sistema, *logs* de chamadas e mensagens, dados em nuvem e dispositivos de armazenamento remoto. A Tabela 2 destaca os processos de que ocorrem nesta etapa, abrangendo a identificação do caso, fontes de dados relevantes e técnicas de coleta. Essa visualização auxilia na compreensão dos passos iniciais cruciais para o sucesso de uma investigação.

Outro ponto a ser considerado, é que uma evidência digital possui duas formas

[3] Log: arquivo ou registro que documenta eventos, atividades ou mensagens importantes que ocorrem em um sistema de computador, aplicativo, servidor ou rede.

Tabela 2 – Processos da etapa de identificação

Processo	Descrição
Identificação do caso	Identificação do caso específico e a determinação do objetivo da investigação, escopo do trabalho e tipo de incidente ocorrido.
Identificação das fontes de dados	Identificar as fontes de dados relevantes para sua investigação. Isso pode incluir discos rígidos, servidores, dispositivos móveis, mídia removível e outros dispositivos que possam conter informações relevantes.
Identificação das evidências potenciais	É crucial identificar qualquer possível evidência que possa estar presente no dispositivo. Isso pode incluir arquivos, mensagens de e-mail, logs de acesso, logs do sistema e outros tipos de informações que podem ser relevantes para uma investigação.
Identificação dos riscos à integridade das evidências	Identificar riscos à integridade das evidências digitais. Incluindo a possibilidade de perda de dados, modificação não autorizada ou outros tipos de danos às evidências. Assim, medidas de segurança serão implementadas para proteger as evidências.
Identificação das técnicas de coleta de dados	Nesta fase, é importante identificar as técnicas de coleta de dados usadas para proteger as evidências digitais. Isso pode incluir imagens forenses, coleta de dados ao vivo e outras técnicas que podem ser relevantes para sua investigação.

Fonte: adaptado da ISO/IEC 27037 (2013).

de representação: física e lógica. A forma física refere-se à representação de dados em um dispositivo tangível, enquanto a forma lógica refere-se à representação virtual de dados no dispositivo (NETO; SANTOS, 2020). Compreender esses dois métodos de apresentação de evidências digitais é fundamental para poder coletar, analisar e interpretar corretamente as evidências durante as investigações forenses digitais.

É importante ainda garantir que o estado do computador e dos periféricos não tenha mudado. Isso significa que, quando o dispositivo estiver desligado, deve-se tomar cuidado para não ligar o dispositivo para preservar as informações existentes e garantir a integridade das evidências (ISO/IEC 27037, 2013). Os cientistas forenses devem estar cientes dos tipos de dispositivos de armazenamento e processamento que as evidências digitais podem conter, incluindo discos rígidos, unidades removíveis, *smartphones* e *tablets*.

5.1.2 Utilidade de um software na etapa de identificação

As ferramentas forenses permitem a busca, detecção e recuperação de possíveis evidências digitais em dispositivos de armazenamento e processamento. Analise logs do sistema, logs de chamadas e atividade de rede para identificar eventos relevantes e padrões suspeitos.

Além disso, um *software* pode facilitar a identificação de dispositivos de armazenamento físicos e virtuais, como discos rígidos, dispositivos móveis e computação em nuvem. Os recursos de análise de metadados extraem informações sobre seus dados, como data, hora e autor, para fornecer informações adicionais.

As ferramentas forenses também simplificam a classificação e priorização de evidências. Esses dispositivos ajudam a selecionar as evidências mais relevantes e importantes, considerando critérios como variabilidade e peso probatório.

Por fim, a visualização e os relatórios são os principais recursos das ferramentas forenses, fornecendo uma exibição clara e compreensível das evidências identificadas. Gráficos, tabelas e linhas do tempo são utilizados para melhor compreensão dos resultados.

As próximas subseções deste trabalho descrevem ferramentas que podem ser utilizadas na aplicação da etapa de identificação. Essas ferramentas efetivamente implementam procedimentos padrão recomendados e desempenham um papel fundamental na identificação adequada de evidências digitais em investigações forenses.

5.1.2.1 The Sleuth Kit

O *The Sleuth Kit (TSK)* é uma ferramenta de análise forense digital de código aberto. Desenvolvida por Brian Carrier, um renomado pesquisador e autor na área de perícia digital, esta ferramenta oferece uma variedade de recursos que facilitam a análise forense. Além disso, esse *software* é regularmente atualizado para melhorar o suporte a novos sistemas de arquivos e melhorar a usabilidade e a funcionalidade geral da ferramenta (CARRIER, 2023b).

Com essa ferramenta é possível que investigadores realizem análises forenses em sistemas de arquivos sem exigir conhecimento extensivo dos sistemas subjacentes e sua complexidade. Adicionalmente, esta ferramenta é frequentemente utilizada como base para o desenvolvimento de outras técnicas e ferramentas de análise forense, permitindo uma abordagem investigativa mais abrangente e precisa (HILGERT *et al.*, 2017).

No entanto, é importante observar que o TSK é composto por um conjunto de

ferramentas de linha de comando, o que pode tornar sua utilização menos intuitiva para usuários menos familiarizados com esse tipo de ambiente (DATA, 2023).

A Tabela 3 ilustra as diferentes funcionalidades fornecidas pelo *Sleuth Kit* para análise forense de sistemas de arquivos. Cada funcionalidade opera em uma categoria específica do modelo, permitindo uma abordagem abrangente e precisa durante a investigação. Essas funcionalidades combinadas possibilitam uma análise completa do sistema de arquivos em questão.

Tabela 3 – Funcionalidades disponíveis no Sleuth Kit para análise forense do sistema de arquivos

Funcionalidade	Descrição
mmls	Analisa um único volume e fornece informações sobre a sua organização.
fsstat	Detecta o tipo de sistema de arquivos armazenado em um único volume e apresenta estatísticas e metadados sobre ele.
fls	Lista todos os arquivos e diretórios de um sistema de arquivos armazenado em um único volume.
istat	Apresenta informações de uma determinada estrutura de metadados.
icat	Extrai dados pertencentes a uma estrutura de metadados.

Fonte: adaptado de Hilgert *et al.* (2017).

Essa ferramenta oferece ao usuário a capacidade de realizar uma análise abrangente dos sistemas de arquivos presentes em um computador. Permitindo ainda examinar de forma não intrusiva independente do sistema operacional da máquina investigada, possibilitando o processamento de sistemas de arquivos, bem como a recuperação de arquivos deletados e ocultos de várias partições, como *Disk Operating System (DOS)*, *Berkeley Software Distribution (BSD)*, *Macintosh (MAC)*, *Sun* e *Linux* (GALVãO, 2016). Com essa funcionalidade, é possível obter informações valiosas para investigações forenses e explorar os dados armazenados nos sistemas de arquivos de maneira eficiente e precisa.

Por outro lado, sua poderosa capacidade de varredura de discos rígidos e outros dispositivos permite uma rápida identificação das fontes de dados relevantes, que podem conter informações cruciais para a investigação em questão (CARRIER, 2023b). Com sua abordagem avançada, o *Sleuth Kit* se destaca como uma ferramenta essencial para profissionais de investigação forense, facilitando a identificação e a análise de evidências de maneira eficiente e precisa.

Combinando a funcionalidade do TSK com a etapa de identificação, os investigadores podem agilizar o processo de identificação de evidências digitais. A ferramenta facilita a busca,

detecção, recuperação e análise de possíveis evidências, contribuindo para investigações forenses mais eficientes e precisas.

Em resumo, trata-se de uma ferramenta valiosa que desempenha um papel fundamental na descoberta de evidências digitais. A análise do sistema de arquivos, a recuperação de arquivos excluídos, sua capacidade de explorar vários dispositivos de armazenamento e processamento e a natureza de código aberto atualizável o tornam uma escolha poderosa para investigadores que desejam identificar e documentar evidências digitais com eficácia.

5.1.2.2 Volatility

O *Volatility* possibilita a análise de despejos de memória de uma ampla variedade de sistemas operacionais. Sua estrutura modular permite a inclusão de novos sistemas operacionais e arquiteturas conforme necessário. Os investigadores têm a flexibilidade de ampliar suas análises forenses para além dos computadores *Windows*, permitindo explorar evidências digitais em outros dispositivos (CASE, 2020).

Segundo Fernando e Rupasinghe (2022), trata-se de uma plataforma especializada em análise de memória que se concentra na recuperação de artefatos digitais a partir de despejos de memória Random Access Memory (RAM) para fins de resposta a incidentes e análise de *malwares*. Com essa ferramenta, os investigadores podem obter informações detalhadas sobre os processos em execução, *sockets* de rede abertos, conexões de rede, bibliotecas de vínculo dinâmico as Dynamic-link Library (DLL) carregadas em cada processo, registros de registro em cache etc. Esses procedimentos de extração são executados independentemente do sistema em investigação, oferecendo uma visão clara do estado de execução do sistema.

Além disso, é oferecida uma variedade de plugins desenvolvidos tanto pela *Volatility Foundation* quanto pela comunidade. Esses plugins, como *malfind*, *cmdscan*, *apihooks* e *impscan*, são úteis para facilitar a análise forense e o desenvolvimento de técnicas nessa área. Eles são capazes de detectar *malwares*, inclusive aqueles com camadas de ofuscação, como o ZEUS[4]. Além disso, a sua *Application Programming Interface (API) scriptável* permite aos desenvolvedores explorar a memória do kernel, adicionar novos *plugins*, executar máquinas virtuais e criar um ambiente de *sandbox*[5] para malwares. Essa funcionalidade amplia as possibilidades de análise e desenvolvimento, contribuindo para o aprimoramento das técnicas forenses (ALMUTAIRI *et al.*,

[4] ZEUS: pacote de malware de cavalo de Tróia executado em versões do *Microsoft Windows*.
[5] *Sandbox*: ambiente de teste isolado.

2020).

A sua ferramenta de análise é amplamente utilizada para investigar despejos de memória de computadores comprometidos. Diferente da versão de linha de comando, possuindo uma interface gráfica intuitiva que simplifica o processo de investigação na memória volátil. Com essa interface amigável, os usuários podem fornecer as informações necessárias de forma simples e eficiente. Além disso, permite a geração de relatórios claros e compreensíveis para os analistas. Outro recurso valioso é a capacidade de detectar e listar informações relacionadas a vírus presentes no despejo de memória, oferecendo uma visão abrangente das ameaças identificadas (FERNANDO; RUPASINGHE, 2022).

É importante destacar algumas de suas desvantagens. A primeira delas é a ausência de uma interface gráfica, o que pode tornar sua utilização mais desafiadora para usuários menos familiarizados com a linha de comando. Dessa forma, pode acabar dificultando a visualização e a compreensão dos resultados, exigindo um maior conhecimento técnico para interpretar as informações extraídas. Além disso, a dependência exclusiva da linha de comando pode ser considerada inconveniente para alguns usuários (GOGAN, 2020).

Esse *software* se destaca ao oferecer análises rápidas e eficientes em despejos de memória de sistemas de grande porte, sem impactar negativamente os recursos de memória. Enquanto outras soluções de análise de memória levariam horas para listar os módulos do kernel em sistemas menores, aqui é possível concluir essa tarefa rapidamente, permitindo que os investigadores identifiquem prontamente os componentes cruciais do sistema comprometido. Além disso, o respaldo do *SANS Institute*, uma renomada instituição de segurança da informação demonstram a confiança e a reputação da ferramenta no campo forense (ALMUTAIRI *et al.*, 2020).

Em suma, o *Volatility* é uma ferramenta valiosa para a etapa de identificação de evidências digitais. Sua capacidade de analisar despejos de memória, a ampla variedade de *plugins* disponíveis, a interface gráfica intuitiva e sua flexibilidade para explorar diferentes sistemas operacionais contribuem para uma análise forense eficiente e precisa. O seu uso permite aos investigadores identificarem e analisarem evidências digitais relevantes presentes na memória volátil, fornecendo *insights*[6] valiosos para a investigação.

[6] Insights: percepções, entendimentos ou conclusões obtidas a partir de informações, dados ou experiências.

5.1.2.3 WinHex

WinHex é um *software* amplamente reconhecido para análise e edição de arquivos binários. Desenvolvido pela *X-Ways Software Technology AG*, uma empresa alemã, foi criado em 1995 por Stefan Fleischmann, fundador e CEO da empresa (FLEISCHMANN, 2023). No Brasil, é utilizado por profissionais que atuam na área de perícia forense e análise de dados. Além disso, o software desfruta de uma reputação internacional sólida e é amplamente utilizado em diversos países.

Trata-se de uma ferramenta versátil que oferece suporte a uma ampla variedade de sistemas de arquivos, além de arquivos de imagem. Sendo possível realizar recuperações seguras em vários tipos de dispositivos, como discos rígidos, cartões de memória, discos *flash*, disquetes, entre outros. Além disso, existem recursos automatizados de recuperação de arquivos, facilitando a recuperação de dados de maneira conveniente e rápida. No entanto, também oferece opções manuais para situações mais específicas, caso necessário (X-WAYS SOFTWARE TECHNOLOGY AG., 2023a).

Para Hermon *et al.* (2023), essa ferramenta de análise forense oferece recursos abrangentes para a análise detalhada do sistema. Algumas de suas funcionalidades incluem:

- Navegador de diretórios para facilitar a visualização e navegação nos sistemas de arquivos suportados.
- Interpretador de dados que permite a compreensão dos dados em diferentes formatos e estruturas.
- Edição da tabela de partição, setores de boot e outros elementos-chave do sistema.
- Capacidade de analisar e comparar arquivos para identificar diferenças e padrões.
- Clonagem e criação de imagens de disco para preservação e investigação forense.
- Múltiplos mecanismos de backup para proteção dos dados durante o processo de análise.
- Recursos avançados de recuperação de dados para recuperar informações perdidas ou corrompidas.
- Limpeza de espaços não utilizados, espaço ocioso e discos ou imagens contendo dados confidenciais, garantindo a segurança da informação.

Esses recursos do WinHex auxiliam os profissionais na análise forense de sistemas, permitindo uma investigação minuciosa e a obtenção de evidências confiáveis.

Em contraponto, essa ferramenta não suporta as funcionalidades do console do

sistema, o que pode limitar sua capacidade de análise e investigação em determinados casos. Outro ponto a ser considerado é que ela não é executável em sistemas *MAC* e *Linux*, o que restringe seu uso a plataformas específicas. Essas limitações podem afetar a usabilidade e a sua abrangência como ferramenta forense digital (KAMBLE *et al.*, 2015).

Além disso, oferece recursos de recuperação de dados, o que pode ser útil na etapa de identificação. Se houverem dados excluídos que possam ser relevantes para a investigação, ela auxilia na sua recuperação, permitindo a análise posterior (X-WAYS SOFTWARE TECHNOLOGY AG., 2023a).

Em termos gerais, WinHex é uma ferramenta útil na etapa de identificação de evidências digitais, pois possui recursos de análise e edição de arquivos binários, suporte para vários sistemas e dispositivos de arquivos, recursos de recuperação automática de dados e recursos avançados que acabam contribuindo para um reconhecimento eficiente e preciso de evidências digitais relevantes para as investigações.

Também, devido à sua versatilidade e riqueza de recursos, desempenha um papel ainda mais importante nesta etapa. Com uma capacidade de analisar e manipular arquivos binários permitindo que profissionais forenses e de análise de dados inspecionem sistemas de arquivos e dispositivos de armazenamento com eficiência.

5.1.2.4 Xplico

Xplico é uma ferramenta de código aberto continuamente aprimorada por uma equipe de desenvolvedores e colaboradores. Essa comunidade trabalha para melhorar a funcionalidade e a usabilidade da ferramenta, garantindo que ela atenda às necessidades dos usuários de forma eficiente.

O seu objetivo é extrair informações relevantes das aplicações presentes nos dados capturados do tráfego da internet. Utilizando um arquivo pcap, o Xplico é capaz de coletar diversos tipos de dados, como *e-mails*, conteúdo *Hypertext Transfer Protocol (HTTP)*, chamadas *Voice Over Internet Protocol (VoIP)*, *File Transfer Protocol (FTP)*, *Trivial File Transfer Protocol (TFTP)* etc. É importante ressaltar que o *Xplico* é uma ferramenta específica para análise forense de rede, oferecendo recursos avançados nesse contexto (XPLICO, 2023).

Além do mais, essa ferramenta busca facilitar a análise dos dados obtidos. Ela permite extrair sessões de áudio de um fluxo e reconstruir dados gerados por outras ferramentas de captura. Além disso, é capaz de extrair páginas da *web* e extrair dados específicos, como

imagens e áudio, dos dados obtidos dessas páginas. É uma ferramenta comumente utilizada na distribuição *Linux Kali* para testes de penetração. Outras vantagens incluem suporte a ambientes multiusuário e a capacidade de oferecer suporte em nuvem(KAUR; MISRA, 2019).

Com suporte a uma ampla gama de protocolos, ela oferece recursos avançados, como identificação de protocolo independente de porta para cada aplicação, suporte a *multithreading* e opções flexíveis de saída de dados em bancos de dados *SQLite* ou *MySQL* e/ou arquivos. Cada dado remontado por ela é associado a um arquivo Extensible Markup Language (XML) único que identifica os fluxos e o arquivo correspondente aos dados montados. Além disso, possui recursos como elaboração em tempo real, reassemblagem *Transmission Control Protocol (TCP)*, consulta reversa de Domain Name System (DNS) a partir de pacotes. Sua modularidade permite que os usuários criem diferentes tipos de despachadores para organizar os dados extraídos de acordo com suas necessidades específicas (XPLICO, 2023).

Em resumo, o Xplico desempenha um papel fundamental nesta etapa de evidências digitais, permitindo a extração e análise de dados de tráfego de rede. A capacidade de coletar informações de vários logs e a flexibilidade da saída de dados contribuem para a identificação e coleta eficientes de evidências digitais relevantes para investigações forenses.

Além disso, capacidade de extrair informações relevantes dos dados capturados no tráfego da Internet desempenha um papel importante na descoberta de evidências digitais. Usando esta ferramenta, é possível coletar uma variedade de dados, como e-mails, conteúdo HTTP, chamadas VoIP e outros protocolos.

5.1.2.5 Conclusões sobre as ferramentas levantadas na etapa de identificação

As ferramentas mencionadas - The Sleuth Kit, Volatility, WinHex e Xplico - apresentam características distintas que as tornam relevantes para a etapa de identificação de investigação forense de evidências digitais. Na Tabela 4 são mostrados alguns do atributos dessas ferramentas.

No contexto da identificação, essas ferramentas permitem uma análise detalhada de sistemas de arquivos, memória volátil e tráfego de rede. Possuindo versatilidade, recursos avançados e suporte a diferentes aspectos da investigação forense digital, elas auxiliam os investigadores na identificação evidências digitais relevantes com eficiência e precisão.

Tabela 4 – Ferramentas da etapa de identificação e suas características

Ferramenta	Características
The Sleuth Kit	• Código aberto e personalizável. • Suporte a uma ampla variedade de sistemas de arquivos. • Atualizações regulares para melhorias e suporte a novos sistemas.
Volatility	• Capacidade de análise de despejos de memória. • Comunidade ativa de desenvolvedores e disponibilidade de plugins. • Permite análise detalhada de processos, conexões de rede e outros dados na memória volátil.
WinHex	• Versatilidade na análise e edição de arquivos binários. • Suporte a vários sistemas de arquivos e dispositivos. • Recursos avançados de análise, navegação e recuperação de dados.
Xplico	• Especializada na análise forense de tráfego de rede. • Coleta de informações relevantes de várias aplicações no tráfego capturado. • Recursos avançados de extração e reconstrução de dados do tráfego de rede.

Fonte: elaborado pelo autor (2023).

5.1.3 Coleta

O processo de coleta é parte fundamental do manuseio de evidências digitais. Isso envolve a remoção de dispositivos que podem conter evidências relevantes de seu local original e sua movimentação para um ambiente controlado, como um laboratório, para posterior aquisição e análise. Um dispositivo pode estar em dois estados: Ligado se o sistema ainda estiver em execução, desligado se o sistema estiver desligado (ISO/IEC 27037, 2013).

Dependendo do estado do dispositivo, diferentes abordagens e ferramentas são necessárias para realizar a coleta de evidências digitais (ISO/IEC 27037, 2013). Em outras palavras, a abordagem para coletar dados de dispositivos ligados é diferente da abordagem adotada quando os dispositivos estão desligados. Além disso, é importante considerar os procedimentos locais que podem influenciar as abordagens e ferramentas utilizadas no processo. Os métodos devem ser adaptados aos padrões e regulamentos locais para garantir uma conformidade adequada.

Para Verber e Smutny (2015), após a identificação dos dispositivos que podem conter evidências digitais, eles são cuidadosamente retirados de seu local de origem e levados a um laboratório para posterior análise e processamento. É importante ressaltar que todo o processo desde a coleta do dispositivo e embalagem para transporte até a chegada ao laboratório foi cuidadosamente documentado.

Além disso, ao coletar dados de um dispositivo digital, é fundamental levar em consideração sua volatilidade e o estado atual do sistema antes de desligá-lo. Isso ocorre porque informações importantes, como chaves de criptografia, podem estar armazenadas na memória ativa ou inativa, que ainda não foi limpa. Caso haja suspeita de criptografia, é recomendável realizar uma coleta lógica dos dados. Além disso, é crucial ter em mente que o sistema operacional local pode não ser confiável, portanto, é necessário utilizar ferramentas apropriadas e confiáveis, que tenham sido validadas (ISO/IEC 27037, 2013). A Tabela 5 mostra os processos que ocorrem durante essa etapa.

Tabela 5 – Processos da etapa de coleta

Processo	Descrição
Planejamento da coleta de evidências	Onde métodos de coleta apropriados são selecionados e o processo de coleta é documentado.
Coleta das evidências	Deve incluir manter a integridade das evidências e documentar informações relevantes, como data e hora da coleta, localização das evidências e método de coleta.
Análise preliminar das evidências coletadas	Buscando determinar a relevância e a utilidade para a investigação.
Registro e documentação das informações coletadas	Visando garantir a sua integridade e precisão.
Armazenamento das evidências coletadas	Sempre buscando as manter em condições adequadas, garantindo a sua segurança e integridade.

Fonte: adaptado da ISO/IEC 27037 (2013).

É importante coletar evidências adequadamente, manter sua integridade e registrar com precisão todas as informações relevantes, como data, hora, local e métodos utilizados. A realização de uma coleta completa e bem documentada é essencial para garantir a eficácia da fase investigativa subsequente.

Durante uma investigação, sempre deve-se coletar corretamente dados ativos, como informações da empresa e dispositivos digitais que controlam equipamentos médicos. Para evitar a perda de informações relevantes, recomenda-se que sejam tomadas medidas para capturar adequadamente os dados voláteis antes de desligar a energia (ISO/IEC 27037, 2013).

5.1.4 Utilidade de um software na etapa de coleta

Um *software* forense pode facilitar a catalogação e a documentação detalhada de todos os dispositivos identificados, capturando informações importantes como data, hora e local da coleta. Desta forma, pode contribuir para a documentação adequada e precisa do processo de coleta e fornece uma base sólida para a fase investigativa subsequente.

Considerando o estado do dispositivo (ligado ou desligado) e usando a abordagem apropriada em cada caso, a detecção pode ser realizada de forma eficiente e confiável. Também garantido que a integridade dos dados coletados seja mantida, verificando a integridade dos dados por meio de técnicas de criptografia e evitando alterações indesejadas.

A extração de metadados é outro aspecto fundamental em uma ferramenta forense. Permitindo a obtenção de informações adicionais sobre as evidências digitais coletadas, como data de criação, data de modificação, informações de localização geográfica e informações do sistema operacional. Esses metadados podem desempenhar um papel crucial na análise e interpretação das evidências, fornecendo contextos importantes para os investigadores.

No geral, o uso de ferramentas forenses durante a fase de coleta melhora muito a eficácia, precisão e conformidade do processo. Com recursos avançados de identificação, documentação, coleta forense e extração de metadados, a ferramenta ajuda os investigadores a recuperar evidências digitais relevantes de maneira confiável e eficiente. O resultado é uma coleção completa, documentada e preservada que fornece uma base sólida para análises e investigações posteriores.

As próximas subseções deste trabalho apresentam algumas ferramentas úteis que podem ser utilizadas durante a fase de coleta seguindo as orientações da norma. Essas ferramentas podem ter um papel fundamental nesse processo.

5.1.4.1 Autopsy

É uma ferramenta de código aberto amplamente utilizada por várias organizações, como policiais, auditores corporativos e militares. Ele utiliza o *Sleuth Kit* para análise de imagem, possibilitando análise de mídia digital e recuperação de dados excluídos. O *Autopsy* possui recursos robustos e pode extrair informações relevantes, como histórico de navegação e cookies de vários navegadores, como *Google Chrome*, *Mozilla Firefox* e *Internet Explorer*. É uma solução eficiente, fácil de usar e econômica com recursos adicionais, como análise temporal,

filtragem de *hash*, artefatos da web, pesquisa de palavras-chave e fornece suporte abrangente para investigações forenses digitais (ADAMU *et al.*, 2021).

Trata-se de uma plataforma abrangente de investigação forense digital que integra vários módulos e que também permite a incorporação de módulos de terceiros. A Tabela 6 destaca os módulos disponíveis, suas funções e descrições, dando uma visão geral dos recursos disponibilizados pela ferramenta.

Tabela 6 – Módulos disponíveis

Funcionalidade	Descrição
Interface gráfica avançada	Facilita a visualização dos eventos em ordem cronológica através de uma interface gráfica intuitiva.
Filtragem de Hash	Possibilita a identificação de arquivos maliciosos conhecidos por meio de comparação com uma lista de hashes.
Pesquisa por palavra-chave	Indexa termos específicos para facilitar a localização de arquivos relevantes durante a investigação, proporcionando agilidade na análise.
Artefatos da Web	Extrai informações relevantes de navegadores populares, como histórico de navegação, favoritos e cookies do Firefox, Chrome e Internet Explorer.
Data Carving	Possibilita a recuperação de arquivos excluídos do espaço não alocado, utilizando a ferramenta PhotoRec.
Multimídia	Extrai metadados de fotos e permite a visualização de vídeos, auxiliando na análise de conteúdo multimídia relevante para a investigação.
Indicadores de Comprometimento	Verifica um computador em busca de indicadores de atividades suspeitas usando a linguagem de marcação STIX.

Fonte: adaptado de (CARRIER, 2023a).

Sua interface do usuário pode apresentar lentidão em máquinas mais antigas. É importante destacar que o software não possui suporte nativo para mensagens de e-mail no formato do Outlook, que é um formato ainda comum. Além disso, sua versão mais recente está disponível apenas para usuários do *Windows*, enquanto os usuários do *Linux* precisam recorrer ao uso da linha de comando do TSK, utilizar versões mais antigas ou compila-lo por conta própria (FZE, 2018).

Esse software forense oferece recursos avançados que são especialmente relevantes para a coleta de evidências digitais. Com o auxílio do *Sleuth Kit* para análise de imagem, a ferramenta possibilita a análise de mídia digital e a recuperação de dados excluídos. Isso é especialmente importante na coleta de evidências, pois permite uma abordagem abrangente e detalhada para aquisição de dados. Além disso, a ferramenta oferece recursos robustos,

como extração de informações relevantes dos navegadores mais populares, incluindo histórico de navegação e cookies. Esses recursos são cruciais para a obtenção de evidências digitais pertinentes e podem fornecer *insights* valiosos durante a investigação.

Em resumo, essa ferramenta é altamente útil nesta etapa, fornecendo recursos avançados e abrangentes para coleta de dados, permitindo a recuperação de informações excluídas e oferecendo suporte para a análise de elementos-chave, como histórico de navegação e cookies. Com sua eficiência e facilidade de uso, ela é uma escolha valiosa para investigações forenses digitais, fornecendo uma base sólida para as fases subsequentes do processo.

5.1.4.2 Forensic Toolkit

Forensic Toolkit (FTK) é desenvolvida e atualizada pela *AccessData*. Essa organização se esforça para fornecer suporte técnico contínuo e atualizações ao FTK para garantir que a ferramenta atenda às necessidades dos investigadores forenses e cumpra os padrões do setor (EXTERRO, 2023).

Essa ferramenta fornece soluções abrangentes para investigações digitais e oferece suporte a profissionais de segurança da informação, tecnologia e aplicação da lei. Recursos avançados, como filtros e um mecanismo de indexação eficiente, fornecem acesso rápido a evidências relevantes para casos sob investigação, reduzindo bastante o tempo necessário para análise (CARBONE, 2014).

Também permite a análise de forma confortável e abrangente dos arquivos de registro e as informações do sistema *Windows*. Além disso, oferece a capacidade de rotular, marcar e exportar objetos individuais agrupados por categoria (EXTERRO, 2023). Esse recurso facilita a realização de pesquisas precisas, filtra dados específicos e cria relatórios detalhados. Vale a pena notar que esta ferramenta é especialmente útil para investigações forenses.

Possui ainda uma função chamada *FTK Imager*, que é capaz de criar imagens de discos rígidos em diferentes formatos. Essas imagens podem ser armazenadas e posteriormente recriadas, garantindo a integridade dos dados através de cálculos de *hash*. O FTK também se destaca por sua interface de usuário intuitiva, recursos avançados de busca, suporte para descriptografia, criação de registros do caso e recursos de relatórios (DAS, 2019).

Embora seja uma ferramenta robusta, ela apresenta algumas limitações a serem consideradas. Por exemplo, não possui recursos de script para automação de tarefas. Além disso, não oferece suporte a multitarefa, o que significa que não é possível executar várias tarefas

simultaneamente. Outra ausência importante é a falta de uma barra de progresso para estimar o tempo restante em uma operação (DAS, 2019)

Adicionalmente, o processamento de uma variedade de tipos de dados provenientes de diversas fontes. Isso inclui dados de discos rígidos, dispositivos móveis, armazenamento em rede e na Internet. Com o FTK, os investigadores e analistas forenses têm acesso a uma plataforma única para coletar e processar todos os dados relevantes em uma investigação (EXTERRO, 2023). Essa abordagem centralizada aumenta a eficiência e a precisão do processo.

O FTK possibilita uma ampla gama de recursos e funcionalidades para a etapa de coleta, incluindo acesso rápido a evidências relevantes, análise abrangente de diferentes tipos de dados e a criação de relatórios detalhados. Embora possua algumas limitações, sua interface intuitiva e recursos poderosos o tornam uma ferramenta valiosa para investigadores forenses durante a coleta de evidências digitais.

Oferecendo ainda uma análise confortável e abrangente de arquivos de registro e informações do sistema *Windows*. Com a capacidade de rotular, marcar e exportar objetos individuais agrupados por categoria, a ferramenta facilita a realização de pesquisas precisas, a filtragem de dados específicos e a criação de relatórios detalhados. Esses recursos fornecem uma abordagem eficiente e abrangente para a coleta de evidências digitais.

5.1.4.3 Oxygen Forensic Suite

O *Oxygen Forensic Suite* é uma ferramenta que oferece uma solução completa para coletar e analisar evidências digitais de dispositivos móveis, como *smartphones*, *tablets* e *GPS*. Conhecida por sua ampla compatibilidade com vários dispositivos móveis e suporte para vários sistemas operacionais.

É uma opção atrativa, pois oferece uma interface de usuário simples e fácil de entender. Além disso, permite a extração física de dados de dispositivos Android e fornece recursos para a quebra de senhas de backups criptografados do *iTunes*, *iPhones* bloqueados ou *backups* do Android. Os relatórios finais gerados podem ser salvos em diferentes formatos (DAS, 2019).

Porém, para Das (2019), devido à sua natureza baseada em computador, é estatisticamente mais provável que vírus/malware entrem no dispositivo verificado. Outro aspecto a considerar é que a ferramenta utiliza uma abordagem de força bruta, o que torna o processo de análise muito demorado.

Para Panigrahi *et al.* (2021), devido sua capacidade de investigação forense avançada em *smartphones* ela permite aos investigadores acessar e analisar informações cruciais em um único local. Por exemplo, a ferramenta possibilita a revisão de logins e senhas armazenados de forma segura, como no banco de dados *keychain* do sistema. Além disso, arquivos de aplicativos também são examinados, pois podem conter dados importantes para a investigação.

Outro ponto a ser considerado é a possibilidade de escolha de diferentes algoritmos de *hash* para garantir a integridade dos dados coletados. Além disso, o *software* fornece informações básicas sobre o *smartphone* e a rede em que o dispositivo estava conectado durante a investigação. Uma capacidade importante dessa ferramenta é a recuperação de contatos, mensagens *Short Message Service (SMS)*, *Multimedia Message System (MMS)* e arquivos do usuário, o que permite acessar e analisar dados essenciais para investigações forenses (YULIANI; RIADI, 2019). Essa ferramenta é extremamente útil para os profissionais que trabalham na área, pois auxilia na obtenção de evidências digitais e na compreensão das atividades do usuário.

Resumindo, o *Oxygen Forensic Suite* desempenha um papel fundamental na etapa de coleta, fornecendo uma solução completa e abrangente para a aquisição de dados de dispositivos móveis. Sua interface intuitiva, recursos avançados de análise e capacidade de lidar com uma variedade de dispositivos e sistemas operacionais contribuem para uma coleta eficiente e organizada de evidências digitais.

Ainda, oferece recursos avançados de análise, como a revisão de logins, senhas e arquivos de aplicativos armazenados de forma segura, bem como a recuperação de contatos, mensagens SMS, MMS e outros dados do usuário. Essas capacidades são especialmente valiosas durante a etapa de coleta, pois permitem que os investigadores obtenham informações cruciais e realizem análises forenses detalhadas.

5.1.4.4 X-Ways Forensics

X-Ways Forensics (XWF) um recurso de trabalho avançada para inspetores forenses de computador. Compatível com uma ampla gama de sistemas operacionais *Windows*, arquiteturas de 32 e 64 *bits*, do XP às versões mais recentes. Fornece ainda recursos e ferramentas poderosas de suporte forense de computador que permitem aos investigadores conduzir investigações de forma eficiente e eficaz (X-WAYS SOFTWARE TECHNOLOGY AG., 2023b).

Os requisitos dessa ferramenta são menores em comparação com outras ferramentas forenses digitais. Você também pode executá-lo sem instalá-lo. Fornecendo recursos de análise

de arquivo de imagem mesmo em dispositivos de baixa especificação (LEE; SOH, 2020a).

Segundo Khalaf e Varol (2019), é uma ferramenta avançada para análise forense onde os arquivos de imagem e todos os diretórios podem ser verificados, fornecendo aos investigadores informações detalhadas, mesmo que o diretório não esteja em um segmento contíguo. O programa suporta vários tipos de arquivos. Além disso, possui opções avançadas de análise e investigação.

Em contrapartida, possui uma interface de usuário complexa, que pode demandar um certo tempo para familiarização. Deve-se ressaltar que esse software requer um *dongle*[7] para funcionar, sendo necessário tê-lo disponível durante o uso. É importante mencionar também que essa ferramenta não oferece suporte para o *Bitlocker*[8], o que pode ser uma limitação para investigações envolvendo esse tipo específico de criptografia (DAS, 2019).

Uma das características mais destacadas do XWF é sua capacidade de ser utilizado em modo portátil, o que confere flexibilidade aos investigadores durante suas operações. O software oferece opções personalizáveis para o processamento de evidências, permitindo adaptar as configurações de acordo com as necessidades de cada caso (DAS, 2019).

Durante a etapa de coleta, o XWF desempenha um papel importante ao oferecer recursos e ferramentas poderosas para inspetores forenses de computador. Sua compatibilidade com uma ampla gama de versões *Windows*, juntamente com a capacidade de análise de arquivos de imagem mesmo em dispositivos de baixa especificação, a tornam uma opção acessível e eficiente para coletar evidências digitais.

Possibilitando a verificação de arquivos de imagem e diretórios garante a integridade dos dados coletados. A capacidade de lidar com vários tipos de arquivos e as opções avançadas de análise e investigação são características que agregam valor à etapa de coleta de evidências digitais.

5.1.4.5 Conclusões sobre as ferramentas levantadas na etapa de coleta

Com base nas características levantadas das ferramentas Autopsy, Forensic Toolkit, Oxygen Forensic Suite e X-Ways Forensics, podemos concluir que todas elas oferecem recursos e funcionalidades relevantes para a etapa de coleta de evidências digitais. A Tabela 7 levanta algumas das características encontradas sobre cada um dos *softwares*.

Em suma, essas ferramentas fornecem uma base sólida e abrangente para a etapa de

[7] Dongle: um dispositivo pequeno, geralmente conectado a um computador ou dispositivo eletrônico, que fornece funcionalidades adicionais ou acesso a recursos específicos.

[8] Bitlocker: ferramenta de criptografia de disco integrada no sistema operacional *Windows*.

Tabela 7 – Ferramentas da etapa de coleta e suas características

Ferramenta	Características
Autopsy	• Recursos robustos para análise forense digital. • Suporte abrangente para investigações digitais. • Extração de informações de navegadores populares.
Forensic Toolkit	• Solução completa para investigações digitais. • Recursos avançados de filtragem e indexação. • Rotulagem e marcação de objetos individuais.
Oxygen Forensic Suite	• Coleta e análise de evidências digitais de dispositivos móveis. • Extração física de dados, quebra de senhas e geração de relatórios detalhados. • Recuperação de informações importantes, como contatos e mensagens.
X-Ways Forensics	• Compatibilidade com sistemas operacionais Windows e arquiteturas diversas. • Requisitos menores e opção de uso portátil. • Análise de arquivos de imagem e verificação de diretórios.

Fonte: elaborado pelo autor (2023).

coleta, permitindo que os investigadores conduzam investigações forenses de maneira eficiente, garantindo a preservação e a integridade dos dados coletados.

5.1.5 Aquisição

Durante a fase de aquisição de evidências digitais, é importante ter uma cópia forense precisa das evidências em questão. Isso inclui copiar o disco inteiro, partições específicas ou apenas arquivos relacionados específicos. É importante documentar detalhadamente todos os métodos e atividades realizadas no escolher o método de aquisição apropriado, considerando a processo de aquisição. Os profissionais de forense digital devem escolher os métodos de obtenção adequados, levando em consideração a situação específica, o custo envolvido e o tempo disponível (ISO/IEC 27037, 2013).

A documentação adequada durante esse processo é essencial na perícia digital, especialmente quando se trata da admissibilidade de evidências digitais em tribunal (ISO/IEC

27037, 2013). É importante que a equipe documente de forma clara e concisa todas as atividades realizadas durante a aquisição, incluindo métodos escolhidos, ferramentas utilizadas, verificações realizadas e outros detalhes relevantes. Essa prática garante a transparência e a confiabilidade das evidências coletadas.

Para garantir a integridade dos dados e evitar erros na coleta e armazenamento de evidências digitais, é recomendado verificar a fonte original e a cópia usando uma função de verificação, como uma função de *hash*. As verificações de hash garantem que a fonte original e cada cópia retornem exatamente os mesmos resultados, demonstrando que os dados não foram modificados no processo (OLIVEIRA, 2019). Além disso, a documentação da verificação de hash também é essencial para fins de rastreabilidade e auditoria. Isso garante a confiabilidade das evidências e facilita o rastreamento das ações tomadas.

Durante a etapa de aquisição, são realizados diversos processos importantes para garantir a integridade e autenticidade das evidências digitais. A Tabela 8 mostra alguns desses processos para assegurar a qualidade e confiabilidade das evidências digitais coletadas, seguindo as diretrizes da norma mencionada.

Tabela 8 – Processos da etapa de aquisição

Processo	Descrição
Verificação da integridade das imagens forenses	Depois de criar as imagens, é importante verificar se elas são idênticas ao dispositivo original. Isso é feito comparando a imagem original e o hash gerado pelo dispositivo.
Coleta de evidências voláteis	São coletadas as evidências que podem ser perdidas quando o dispositivo é desligado ou reiniciado.
Identificação de dados ocultos	São identificados dados que não são visíveis aos usuários comuns, mas podem ser recuperados por ferramentas forenses. Isso inclui arquivos excluídos que ainda podem ser recuperados e informações armazenadas em áreas do disco não acessíveis pelo sistema operacional.
Identificação de metadados	São identificadas informações sobre os arquivos que não são visíveis aos usuários comuns, como data de criação, autor, tipo de arquivo, entre outros dados relevantes.
Validação da autenticidade das evidências	As evidências coletadas são verificadas para garantir que não foram adulteradas. Um hash de arquivo é usado para essa verificação, pois é um valor exclusivo e irreversível calculado com base no conteúdo do arquivo.
Criação de imagens forenses	Será feita uma cópia exata da mídia de armazenamento contendo as evidências coletadas.

Fonte: adaptado da ISO/IEC 27037 (2013).

Em certas circunstâncias, pode não ser possível verificar a integridade da imagem forense, por exemplo, quando é adquirido um sistema em execução, quando existem erros setoriais na cópia original ou existem limitações de tempo na aquisição. Nessas circunstâncias, é crucial que o profissional de forense digital utilize o método mais adequado disponível e possa explicar e justificar sua escolha. Caso não seja possível verificar a imagem forense, é essencial registrar e justificar esse fato para garantir a admissibilidade e integridade das evidências digitais em um eventual processo judicial (ISO/IEC 27037, 2013).

5.1.6 Utilidade de um software na etapa de aquisição

Durante a aquisição, um *software* permite copiar o disco, partições ou arquivos relevantes para o caso em questão. Além disso, ela ajuda a documentar todos os métodos e atividades realizadas durante o processo, garantindo transparência e rastreabilidade.

Uma vantagem importante é que podem auxiliar verificar a integridade dos dados usando funções de verificação, como as funções de hash. Isso garante que as evidências originais e as cópias sejam idênticas, assegurando a integridade das evidências coletadas.

Esses dispositivos também podem facilitar o gerenciamento dos metadados das evidências, fornecendo informações relevantes, como datas, horários e propriedade dos arquivos.

As subseções a seguir deste trabalho mostram uma seleção de ferramentas pertinentes que se mostram valiosas para a etapa de aquisição, alinhadas às diretrizes estabelecidas pela norma.

5.1.6.1 Avilla Forensics

Avilla Forensics é uma ferramenta interessante para profissionais que trabalham com perícia em dispositivos móveis. Com recursos confiáveis e especializados, essa ferramenta oferece suporte na análise e captura detalhada de dados digitais.

Um dos seus recursos é o espelhamento de dispositivos. Esse recurso permite que você visualize a tela do seu dispositivo móvel em tempo real, facilitando a análise dos dados e o registro das evidências (AVILLA, 2023). Com o espelhamento, é possível capturar imagens e gravar vídeos diretamente do dispositivo, fornecendo uma abordagem completa durante o processo de investigação.

Através da utilização da interface do Android Debug Bridge (ADB), uma ferramenta de linha de comando versátil que possibilita a comunicação com dispositivos móveis, é possível

interagir de maneira prática e eficiente. Com uma capacidade de criar *backups* completos e instalar um agente personalizado para análise de dados em tempo real, essa ferramenta é desenvolvida em C# (HENRIQUES, 2022).

Essa variedade de coleções ADB incluem: informações de sistema, geolocalização, detalhes de CPU e memória, e muito mais. Essas coleções fornecem insights valiosos durante as investigações forenses (AVILLA, 2023).

Além disso, oferece a opção de realizar uma cópia única geral do dispositivo. Essa cópia garante a preservação integral dos dados, evitando qualquer alteração ou perda de informações durante a investigação. Ao realizar uma cópia única geral, os investigadores têm a certeza de que todas as evidências foram coletadas de forma íntegra, fortalecendo a validade e a confiabilidade dos resultados obtidos (AVILLA, 2023). Essa cópia é crucial para cumprir as diretrizes da norma, pois preserva todos os dados presentes no dispositivo, garantindo que nenhuma informação seja modificada ou perdida durante a etapa de aquisição. Isso contribui para a autenticidade das evidências e sua validade jurídica.

Ainda, por se tratar de uma ferramenta brasileira, ela está alinhada com as especificidades e demandas locais. Com sua interface intuitiva e recursos avançados, auxilia os profissionais a extrair e analisar dados de dispositivos móveis de forma precisa e eficiente, contribuindo para o sucesso de suas investigações.

É importante ressaltar que, como toda ferramenta recente, o Avilla Forensics pode apresentar algumas desvantagens. Por exemplo, ele ainda está em fase de desenvolvimento e passando por constantes aprimoramentos. Além disso, há uma quantidade limitada de documentação detalhada disponível.

Essa ferramenta pode desempenhar um papel fundamental na etapa de aquisição de evidências digitais. Seus recursos robustos e confiáveis permitem que os profissionais de forense digital realizem uma captura aprofundada e precisa de dados em dispositivos móveis.

Podendo ainda oferecer recursos avançados e confiáveis para a análise e captura de dados em dispositivos móveis. Sua capacidade de espelhamento de dispositivos, interação com a interface ADB e opção de cópia única geral do dispositivo são elementos-chave que contribuem para o sucesso das investigações forenses, garantindo a integridade, autenticidade e validade das evidências coletadas.

5.1.6.2 DDrescue

DDrescue é uma ferramenta de recuperação de dados que pode copiar dados de um arquivo ou dispositivo de bloco para outro, recuperando preferencialmente as partes sem erros de leitura. Desenvolvido pela equipe GNU, este *software* de código aberto está disponível gratuitamente (DDRESCUE ORG, 2022).

Um recurso útil dessa ferramenta é a mesclagem automática de *backups*. Se existir várias cópias corrompidas de arquivos, CD-ROMs, etc. e for executado o *DDrescue* em cada cópia separadamente com o mesmo arquivo de saída, é mais provável que se obtenha uma cópia completa do arquivo. Isso ocorre porque é altamente improvável que todas as cópias tenham a mesma área danificada, especialmente se os defeitos forem colocados aleatoriamente. Essa ferramenta usa um *mapfile* para ler apenas os blocos necessários da cópia adicional, aumentando ainda mais as chances de recuperação de dados bem-sucedida (DIAZ, 2023).

Durante o processo de geração de imagens de disco, o arquivo de saída do ddrescue difere significativamente dos arquivos de saída de outras ferramentas forenses, o que pode ser considerado uma desvantagem. Ao contrário das ferramentas projetadas especificamente para fins de perícia digital, o ddrescue não foi desenvolvido apenas com foco nessa área específica (COLLOTON *et al.*, 2019). Isso pode limitar sua utilidade em certos contextos forenses onde a precisão e a abrangência dos dados são essenciais.

Os algoritmos usados por essa plataforma são úteis para garantir assim uma aquisição de dados completa e confiável. O *DDrescue* tenta recuperar setores defeituosos em um disco rígido ou CD-ROM em quatro fases: copiar, cortar, raspar e tentar novamente. Isso é especialmente relevante para investigações forenses. Além disso, os usuários têm a flexibilidade de interromper o processo a qualquer momento, o que ajuda a limitar a quantidade de dados coletados ou a acelerar o processo. No entanto, é importante observar que uma falha de disco pode causar atrasos significativos nessa ferramenta, afetar a eficiência da captura e possivelmente exigir o desligamento do *kernel* (DIAZ, 2023).

O *DDrescue* oferece recursos que são especialmente relevantes e úteis na etapa de aquisição de evidências digitais. Com sua capacidade de recuperar partes sem erros de leitura, aliada à mesclagem automática de *backups*, aumenta consideravelmente as chances de obter cópias completas e íntegras dos arquivos desejados. Isso é particularmente importante em casos em que existem múltiplas cópias corrompidas.

Dessa maneira, com a funcionalidades que essa ferramenta possui, ela desempenha

um papel importante na garantia da integridade dos dados durante a etapa de aquisição, possibilitando a obtenção de evidências digitais confiáveis e completas para investigações forenses.

5.1.6.3 Digital Forensics Framework

Digital Forensics Framework (DFF) é uma estrutura forense de código aberto que ajuda a inspecionar discos rígidos e memória volátil, também a gerar relatórios sobre a atividade do usuário e do sistema. Sua interface facilita o processo de pesquisa digital, guiando automaticamente o usuário pelas principais etapas necessárias. Isso torna a condução de investigações e a resposta a incidentes mais rápida e fácil (ANGHEL, 2019).

Deve-se acrescentar ainda que essa estrutura desenvolvida em *Python* e C++ é uma arquitetura modular de plataforma cruzada combinada com uma interface de usuário intuitiva torna a aquisição, armazenamento e análise de evidências digitais rápida e fácil. A estrutura é baseada em uma *API* dedicada para garantir a integridade do sistema e dos dados em operação. Além disso, o DFF possui recursos como bloqueadores de gravação de *software* e cálculos de *hash* criptográfico para tornar as investigações mais seguras (BUBULEAN, 2015).

Essa ferramenta é utilizada por profissionais para coletar, armazenar e apresentar evidências digitais de forma ágil e eficiente, sem danificar os sistemas ou dados envolvidos. Segundo Kolla (2022), ela possui uma interface de linha de comando que permite uma análise digital remota usando recursos comuns, como preenchimento automático, gerenciamento de tarefas e atalhos de teclado. Além disso, o programa pode coletar, proteger e apresentar evidências digitais sem afetar os sistemas ou dados em questão.

Possui a capacidade de visualizar registros New Technology File System (NTFS), Extended File System (ExTFS) 2/3/4 e File Allocation Table (FAT) 12/16/32, caixas de correio e sistemas de arquivos, o DFF fornece aos usuários recursos forenses abrangentes. Isso inclui a capacidade de realizar pesquisas rápidas em metadados, expressões regulares, dicionários, conteúdo, *tags* e cronogramas. Além disso, esta ferramenta possui recursos avançados para recuperar artefatos ocultos e excluídos, como arquivos e pastas excluídos, espaço não alocado, escultura de arquivo, etc. Ele também oferece suporte à análise de memória volátil, permitindo que os usuários visualizem processos e arquivos locais, executem extrações binárias e inspecionem conexões de rede (BUBULEAN, 2015).

No entanto, o DFF apresenta duas desvantagens significativas: existe uma falta de documentação adequada para o seu uso e para acessar recursos adicionais, é necessário adquirir

uma licença paga (FZE, 2018). A primeira desvantagem pode acabar dificultando a compreensão e a implementação efetiva da plataforma, especialmente para usuários iniciantes ou menos familiarizados.

E ainda, as estruturas forenses digitais fornecem a capacidade de automatizar tarefas repetitivas por meio da execução de *scripts*. Usuários e engenheiros avançados podem usar esse *framework* por meio do mediador *Python* para pré-planejar suas investigações, tornando o processo mais eficiente e preciso (KOLLA, 2022). Essa abordagem agiliza a aquisição de evidências digitais e nos permite atender aos requisitos exigidos na etapa.

Dessa forma, o DFF é uma ferramenta forense que desempenha um papel essencial na etapa de aquisição de evidências digitais. Devido sua interface intuitiva e recursos avançados. Sua arquitetura modular e plataforma cruzada, juntamente com recursos como bloqueadores de gravação de software e cálculos de hash criptográfico, garantem a integridade dos sistemas e dados durante o processo. Com sua abordagem automatizada por meio de *scripts*, agiliza a aquisição de evidências digitais e atende aos requisitos exigidos nessa etapa.

5.1.6.4 EnCase Forensic

EnCase Forensic é uma ferramenta amplamente utilizada por diversos investigadores em todo o mundo. Fornecemos o ciclo de vida forense completo desde a investigação inicial até a coleta de dados, análise e relatórios. Os principais recursos do EnCase incluem relatórios abrangentes, recursos de escultura, captura de memória, imagem de disco e recuperação de senha (JAVED *et al.*, 2022).

Funcionalmente, oferece recursos avançados de processamento, análise e geração de relatórios. Para garantir a segurança dos dados diante de ameaças cibernéticas, essa ferramenta vem com suporte integrado para diferentes tipos de criptografia, como *Bitlocker*. Além disso, possui recursos eficientes de pesquisa de palavras-chave e opções de *script* estão disponíveis (DAS, 2019).

Essa ferramenta é utilizada para capturar dados digitais, analisá-los, criar relatórios e armazenar descobertas legalmente. Ele oferece recursos avançados de análise técnica para ajudar os investigadores a encontrar informações relevantes e ocultas para auxiliar nas investigações e atender aos requisitos de conformidade (ONDATA, 2023).

Para Das (2019), existem algumas limitações em relação ao suporte a dispositivos móveis. Ainda, o processo de análise executado pelo *Encase* usa uma abordagem de força bruta,

que pode desperdiçar uma quantidade significativa de tempo na conclusão de tarefas. Dessa forma, para digitalizar dispositivos móveis, é importante manter as essas considerações em mente.

Em resumo, o *EnCase Forensic* é amplamente utilizado durante a etapa de aquisição de evidências digitais devido aos seus recursos abrangentes e avançados. Recursos de processamento e análise técnica visando identificar informações relevantes e ocultas ajudam a tornar as investigações mais eficientes e precisas. Além disso, a ferramenta oferece recursos de segurança, como suporte para diferentes tipos de criptografia para garantir que seus dados estejam protegidos contra ameaças cibernéticas.

5.1.6.5 Conclusões sobre as ferramentas levantadas na etapa de aquisição

De acordo com as características levantadas das ferramentas Avilla Forensics, DDrescue, Digital Forensics Framework e EnCase Forensic em relação à etapa de aquisição da norma, podemos concluir que essas ferramentas fornecem recursos essenciais e diferenciados para uma aquisição eficiente e confiável de evidências digitais. A Tabela 9 mostra um resumo de algumas

Tabela 9 – Ferramentas da etapa de aquisição e suas características

Ferramenta	Características
Avilla Forensics	• Espelhamento de dispositivos para visualizar em tempo real. • Interação fácil com dispositivos. • Opção de fazer uma cópia única completa do dispositivo.
DDrescue	• Recuperação preferencial de dados sem erros em cópias corrompidas. • Mesclagem automática de backups. • Uso de um mapa para ler apenas os blocos necessários.
Digital Forensics Framework	• Interface intuitiva e orientação automatizada. • Arquitetura modular que suporta análise forense. • Bloqueadores de gravação de software .
EnCase Forensic	• Suporte completo ao ciclo de vida forense. • Recursos avançados de relatórios. • Suporte integrado para criptografia.

Fonte: elaborado pelo autor (2023).

das características levantadas sobre essas ferramentas.

Em resumo, essas ferramentas apresentam características únicas que são altamente relevantes para a etapa de aquisição de evidências digitais. Utilizando essas ferramentas, os profissionais de investigação forense têm acesso a recursos poderosos que contribuem para a integridade, a confiabilidade e a abrangência das evidências coletadas, atendendo aos padrões estabelecidos pela norma.

5.1.7 Preservação

A etapa de preservação desempenha um papel fundamental na proteção e integridade das evidências digitais durante uma investigação. Envolve o armazenamento seguro do dispositivo digital que pode conter evidências relevantes desde o momento em que são identificadas até o final do processo. Para garantir a utilidade e a confiabilidade das evidências digitais, é importante iniciar o processo de preservação o mais cedo possível e mantê-lo durante todo o processo (ISO/IEC 27037, 2013). Na Tabela 10 são exibidos alguns dos processos durante a etapa de preservação, Esses processos contribuem para a preservação adequada das evidências digitais, seguindo os padrões estabelecidos pela norma.

Além disso, para evitar a espoliação, é crucial considerar os aspectos do ambiente e implementar medidas apropriadas. É fundamental garantir o uso de uma função de verificação

Tabela 10 – Processos da etapa de preservação

Processo	Descrição
Armazenamento das evidências coletadas	A realização desse processo em um local seguro e controlado é fundamental para manter a integridade das evidências ao longo do tempo.
Criação de backups das evidências	É importante criar uma cópia de backup que seja preservada de forma confiável em caso de falha ou problema na memória principal.
Controle de acesso às evidências	É importante gerenciar o acesso às evidências e garantir que apenas pessoas autorizadas possam trabalhar com elas.
Identificação de vulnerabilidades	É importante identificar e corrigir quaisquer vulnerabilidades nos sistemas ou dispositivos utilizados, a fim de garantir sua segurança e a preservação adequada das evidências.
Manutenção de registros	É importante documentar quem teve acesso às evidências coletadas, quais atividades foram realizadas e quais procedimentos foram seguidos para garantir sua integridade e confiabilidade.

Fonte: adaptado da ISO/IEC 27037 (2013).

adequada para comprovar que os arquivos copiados são idênticos aos originais. Além disso, pode ser recomendável associar a evidência digital adquirida a assinaturas digitais, biometria ou fotografias, quando aplicável (ISO/IEC 27037, 2013).

De acordo com Neto e Santos (2020), é crucial que o processo de preservação de provas englobe tanto a proteção meticulosa das evidências físicas quanto dos dispositivos digitais, com o objetivo de assegurar a confiabilidade das informações coletadas. É essencial reduzir ao mínimo as manipulações realizadas nas evidências e nos dispositivos, registrando todas as alterações e ações efetuadas. Ademais, é de extrema importância que os peritos forenses atuem em suas áreas de especialização, a fim de garantir a qualidade e a confiabilidade do processo de preservação das provas digitais.

5.1.8 Utilidade de um software na etapa de preservação

Uma ferramenta forense pode facilitar o armazenamento seguro de dispositivos digitais e evidências relevantes, garantindo a criptografia de dados, o acesso restrito e o controle de permissões. Além disso, ela auxilia registrando todas as alterações e ações realizadas nas evidências digitais.

A verificação de integridade é outra funcionalidade importante oferecida pelas ferramentas forenses. Elas realizam verificações para garantir que os arquivos copiados sejam idênticos aos originais, por meio de funções de hash e comparação de assinaturas digitais.

A preservação de metadados e informações associadas às evidências também é contemplada pelas ferramentas forenses. Elas garantem a integridade dessas informações, como data e horário, assinaturas digitais, biometria ou fotografias.

Além disso, elas automatizam processos, reduzindo erros e aumentando a eficiência. Elas oferecem recursos como criação de relatórios automatizados, geração de registros de auditoria e documentação detalhada de todas as etapas do processo de preservação.

Em suma, as ferramentas de software forense desempenham um papel essencial na etapa de preservação das evidências digitais. Elas proporcionam recursos de armazenamento seguro, garantia de integridade, preservação de metadados e automação de processos, contribuindo para a eficácia e confiabilidade das investigações forenses. As próximas subseções deste trabalho descrevem algumas das ferramentas disponíveis para aplicação da etapa de preservação.

5.1.8.1 Bulk Extractor

O *Bulk Extractor* é um programa poderoso que permite extrair informações relevantes, como endereços de e-mail, números de cartão de crédito e *Uniform Resource Locator (URL)*, de qualquer tipo de evidência digital. Ele é capaz de trabalhar com diferentes formatos de imagens de disco e oferece suporte para a análise de tráfego de rede, memória e arquivos baixados da Internet. Além disso, o programa possibilita a conexão direta de dispositivos de mídia ao computador do analista, por exemplo, utilizando um bloqueador de gravação. Os dados a serem analisados são divididos em páginas e processados por um ou mais *scanners*. As informações identificadas são armazenadas em arquivos de recursos, que apresentam um formato simples contendo detalhes sobre os recursos extraídos, incluindo sua localização e contexto (GARFINKEL, 2013).

Para Alazab *et al.* (2023), essa ferramenta se destaca das outras ferramentas forenses por sua rapidez e abrangência. Ele é capaz de processar várias áreas do disco simultaneamente, sem se preocupar com a estrutura do sistema de arquivos. Além disso, ele pode recuperar dados de qualquer tipo de arquivo compactado, demonstrando sua eficácia contra diversos algoritmos. O programa também consegue reduzir a quantidade de dados sem afetar as evidências importantes e os dados de inteligência.

É amplamente reconhecido como uma ferramenta forense digital essencial e altamente conceituada. Sua capacidade de analisar imagens de disco, arquivos e diretórios em busca de informações valiosas é inigualável. Ao contrário de outras ferramentas semelhantes, ignora a estrutura do sistema de arquivos, garantindo uma velocidade impressionante. Essa poderosa ferramenta é amplamente utilizada por agências de inteligência e aplicação da lei para solucionar crimes cibernéticos de forma eficaz (ADIL, 2020).

Uma desvantagem dessa ferramenta é a falta de suporte ou atualizações frequentes. Dependendo da versão e do desenvolvedor, pode haver lacunas na assistência técnica ou na correção de *bugs*. Isso pode resultar em problemas de compatibilidade com novos sistemas operacionais, formatos de arquivo ou algoritmos de criptografia, diminuindo a eficácia da ferramenta ao lidar com casos mais recentes.

Pode ser útil na etapa de preservação, pois ela é capaz de extrair informações relevantes de forma eficiente, preservando a integridade dos dados originais. Sendo capaz de analisar imagens de disco, arquivos ou diretórios de arquivos, e extrair informações úteis sem comprometer a estrutura do sistema de arquivos. Isso permite preservar a evidência digital e

obter dados importantes sem modificar ou alterar os arquivos originais. Isso significa que as evidências digitais podem ser preservadas e analisadas sem modificar ou alterar os arquivos originais, garantindo a confiabilidade e a autenticidade das informações coletadas.

Possuindo ainda uma capacidade abrangente de processamento e velocidade impressionante, o *Bulk Extractor* pode ajudar os investigadores a lidar com grandes volumes de dados de forma eficaz, contribuindo para o sucesso da etapa e das investigações forenses.

5.1.8.2 Forensic Explorer

Forensic Explorer (FEX) oferece uma interface gráfica intuitiva e recursos avançados para facilitar a análise forense. Com recursos de classificação, filtragem, busca por palavras-chave, recuperação de dados e *script*, essa ferramenta permite processar grandes volumes de dados de forma rápida e automatizar tarefas complexas de investigação. Ainda, ela gerencia todos os aspectos da investigação, incluindo análise do sistema de arquivos, busca de palavras-chave, virtualização de boot ao vivo, *e-mail*, registro e relatórios detalhados (GETDATAFORENSICS, 2023).

Segundo Singh e Yadav (2023), essa ferramenta é amplamente utilizada por agências policiais, governamentais e militares para armazenamento e análise de memória. A interface de usuário simplificada melhora a usabilidade e pode lidar com grandes quantidades de dados para gerar relatórios detalhados sobre análise de arquivos, registro e virtualização de inicialização.

Além disso, os recursos deste software incluem recursos antivírus integrados, capacidade de sinalizar possíveis evidências, gerenciamento de casos, acesso a dados em diferentes níveis, ferramentas para restaurar arquivos conhecidos, suporte por e-mail e opções de exportação de arquivos. A ferramenta oferece funções de valores de resumo, funções de indexação, suporte para vários algoritmos de criptografia e recursos personalizáveis. Esses recursos oferecem ao usuário uma ampla gama de possibilidades para ajustar o ambiente de trabalho para atender às suas necessidades durante o exame (GETDATAFORENSICS, 2023).

Para Lee e Soh (2020b), embora ofereça suporte a várias funcionalidades, como unidades de instalação do sistema operacional, imagens e dispositivos portáteis, sua desvantagem significativa é a necessidade de escrever *scripts* em Pascal para análise. Isso implica que os usuários precisam adquirir conhecimento nessa linguagem específica, o que pode ser um obstáculo para muitos investigadores.

Portanto, a ferramenta FEX pode ser uma aliada valiosa na etapa de preservação,

pois facilita a análise forense, a proteção das evidências e a obtenção de informações cruciais sem comprometer a integridade dos dados originais. Sua interface intuitiva e recursos avançados contribuem para a preservação adequada das evidências digitais durante todo o processo de investigação.

5.1.8.3 Indexador e Processador de Evidência Digital

O Indexador e Processador de Evidência Digital (IPED) é uma ferramenta em *Java* desenvolvida por peritos investigativos forenses da Polícia Federal do Brasil desde 2012. Seu código foi lançado oficialmente em 2019. Esta ferramenta visa o processamento eficiente e estável de dados digitais. Algumas de suas características importantes incluem o processamento por linha de comando para criação de casos em lote, suporte a diferentes sistemas operacionais como *Windows* e *Linux*, portabilidade de casos que podem ser executados em unidades removíveis, uma interface de análise integrada e intuitiva, desempenho avançado com múltiplas *threads* e suporte para casos de grande escala. Além disso, utiliza a Biblioteca *Sleuthkit* para decodificar imagens de disco e sistemas de arquivos, oferecendo suporte para diversos formatos de imagem (NASSIF, 2023).

Essa ferramenta forense possui diversos meios para facilitar a análise de evidências digitais. Ela oferece recursos como cálculo de valor de resumo, análise de assinaturas, expansão de contêineres, indexação de arquivos, geração de miniaturas e varredura de expressões regulares. Embora a recuperação de dados não seja uma funcionalidade habilitada, o IPED é capaz de recuperar arquivos com base nas tabelas do sistema de arquivos, proporcionando uma visão abrangente das informações relevantes (NASSIF, 2023).

Para Tolosa (2022), o processamento ocasionalmente pode apresentar travamentos em determinados itens. Isso pode ocorrer devido à falta de controle de tempo limite em algumas tarefas aparentemente simples, que dependem de bibliotecas externas que podem conter bugs.

Trata-se de um programa que utiliza linhas de comando e oferece diversas funcionalidades encontradas em *softwares* forenses. Isso inclui o processamento de imagens, a categorização de arquivos, a detecção de arquivos criptografados, o cálculo e consulta à base de valores de resumo, e, principalmente, a indexação de conteúdo. A capacidade de indexação permite realizar buscas de forma mais fácil e rápida (SILVA; SILVA, 2019).

Além disso, também possui recursos avançados, como a identificação rápida de duplicatas, análise de assinaturas, categorização por tipo de arquivo e suas propriedades, e a

capacidade de expandir contêineres recursivamente em diversos formatos de arquivo. Existe a possibilidade de expandir discos forenses ou virtuais (NASSIF, 2023).

O uso dessa ferramenta é fundamental para preservar as evidências digitais de forma eficiente. Com recursos avançados para criação de casos em lote e compatibilidade com diferentes formatos de imagem de disco e sistemas de arquivos, torna-se facilitado o processamento de grandes volumes de dados, garantindo a preservação adequada das evidências. Adicionalmente, oferece recursos de *hashing* e indexação que agilizam a identificação e recuperação de informações relevantes, seguindo as diretrizes da norma. Ao utilizar essa ferramenta, os profissionais de investigação forense têm uma solução confiável para preservar a integridade e validade das evidências ao longo de todo o processo.

Assim, o IPED se mostra uma ferramenta valiosa na etapa de preservação, facilitando o processo de análise forense e garantindo a manutenção da integridade das evidências digitais.

5.1.8.4 OSForensics

OSForensics é uma ferramenta que fornece informações detalhadas sobre o uso do seu computador e os arquivos armazenados nele. Esta ferramenta permite aos usuários gerenciar suas tarefas e projetos de forma mais eficiente. Os recursos de investigação forense do sistema operacional permitem que você monitore a atividade do usuário e obtenha assistência jurídica para as investigações. De fácil instalação, a ferramenta permite ao usuário pesquisar documentos específicos, recuperar dados apagados, rastrear atividades e gerar relatórios com informações especiais sobre o sistema Kolla (2022).

Com essa ferramenta, é possível pesquisar arquivos com base em critérios como nome, tamanho, datas de criação e modificação. Além disso, é oferecido diferentes exibições de resultados, incluindo uma exibição de linha do tempo para ajudá-lo a entender os padrões de atividade do usuário em seu computador (OSFORENSICS, 2023a).

Além disso, essa ferramenta oferece a capacidade de criar uma identificação exclusiva para seus arquivos usando algoritmos de *hash* avançados. Essa identificação pode ser usada para verificar se um arquivo foi corrompido ou alterado e para ajudar a identificar arquivos desconhecidos de arquivos conhecidos. O software também pode identificar rapidamente arquivos suspeitos ou conhecidos usando frases de identificação, reduzindo a necessidade de análises demoradas. Esse recurso inclui a detecção de arquivos maliciosos, ilegais ou incriminatórios, como conteúdo pirata, pornografia, vírus e arquivos de evidências (OSFORENSICS, 2023b).

Para Bhat *et al.* (2021b), embora o *OSForensics* se destaque em algumas áreas, suas limitações em relação à detecção precisa de certos ataques AF e sua inabilidade de identificar completamente espaços ocultos ou ataques de falsificação de dados, podem acabar enfraquecendo sua eficácia em uma análise forense mais abrangente.

Durante a etapa de preservação de evidências o *OSForensics* pode ser uma opção útil para investigadores forenses. Ele oferece recursos que permitem coletar e preservar informações da máquina de forma adequada, garantindo a integridade das evidências digitais para análises futuras. Com essa ferramenta, devido a possibilidade de criar uma assinatura da estrutura de diretórios da unidade no momento da coleta, facilitando a identificação de possíveis alterações suspeitas nos arquivos ou na estrutura. Além disso, é capaz de auxiliar na recuperação de dados excluídos e no rastreamento da atividade do usuário.

Suas características avançadas de busca, recuperação de dados e geração de relatórios permitem que os investigadores identifiquem, capturem e preservem adequadamente as evidências digitais relevantes.

5.1.8.5 Conclusões sobre as ferramentas levantadas na etapa de preservação

A Tabela 11 apresenta alguns dos levantamentos encontrados sobre o Bulk Extractor, Forensic Explorer, Indexador e Processador de Evidência Digital e OSForensics.

Tabela 11 – Ferramentas da etapa de preservação e suas características

Ferramenta	Características
Bulk Extractor	• Suporta análise de tráfego de rede e arquivos. • Preserva a integridade dos dados originais.
Forensic Explorer	• Gerencia casos e gera relatórios detalhados. • Preserva a integridade das evidências digitais.
Indexador e Processador de Evidência Digital	• Realiza análise, indexação e busca de arquivos. • Cria identificações exclusivas para arquivos.
OSForensics	• Pesquisa arquivos com diferentes critérios. • Identifica arquivos usando algoritmos de hash. • Recupera dados apagados e gera relatórios detalhados.

Fonte: elaborado pelo autor (2023).

Em resumo, essas ferramentas apresentam características únicas que contribuem para a etapa de preservação, permitindo a análise e o processamento eficientes de evidências digitais, enquanto garantem a integridade dos dados. A escolha da ferramenta mais adequada dependerá das necessidades específicas de cada caso e das preferências dos investigadores forenses.

5.2 Observações finais sobre as ferramentas propostas

Ao final deste trabalho, as ferramentas foram organizadas de acordo com a estrutura apresentada na Tabela 12. Cada seção específica das ferramentas abordou suas vantagens, possíveis desvantagens, funcionalidades e a sua importância dentro da respectiva etapa em que foi proposta.

Tabela 12 – Divisão por etapa das ferramentas forenses

Identificação	Coleta	Aquisição	Preservação
The Sleuth Kit	Autopsy	Avilla Forensics	Bulk Extractor
Volatility	Forensic Toolkit	DDrescue	Forensic Explorer
WinHex	Oxygen Forensic Suite	Digital Forensics Framework	IPED
Xplico	X-Ways Forensics	EnCase Forensic	OSForensics

Fonte: elaborado pelo autor (2023).

Essa abordagem permitiu uma análise abrangente das características e contribuições de cada ferramenta, fornecendo uma visão clara sobre sua relevância no contexto da investigação forense digital.

Na Tabela 13, foram listados os tipos de software correspondentes a cada ferramenta, indicando se são de código aberto ou comerciais, juntamente com os sistemas operacionais nos quais essas ferramentas podem ser executadas, com base na pesquisa realizada. Possibilitando uma visão abrangente das características de cada ferramenta, incluindo sua disponibilidade e compatibilidade com diferentes sistemas operacionais.

É importante ressaltar que a divisão das ferramentas de acordo com as etapas estabelecidas pela norma ISO/IEC 27037 (2013) é apenas uma abordagem geral e com o propósito de organização.As ferramentas foram classificadas levando em consideração suas características, a etapa em que esses atributos podem ser aplicáveis e com o objetivo de abranger uma ampla gama de opções disponíveis na área de investigação forense digital. Dessa forma, a ordem de apresentação reflete a seleção criteriosa para contemplar diferentes aspectos e atender às necessidades variadas nesse campo. Dessa forma, busca-se oferecer uma variedade de ferramentas para

Tabela 13 – Tipos dos softwares e os ambientes onde eles podem ser executados

Ferramenta	Tipo do Software	Sistema Operacional
Autopsy	Livre	Linux, MAC e Windows
Avilla Forensics	Livre	Windows
Bulk Extractor	Livre	Linux, MAC e Windows
DDrescue	Livre	Linux
Digital Forensics Framework	Livre	Linux e Windows
EnCase Forensic	Comercial	Windows
Forensic Explorer	Comercial	MAC e Windows
Forensic Toolkit	Comercial	Windows
IPED	Livre	Linux e Windows
OSForensics	Comercial	Windows
Oxygen Forensic Suite	Livre	Windows
The Sleuth Kit	Livre	Linux e Windows
Volatility	Livre	Linux, MAC e Windows
WinHex	Comercial	Windows
X-Ways Forensics	Comercial	Windows
Xplico	Livre	Linux

Fonte: elaborado pelo autor (2023).

atender às diferentes necessidades e preferências de profissionais da área.

Dependendo do contexto específico e dos recursos de cada ferramenta, suas capacidades podem ser aplicáveis em etapas adicionais ou variar em relação às informações fornecidas. É importante consultar a documentação oficial de cada ferramenta para obter informações detalhadas sobre suas funcionalidades e aplicabilidade em cada etapa do processo forense.

6 CONCLUSÕES E TRABALHOS FUTUROS

A presente pesquisa teve como objetivo analisar e identificar as ferramentas de computação forense aplicadas nas investigações no Brasil, em conformidade com a norma ABNT ISO/IEC 27037:2013. Ao longo deste estudo, foram exploradas as etapas da norma: identificação, coleta, aquisição e preservação, cada uma com suas particularidades e processos específicos.

Durante o levantamento das ferramentas em utilização no Brasil, foram selecionadas quatro ferramentas para cada etapa, levando em consideração suas funcionalidades e características relevantes. Essa análise proporcionou uma melhor compreensão sobre a diversidade de ferramentas disponíveis no mercado e sua aplicabilidade nas investigações digitais brasileiras.

A norma desempenha um papel muito importante ao estabelecer diretrizes e princípios que buscam padronizar e assegurar a correta manipulação das evidências digitais. Ao seguir essas diretrizes, é possível garantir a integridade, autenticidade e admissibilidade das evidências no âmbito forense.

No entanto, é importante ressaltar que a aplicação da dela vai além do uso de ferramentas específicas. O cumprimento adequado da norma requer a implementação de um conjunto abrangente de processos e procedimentos, adaptados de acordo com os requisitos estabelecidos.

Ao final deste estudo, podemos concluir que as ferramentas de computação forense desempenham um papel crucial na investigação de crimes digitais, contribuindo para uma identificação, coleta, aquisição e preservação adequada das evidências. A seleção criteriosa dessas ferramentas, considerando suas funcionalidades, confiabilidade e conformidade com as práticas forenses aceitas, é fundamental para o sucesso das investigações.

Por fim, este trabalho busca fornecer um panorama geral das ferramentas de computação forense utilizadas no Brasil, bem como destacar a importância da norma ABNT ISO/IEC 27037:2013 na garantia da qualidade e confiabilidade das investigações digitais. Espera-se que os resultados deste estudo contribuam para o aperfeiçoamento das práticas forenses no país e auxiliem os profissionais e pesquisadores a realizar investigações mais eficientes e confiáveis no campo da computação forense.

Para trabalhos futuros, deseja-se aprofundar-se nas ferramentas propostas, com especial atenção para aquelas desenvolvidas no Brasil. É importante explorar e analisar mais detalhadamente essas ferramentas, bem como compreender como elas podem contribuir de forma única para o campo da perícia forense no Brasil.

REFERÊNCIAS

ADAMU, H.; AHMAD, A. A.; HASSAN, A.; GAMBASHA, S. B. Web browser forensic tools: Autopsy, bhe and netanalysis. **International Journal of Research and Scientific Innovation (IJRSI)**, v. 8, n. 5, p. 103–107, 2021.

ADIL, J. **Computação Forense**. 2020. Disponível em: https://acaditi.com.br/computacao-forense/. Acesso em: 30 jun 2023.

ALAZAB, A.; KHRAISAT, A.; SINGH, S. A review on the internet of things (iot) forensics: Challenges, techniques, and evaluation of digital forensic tools. In: ____. [*S. l.*: *s. n.*], 2023.

ALMUTAIRI, A.; SATARI, B. S.; RIVAS, C.; STANCIU, C. F.; YAMANI, M.; ZOHOORSAADAT, Z.; MOKHOV, S. A. Evaluation of autopsy and volatility for cybercrime investigation. **International Journal of Digital Crime and Forensics**, v. 12, n. 1, p. 58–89, 2020.

ANGHEL, C. Digital forensics – a literature review. **The Annals of "Dunarea de Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics**, v. 42, n. 1, p. 23–27, 2019.

AVILLA, D. **Avilla Forensics: Ferramenta Gratuita para Coleta e Análise de Smartphones**. 2023. Disponível em: https://github.com/AvillaDaniel/AvillaForensics. Acesso em: 30 junho 2023.

BHAT, W. A.; ALZAHRANI, A.; WANI, M. A. Can computer forensic tools be trusted in digital investigations? **Science Justice**, v. 61, n. 2, p. 198–203, 2021.

BHAT, W. A.; ALZAHRANI, A.; WANI, M. A. Can computer forensic tools be trusted in digital investigations? **Science Justice**, v. 61, n. 2, p. 198–203, 2021.

BIGELOW, D. **Troubleshooting and Maintaining Your PC All-in-One For Dummies, 4th Edition**. [*S. l.*]: Wiley, 2020.

BRASIL. lei, **Lei do Software**: Lei nº 9609, de 19 de fevereiro de 1998. 1998.

BRASIL. lei, **Lei do Processo Judicial Eletrônico**: Lei nº 11419, de 19 de dezembro de 2006. 2006.

BRASIL. lei, **Lei das Perícias Oficiais**: Lei nº 12.030, de 17 de setembro de 2009. 2009.

BRASIL. lei, **Lei de Acesso à Informação**: Lei nº 12.527, de 18 de novembro de 2011. 2011.

BRASIL. lei, **Lei Carolina Dieckman**: Lei nº 12.737, de 30 de novembro de 2012. 2012.

BRASIL. lei, **Marco Civil da Internet**: Lei nº 12.965, de 23 de abril de 2014. 2014.

BRASIL. lei, **Lei Geral de Proteção de Dados Pessoais**: Lei nº 13.709, de 14 de agosto de 2018. 2018.

BUBULEAN, C. Digital forensics capabilities in an open source framework. **Journal of Mobile, Embedded and Distributed Systems**, v. 7, n. 2, p. 60–64, 2015.

CARBONE, F. **Computer Forensics with FTK**. [*S. l.*]: Packt Publishing Ltd, 2014.

CARRIER, B. **File system forensic analysis**. [*S. l.*]: Addison-Wesley Professional, 2005.

CARRIER, B. **Autopsy**. 2023. Disponível em: sleuthkit.org/autopsy/. Acesso em: 05 jun. 2023.

CARRIER, B. **The Sleuth Kit 4.12.0**. 2023. Disponível em: https://github.com/sleuthkit/sleuthkit/releases. Acesso em: 20 mai. 2023.

CASE, A. **Volatility**. 2020. Disponível em: https://github.com/volatilityfoundation/volatility/wiki. Acesso em: 20 mai. 2023.

CASEY, E. **Digital Evidence and Computer Crime**: Forensic science, computers and the internet. [*S. l.*]: Elsevier, 2011. v. 3.

CHAVES, A.; CAVALCANTE, E.; COSTA, A.; FERREIRA, R. A lgpd e a perícia forense computacional: Uma relação necessária. **Revista UNIABEU**, v. 13, n. 36, p. 34–45, 2020.

CHAWKI, M.; DARWISH, A.; KHAN, M. A. **Cybercrime, Digital Forensics and Jurisdiction**. [*S. l.*]: Springer, 2015. v. 593.

COLLOTON, E.; FARBOWITZ, J.; FORTUNATO, F.; GIL, C. Towards best practices in disk imaging: A cross-institutional approach. **Electronic Media Review**, v. 6, 2019.

COSTA, M. A. S. L. **Computação Forense - A análise forense no contexto da resposta a acidentes computacionais**. [*S. l.*]: Millennium, 2011. v. 3.

DAS, R. **Comparison of Popular Computer Forensics Tools**. 2019. Disponível em: https://resources.infosecinstitute.com/topic/comparison-popular-computer-forensics-tools/. Acesso em: 20 jun. 2023.

DATA, S. **The Top 20 Open Source Digital Forensic Tools for 2023**. 2023. Disponível em: https://www.salvationdata.com/work-tips/the-top-20-open-source-digital-forensic-tools-for-2023/. Acesso em: 20 jun. 2023.

DDRESCUE ORG. **Ddrescue**: Data recovery tool. 2022. Disponível em: https://www.gnu.org/software/ddrescue/. Acesso em: 06 jun. 2023.

DIAZ, A. **GNU ddrescue Manual**. 2023. Disponível em: https://www.gnu.org/software/ddrescue/manual/ddrescue_manual.html#Introduction. Acesso em: 06 jun. 2023.

DWEIKAT, M.; ELEYAN, D.; ELEYAN, A. Digital forensic tools used in analyzing cybercrime. **Journal of University of Shanghai for Science and Technology**, v. 23, n. 3, p. 367–379, 2021.

ELEUTéRIO, P. M. d. S.; MACHADO, M. P. **Desvendando a Computação Forense**. [*S. l.*]: Novatec Editora, 2011. v. 1.

EXTERRO. **FTK® Forensic Toolkit**. 2023. Disponível em: https://www.exterro.com/forensic-toolkit. Acesso em: 20 mai. 2023.

FACHONE, P.; VELHO, L. Ciência forense: Interseção justiça, ciência e tecnologia. **revista tecnologia e sociedade**, v. 3, p. 139–161, 2007.

FERNANDO, D. N.; RUPASINGHE, D. L. Forensic investigation tool for volatility framework. **International Journal of Innovative Science and Research Technology**, v. 7, n. 3, p. 334–338, 2022.

FLEISCHMANN, S. **Ways Forensics/WinHex**: physics and effects. [*S. l.*]: X-Ways Software Technology AG, 2023.

FZE, B. B. C. **Improvement of Open-Source Digital Forensics Toolkit**. 2018. Disponível em: https://ukdiss.com/examples/open-source-digital-forensics-toolkit.php?vref=1. Acesso em: 05 jun. 2023.

GALVãO, R. K. M. Computer forensics with the sleuth kit and the autopsy forensic browser. **The International Journal of FORENSIC COMPUTER SCIENCE**, n. 1, p. 41–44, 2016.

GARFINKEL, S. L. Digital media triage with bulk data analysis and bulk extractor. **Comput. Secur.**, Elsevier Advanced Technology Publications, v. 32, n. C, p. 56–72, 2013.

GETDATAFORENSICS. **About Forensic Explorer**. 2023. Disponível em: https://getdataforensics.com/product/forensic-explorer-fex/. Acesso em: 15 jun. 2023.

GOGAN, M. **Comparative Analysis of Free Tools for Physical Memory Dumps Parsing**. disponível em: https://soshace.com/comparative-analysis-of-free-tools-for-physical-memory-dumps-parsing/: [*S. n.*], 2020. Acesso em: 20 mai. 2023.

HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. **d i g i t a l i n v e s t i g a t i o n**, v. 3, p. 44–49, 2006.

HENRIQUES, A. **Avilla Forensics: Ferramenta Gratuita para Coleta e Análise de Smartphones**. disponível em: https://academiadeforensedigital.com.br/avilla-forensics-ferramenta-gratuita-de-analise-de-smartphones/: [*S. n.*], 2022. Acesso em: 30 jun. 2023.

HERMON, R.; SINGH, U.; SINGH, B. Ntfs: Introduction and analysis from forensics point of view. In: **2023 International Conference for Advancement in Technology (ICONAT)**. [*S. l.*]: International Institute of Informatics and Systemics, 2023. p. 1–6.

HILGERT, J.-N.; LAMBERTZ, M.; PLOHMANN, D. Extending the sleuth kit and its underlying model for pooled storage file system forensic analysis. **Digital Investigation**, n. Supplement, p. 98–117, 2017.

HOUCK, M. M.; SIEGEL, J. A. **Fundamentals of Forensic Science**. [*S. l.*]: Elsevier, 2015. v. 3.

ISO. **ISO/IEC Guide 21-1:2005**. 2005. International Organization for Standardization. Disponível em: https://www.iso.org/standard/39799.html. Acesso em: 30 jun. 2023.

ISO/IEC 27037. **Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança**: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013. https://www.abntcatalogo.com.br/pnm.aspx?Q=NDlLZHR1a1ZUajB2WUJLRFc0c2tsNjd3RGRHN25lajNRa2tIR2U1Z3FzYz0=. Acesso em: 05 jun. 2023.

JAVED, A. R.; AHMED, W.; ALAZAB, M.; JALIL, Z.; KIFAYAT, K.; GADEKALLU, T. R. A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. **IEEE Access**, v. 10, p. 11065–11089, 2022.

JOHNSON, L. **Computer Incident Response and Forensics Team Management Conducting a Successful Incident Response**. [*S. l.*]: Syngress, 2014. v. 1.

KAMBLE, D.; JAIN, N.; DESHPANDE, S. Cybercrimes solutions using digital forensic tools. **International Journal of Wireless and Microwave Technologies**, v. 5, p. 11–18, 2015.

KAUR, P.; MISRA, N. A methodical review on network traffic monitoring analysis tools. **A JOURNAL OF COMPOSITION THEORY**, v. 12, n. 9, p. 1964–1968, 2019.

KHALAF, R. S.; VAROL, A. Digital forensics: Focusing on image forensics. **7th International Symposium on Digital Forensics and Security (ISDFS)**, p. 1–5, 2019.

KOLLA, V. R. K. A comparative analysis of os forensics tools. **International Journal of Research in IT and Management (IJRIM)**, v. 12, n. 4, p. 11–24, 2022.

LEE, J.-U.; SOH, W.-Y. Comparative analysis on integrated digital forensic tools for digital forensic investigation. **IOP Conference Series: Materials Science and Engineering**, v. 834, p. 12–34, 2020.

LEE, J.-U.; SOH, W.-Y. Comparative analysis on integrated digital forensic tools for digital forensic investigation. **IOP Conference Series: Materials Science and Engineering**, IOP Publishing, v. 834, n. 1, p. 012–034, 2020.

LOCARD, E. **Principles of judicial identification**. Baltimore: Warwick and York, 1925. 276 p.

MARAS, M.-H. **Computer forensics : cybercriminals, laws, and evidence**. [*S. l.*]: Jones Bartlett Learning, 2015. v. 2.

MARSHALL, A. M. **Digital forensics : digital evidence in criminal investigation**. [*S. l.*]: Wiley-Blackwell, 2008. v. 1.

MARSHALL, A. M. Digital forensic tool verification: An evaluation of options for establishing trustworthiness. **Forensic Science International: Digital Investigation**, v. 38, n. 1, p. 1–5, 2021.

MONTEIRO, M. F. A. **Investigação Digital de Crimes Eletrônicos**. [*S. l.*]: Brasport, 2016.

NASSIF, L. F. **IPED Digital Forensic Tool**. 2023. Disponível em: https://github.com/sepinf-inc/IPED#iped-digital-forensic-tool. Acesso em: 10 jun. 2023.

NELSON, B.; PHILLIPS, A.; STEUART, C. **Guide to Computer Forensics and Investigations: Processing Digital Evidence**. [*S. l.*]: Cengage, 2019. v. 6.

NETO, M. F.; SANTOS, J. E. L. d. Apontamentos sobre a cadeia de custÓdia da prova digital no brasil. **Em Tempo**, v. 20, 2020.

OLIVEIRA, V. M. d. **ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/: [*S. n.*], 2019. Acesso em: 6 fev. 2022.

ONDATA. **Encase Forensic Software**: Características e funções. 2023. Disponível em: https://www.ondata-pt.com/recuperacao-dados/encase_forensic.htm. Acesso em: 10 jun. 2023.

OSFORENSICS. **Find files faster**. 2023. Disponível em: https://www.osforensics.com/. Acesso em: 15 jun. 2023.

OSFORENSICS. **Verify and Match Files**. 2023. Disponível em: https://www.osforensics.com/verify-and-match-files.html. Acesso em: 15 jun. 2023.

PANIGRAHI, G. R.; BARPANDA, N. K.; MISHRA, S. **A Review on: the Rise in Cyber Forensics Innovations**. 2021.

PEREIRA, K. d. S.; OLIVEIRA, F. M. d. Pericia forense computacionall e crimes cinernéticos. **Revista Interdisciplinar do Pensamento Científico**, v. 5, p. 210–228, 2019.

RODRIGUES, C. V.; SILVA, M. T. d.; TRUZZI, O. M. S. **Perícia criminal**: uma abordagem de serviços. 2011. Disponível em: https://www.scielo.br/j/gp/a/cdqMpjgTTNvKtqXJQ5KGJdg/?lang=pt#. Acesso em: 6 fev. 2022.

SAFERSTEIN, R. **Criminalistics : an introduction to forensic science**. [*S. l.*]: Pearson, 2018. v. 12.

SILVA, F. C. d.; SILVA, P. C. d. **Metodologia e análise utilizadas na solução de crimes sexuais contra crianças e adolescentes na era digital**: um estudo de caso baseado no software iped. 2019. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/4263. Acesso em: 10 jun. 2023.

SINGH, D.; YADAV, R. A comprehensive study and implementation of memory malware analysis with its application for the case study of cridex. **Intelligent Cyber Physical Systems and Internet of Things**, v. 3, p. 31–44, 2023.

STüTTGEN, J.; COHEN, M. Anti-forensic resilient memory acquisition. **d i g i t a l i n v e s t i g a t i o n**, v. 10, p. 105–115, 2013.

TAVARES, G. M. **Perícia forense computacional e o Marco Civil da Internet**. disponível em: https://www.jota.info/opiniao-e-analise/artigos/pericia-forense-computacional-e-o-marco-civil-da-internet-11082020: [*S. n.*], 2020. Acesso em: 25 de mar. de 2023.

TOLOSA, C. A. P. **Indexador e processador de evidências digitais (IPED)**: Um poderoso software forense computacional. Instituto Federal de educação, Ciência e Tecnologia do Amapá, 2022. Disponível em: http://repositorio.ifap.edu.br/jspui/handle/prefix/673. Acesso em: 10 jun. 2023.

VELHO, J. A.; GEISER, G. C. O.; ESPINDULA, A. O. **Ciências Forenses - Uma introdução às principais áreas da Criminalística Moderna**. [*S. l.*]: Campinas: Millennium, 2011. v. 1.

VERBER, J.; SMUTNY, Z. **Fast and robust equalization**. ACPI - UK: Academic Conferences and Publishing International Limited, 2015. 294-299 p.

WELLS, J. **Longman Pronunciation Dictionary**. [*S. l.*]: Pearson Longman, 2009. v. 3.

X-WAYS SOFTWARE TECHNOLOGY AG. **Computer Forensics, Investigations and Security**. 2023. Disponível em: https://www.x-ways.net/winhex/forensics.html. Acesso em: 20 mai. 2023.

X-WAYS SOFTWARE TECHNOLOGY AG. **X-Ways Forensics**: Integrated computer forensics software. 2023. Disponível em: https://www.x-ways.net/forensics/index-m.html. Acesso em: 20 mai. 2023.

XPLICO. **Xplico - About**. 2023. Disponível em: https://www.xplico.org/about. Acesso em: 20 mai. 2023.

YULIANI, V.; RIADI, I. Forensic analysis whatsapp mobile application on android-based smartphones using national institute of standard and technology (nist) framework. **International Journal of Cyber-Security and Digital Forensics**, v. 8, p. 223–231, 2019.