UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE RUSSAS

CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

ANDERSON OLIVEIRA PONTES

ANÁLISE DE MÉTODOS E FERRAMENTAS NA INVESTIGAÇÃO FORENSE DIGITAL EM DISPOSITIVOS MÓVEIS

RUSSAS

2025

ANDERSON OLIVEIRA PONTES

ANÁLISE DE MÉTODOS E FERRAMENTAS NA INVESTIGAÇÃO FORENSE DIGITAL EM DISPOSITIVOS MÓVEIS

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Orientador: Prof. Me. Pitágoras Graça Martins.

RUSSAS

2025

ANDERSON OLIVEIRA PONTES

ANÁLISE DE MÉTODOS E FERRAMENTAS NA INVESTIGAÇÃO FORENSE DIGITAL EM DISPOSITIVOS MÓVEIS

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Aprovado em 16/07/2025.

BANCA EXAMINADORA

_____

Prof. Me. Pitágoras Graça Martins, Presidente

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Reuber Gegis de Melo, Membro

Universidade Federal do Ceará (UFC)

_____

Glaydson De Farias Lima, Membro

Associação Nacional dos Peritos em Computação Forense (APECOF)

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)

P858a Pontes, Anderson Oliveira.

Análise de métodos e ferramentas na investigação forense digital em dispositivos móveis / Anderson Oliveira Pontes. – 2025.
54 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, , Russas, 2025.
Orientação: Prof. Me. Pitágoras Graça Martins.
1. Análise forense digital. 2. Dispositivos móveis. 3. Ferramentas Forenses. 4. Segurança da Informação. 5. LGPD. I. Título.

CDD

RESUMO

A análise forense digital em dispositivos móveis desempenha um papel fundamental na segurança da informação, especialmente devido ao aumento do uso de smartphones e tablets que armazenam dados sensíveis, como credenciais, mensagens e informações bancárias. Este trabalho tem como objetivo analisar os métodos e ferramentas utilizadas na investigação forense digital, com destaque para Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective. A pesquisa adota uma abordagem descritiva e qualitativa, com revisão bibliográfica e análise documental, avaliando desafios como a fragmentação do sistema Android, as barreiras de segurança do iOS e a constante evolução tecnológica. Os resultados destacam práticas eficientes para a coleta e preservação de evidências digitais, respeitando aspectos éticos e legais, como os definidos pela LGPD. Além disso, são propostas estratégias para superar limitações operacionais e tecnológicas, garantindo maior integridade e confiabilidade das provas. Embora as ferramentas atuais ofereçam recursos avançados, elas enfrentam dificuldades no acesso a dados criptografados e na análise de dispositivos recentes. Conclui-se que o aprimoramento contínuo de técnicas, ferramentas e metodologias é essencial para atender às demandas crescentes da área. Este estudo contribui para fortalecer as práticas forenses digitais, fornecendo insights teóricos e práticos que auxiliam profissionais na superação dos desafios impostos pelas crescentes ameaças cibernéticas e pela diversidade tecnológica.

Palavras-chave: análise forense digital; dispositivos móveis; ferramentas forenses; segurança da informação; LGPD.

ABSTRACT

Digital forensic analysis on mobile devices plays a crucial role in information security, especially given the increasing use of smartphones and tablets, which store sensitive data such as credentials, messages, and banking information. This study aims to analyze the methods and tools used in digital forensic investigations, focusing on Cellebrite UFED, Magnet AXIOM, and Oxygen Forensic Detective. The research adopts a descriptive and qualitative approach, including a literature review and document analysis, addressing challenges such as Android system fragmentation, iOS security barriers, and rapid technological evolution. The results highlight efficient practices for the collection and preservation of digital evidence, ensuring compliance with ethical and legal aspects, such as those defined by the LGPD. Furthermore, strategies are proposed to overcome operational and technological limitations, ensuring greater integrity and reliability of evidence. Although current tools offer advanced features, they face difficulties in accessing encrypted data and analyzing recently released devices. It is concluded that the continuous improvement of techniques, tools, and methodologies is essential to meet the increasing demands of the field. This study contributes to strengthening digital forensic practices, providing theoretical and practical insights to help professionals overcome the challenges posed by growing cyber threats and technological diversity.

Keywords: digital forensic analysis; mobile devices; forensic tools; information security; LGPD.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

Sumário

1 INTRODUÇÃO

1.1 Tema

A rápida popularização de dispositivos móveis, como smartphones e tablets, transformou profundamente a forma como as pessoas se comunicam, armazenam dados e acessam serviços digitais. Esses aparelhos, ao concentrarem informações sensíveis como registros de comunicação, dados financeiros, localização geográfica e credenciais de acesso, tornaram-se alvos frequentes em investigações criminais e corporativas. Paralelamente, o aumento da criminalidade digital e o uso desses dispositivos em práticas ilícitas ampliaram a demanda por análises forenses digitais eficientes.

Nesse contexto, a análise forense digital em dispositivos móveis desponta como uma área estratégica para a segurança da informação, pois permite recuperar, examinar e preservar dados digitais com valor probatório. Contudo, a constante evolução tecnológica, a diversidade de modelos e sistemas operacionais (em especial Android e iOS) e o avanço de mecanismos de segurança e criptografia impõem desafios significativos à atuação dos analistas forenses.

Além dos entraves técnicos, questões éticas e legais — sobretudo relacionadas à privacidade e ao tratamento de dados pessoais, reguladas por legislações como a LGPD — exigem atenção redobrada. Ferramentas como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective vêm sendo amplamente utilizadas, mas ainda enfrentam limitações operacionais, principalmente frente a dispositivos mais recentes ou altamente protegidos.

Diante dessa realidade, este estudo propõe uma análise crítica dos métodos e ferramentas forenses mais utilizados na investigação de dispositivos móveis, buscando identificar suas limitações e propor estratégias para otimizar o processo de coleta e análise de evidências digitais, em consonância com os princípios legais e éticos que regem essa atividade.

1.2 Problema

A análise forense digital em dispositivos móveis enfrenta desafios crescentes, impulsionados pela diversidade de sistemas operacionais, pela implementação de barreiras de segurança avançadas (como criptografia e autenticação biométrica) e pela constante evolução dos dispositivos e aplicativos. Além disso, a escassez de profissionais capacitados e a fragmentação de conhecimentos na literatura dificultam a adoção de práticas padronizadas e eficazes. Diante desse cenário, surge a seguinte questão de pesquisa que orienta este trabalho:

Como realizar a análise forense digital em dispositivos móveis de forma eficaz e ética, considerando a diversidade de plataformas, as barreiras de segurança tecnológica e as limitações das ferramentas forenses atualmente disponíveis?

1.3 Contextualização

> Os dispositivos móveis têm se consolidado como ferramentas essenciais para a sociedade moderna, sendo utilizados tanto em ambientes pessoais quanto corporativos. Eles carregam informações críticas, desde registros de comunicação até dados financeiros e arquivos confidenciais. Em paralelo, o crescimento do uso desses dispositivos vem acompanhado por uma alta na incidência de crimes cibernéticos. Por exemplo, em 2022, foram registrados 1.819.409 casos de estelionato no Brasil, representando um aumento de 326% em relação a 2018. Além disso, o número de tentativas de golpes por meios digitais cresceu 20% no segundo trimestre de 2022. (PORTAL DA SEGURANÇA, 2022).

Diante desse cenário, a análise forense digital em dispositivos móveis surge como um campo essencial para a investigação e resolução de incidentes, permitindo que especialistas recuperem e analisem informações armazenadas nesses aparelhos para auxiliar em processos judiciais ou em investigações internas.

No entanto, as técnicas atuais de análise forense digital ainda apresentam várias deficiências. Segundo Casey (2011) "muitos métodos forenses ainda dependem de processos manuais que exigem conhecimento especializado, tornando a investigação mais demorada e propensa a erros". Além disso, estudos indicam que "a ausência de ferramentas automatizadas eficientes pode comprometer a integridade da análise e dificultar a extração de dados cruciais" (MASTROIANNI, 2022).

Muitos métodos dependem de processos manuais e carecem de automação, o que pode levar a erros humanos e atrasos nas investigações. Além disso, a rápida evolução tecnológica e a diversificação de sistemas operacionais e aplicativos móveis apresentam desafios contínuos para os profissionais da área.

Este trabalho busca não apenas compreender as técnicas e melhores práticas atuais, mas também identificar lacunas e áreas para melhorias, contribuindo assim para o avanço da análise forense digital em dispositivos móveis.

1.4 Delimitação do tema

Este trabalho delimita-se ao estudo da análise forense digital aplicada exclusivamente a dispositivos móveis, com enfoque nos sistemas operacionais Android e iOS. A escolha

desses dois sistemas se justifica pela sua predominância global, representando praticamente a totalidade do mercado de smartphones. Segundo a Statista (2024) “Em 2024, o Android lidera com uma participação de 72,15%, enquanto o iOS detém 27,19% do mercado mundial”, outras plataformas, como KaiOS e Windows Mobile, foram excluídas por não apresentarem relevância significativa no contexto global de smartphones.

Tais sistemas também apresentam desafios técnicos únicos na análise forense digital, como criptografia avançada e diferentes implementações de segurança. Portanto, investigar esses dois sistemas permitirá uma compreensão abrangente das técnicas forenses mais relevantes, oferecendo soluções aplicáveis à maioria dos casos encontrados na prática profissional. Este estudo foca exclusivamente na análise forense de dispositivos móveis com sistemas operacionais Android e iOS, os mais representativos do mercado atual.

1.5 Hipóteses

Este estudo parte das seguintes hipóteses:

a) A análise forense digital em dispositivos móveis é limitada por barreiras técnicas como criptografia avançada, fragmentação de sistemas operacionais e restrições de acesso a dados protegidos.

b) Técnicas de extração física e análise de dados em nuvem, aplicadas com ferramentas especializadas como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective, são atualmente as mais eficazes para a recuperação de evidências digitais em dispositivos móveis.

c) A conformidade com a legislação vigente (como a LGPD) e o uso de protocolos éticos são indispensáveis para garantir a legalidade, a integridade e a confidencialidade na análise forense digital.

1.6 Justificativa

A análise forense digital em dispositivos móveis representa um dos maiores desafios contemporâneos no campo da segurança da informação. Diante da crescente sofisticação dos crimes cibernéticos e da massiva utilização de smartphones no cotidiano pessoal e profissional, torna-se essencial compreender as técnicas, ferramentas e boas práticas que viabilizam a recuperação segura e legal de evidências digitais.

A relevância do tema também se evidencia no contexto brasileiro, onde a legislação sobre proteção de dados (como a LGPD) impõe exigências rigorosas quanto à integridade, privacidade e confidencialidade na manipulação de informações pessoais. Nesse cenário, profissionais da área precisam dominar não apenas os aspectos técnicos, mas também os fundamentos éticos e legais que orientam a atuação pericial.

Este trabalho justifica-se por sua contribuição prática e teórica. De um lado, busca sistematizar conhecimentos sobre ferramentas amplamente utilizadas (Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective), analisando suas capacidades e limitações. De outro, pretende propor estratégias para aprimorar o processo investigativo digital, enfrentando os desafios impostos pelas novas barreiras tecnológicas e exigências legais.

Além disso, a escolha deste tema está fortemente ligada à minha trajetória acadêmica e ao interesse profissional em atuar na área de perícia forense digital. Por meio deste estudo, busco aprofundar minha compreensão sobre os principais métodos aplicados no campo e contribuir para o desenvolvimento de práticas mais eficazes, éticas e alinhadas à legislação vigente.

1.7 Objetivos

1.7.1 Objetivo geral

Analisar criticamente os métodos e ferramentas aplicados à análise forense digital em dispositivos móveis, com foco na identificação de limitações técnicas e legais, e na proposição de estratégias que otimizem a recuperação de evidências digitais de forma ética e eficaz.

1.7.2 Objetivos específicos

a) Mapear e comparar as principais ferramentas forenses utilizadas na extração de dados de dispositivos móveis (Cellebrite UFED, Magnet AXIOM, Oxygen Forensic Detective).
b) Analisar os principais desafios técnicos impostos pelos sistemas operacionais Android e iOS no contexto da análise forense digital.
c) Investigar as práticas recomendadas para a coleta, preservação e documentação de evidências digitais, em conformidade com os princípios éticos e com a LGPD.

d) Elaborar propostas de melhoria para superar limitações operacionais e legais enfrentadas no uso das ferramentas analisadas.

2 REFERENCIAL TEÓRICO

O avanço da tecnologia e a crescente digitalização das interações humanas tornam a análise forense digital um campo essencial para a segurança da informação e a investigação criminal. Em especial, dispositivos móveis desempenham um papel central na coleta de evidências, pois armazenam uma grande quantidade de dados pessoais e corporativos.

Para embasar este estudo, foi realizada uma ampla revisão bibliográfica sobre análise forense digital, com foco em dispositivos móveis, abordando os conceitos fundamentais da análise forense digital, as ferramentas disponíveis, os desafios técnicos e as questões éticas e legais envolvidas no processo investigativo. Tal revisão inclui pesquisas recentes e clássicas, proporcionando um panorama atualizado sobre as melhores práticas e limitações na recuperação e preservação de evidências digitais em dispositivos móveis.

Foram consultados livros, artigos acadêmicos e relatórios técnicos publicados entre 2010 e 2024, priorizando materiais recentes devido à rápida evolução tecnológica da área. Bases de dados como IEEE Xplore, ScienceDirect e Google Scholar foram as principais fontes de pesquisa. Essa revisão teve como objetivo identificar:

- Os principais conceitos e fundamentos da análise forense digital;
- As ferramentas mais utilizadas no mercado;
- Os desafios impostos pelos sistemas operacionais Android e iOS.

Também foram analisadas as principais ferramentas de análise forense digital disponíveis no mercado, como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective. Essa análise foi realizada com base em documentação técnica, tutoriais e casos de uso publicados por fabricantes ou especialistas da área. Os critérios utilizados para avaliação das ferramentas incluíram:

- Capacidade de extração de dados (física e lógica);
- Compatibilidade com diferentes versões de Android e iOS;
- Limitações técnicas, como restrições de acesso a dados criptografados.

Por fim, com base nas informações coletadas, foram levantados os principais desafios enfrentados por analistas forenses, como a fragmentação do sistema Android e as barreiras de segurança do iOS. Paralelamente, foram identificadas boas práticas para a coleta e preservação de evidências digitais, como o uso de sacos de Faraday e a criação de imagens forense.

2.1 Análise forense digital: conceitos e evolução

A análise forense digital é uma ciência interdisciplinar que combina conhecimentos de tecnologia da informação, direito e investigação criminal para recuperar, analisar e apresentar dados digitais de forma que possam ser utilizados como evidências em processos judiciais ou investigações internas. Segundo Casey (2011) "a análise forense digital envolve a identificação, preservação, extração, documentação e interpretação de dados digitais com o objetivo de apoiar investigações legais e administrativas".

Ela surgiu como uma resposta à necessidade de investigar crimes envolvendo dispositivos eletrônicos, inicialmente focada em computadores e redes. Com a explosão do uso de dispositivos móveis, seu escopo se expandiu, tornando-se uma área indispensável na investigação de crimes cibernéticos.

De acordo com Pollitt (1995) “a análise forense digital segue princípios básicos que garantem a integridade das evidências: a preservação do estado original dos dados, a documentação precisa de todas as etapas e a validação das técnicas utilizadas". No contexto dos dispositivos móveis, esses princípios são desafiados pela volatilidade dos dados, pela diversidade de sistemas operacionais e pelas constantes atualizações tecnológicas.

2.2 Dispositivos móveis no cenário atual: o papel central na sociedade e nos crimes digitais

O uso de dispositivos móveis transformou a maneira como interagimos e armazenamos informações, tornando-os alvos preferenciais para atividades ilícitas, como fraudes financeiras, espionagem industrial e crimes cibernéticos. Segundo o relatório de segurança da Kaspersky (2023) "os ataques a dispositivos móveis cresceram cerca de 40% nos últimos cinco anos, com métodos sofisticados que variam de malware até phishing direcionado".

Essa nova realidade coloca os dispositivos móveis no centro das investigações digitais, pois eles contêm informações valiosas, como históricos de chamadas, mensagens de texto, dados de localização e registros de aplicativos financeiros. Além disso, a integração com serviços em nuvem amplia o volume e a complexidade dos dados a serem analisados, criando um novo campo de estudo dentro da análise forense digital. Segundo Schaefer et al. (2022) “a crescente dependência de dispositivos móveis para armazenar e processar informações

sensíveis reforça sua relevância nas investigações forenses, exigindo novas abordagens e ferramentas para análise de dados distribuídos em múltiplas plataformas".

2.3 Sistemas operacionais: Android e iOS em foco

A análise forense em dispositivos móveis é altamente dependente do sistema operacional utilizado, uma vez que cada plataforma possui características únicas que influenciam diretamente a recuperação de dados:

***Android*:** amplamente adotado, o Android é um sistema de código aberto, mas sua fragmentação apresenta desafios. Diferentes fabricantes aplicam customizações que impactam o acesso aos dados. O'Shoughnessy e Sappenfield (2018) afirmam que "a aplicação de criptografia padrão, implementada desde o Android 6.0, e a introdução do Secure Boot tornaram a extração forense significativamente mais difícil, exigindo novas abordagens para obtenção de dados".

***iOS*:** embora menos fragmentado, o iOS apresenta desafios significativos devido à forte implementação de medidas de segurança, como Secure Enclave e Data Protection API. Al-Khasawneh et al. (2021) destacam que "a criptografia no iOS é ativada por padrão, e a sincronização automática de dados com o iCloud impõe obstáculos adicionais para a recuperação de informações sem comprometer sua integridade".

Ambos os sistemas operacionais impõem restrições legais e técnicas que desafiam os investigadores forenses a encontrar soluções criativas e éticas para acessar dados protegidos.

2.4 Ferramentas e métodos de análise forense digital

As ferramentas utilizadas na análise forense digital de dispositivos móveis são diversas e constantemente evoluem para acompanhar as inovações tecnológicas e as novas ameaças cibernéticas. Algumas das mais reconhecidas incluem:

***Cellebrite UFED*:** considerada uma das líderes do mercado, oferece soluções para extração física e lógica de dispositivos móveis, mesmo em situações onde há bloqueios complexos;

***Oxygen Forensic Detective*:** permite análise detalhada de aplicativos de redes sociais, dados de localização e registros de chamadas;

***Magnet AXIOM*:** especializada em análises avançadas, incluindo recuperação de arquivos deletados e dados criptografados.

Apesar das capacidades dessas ferramentas, há limitações significativas, como a incapacidade de acessar dados protegidos por criptografia avançada sem a colaboração do proprietário do dispositivo ou de obter informações hospedadas exclusivamente na nuvem.

2.5 Técnicas de coleta e preservação de evidências

A coleta de evidências em dispositivos móveis requer procedimentos que garantam a preservação da integridade dos dados, incluindo a criação de imagens forenses do dispositivo para análise posterior. Técnicas de bloqueio de comunicação, como o uso de sacos de Faraday, evitam que os dispositivos sejam acessados remotamente durante o processo de coleta, impedindo a destruição de dados. Segundo KRUSE; HEISER "O isolamento do dispositivo por meio de técnicas como sacos de Faraday é uma prática essencial para evitar alterações nos dados armazenados, garantindo que as evidências digitais permaneçam intactas durante a investigação forense." (KRUSE; HEISER, 2002).

2.5.1 Cadeia de Custódia na Investigação Forense Digital

A cadeia de custódia é um elemento jurídico essencial na análise forense digital, sendo regulamentada no Brasil pelos artigos 158-A a 158-F do Código de Processo Penal, incluídos pela Lei nº 13.964/2019 (Pacote Anticrime). Ela se refere ao conjunto de procedimentos que asseguram a integridade, autenticidade e rastreabilidade das evidências coletadas desde a sua origem até sua apresentação em juízo. No contexto da análise forense em dispositivos móveis, respeitar a cadeia de custódia significa documentar cuidadosamente cada etapa da manipulação do dispositivo: desde a apreensão, passando pela extração de dados com ferramentas como Cellebrite UFED, Magnet AXIOM ou Oxygen Forensic Detective, até o armazenamento e análise das evidências.

A ausência ou falha na documentação da cadeia pode acarretar na nulidade da prova digital, mesmo que o conteúdo seja relevante. Por isso, os profissionais forenses devem seguir protocolos estritos, utilizando técnicas reconhecidas e documentando todo o processo com datas, horários, responsáveis e ferramentas empregadas. A correta observância da cadeia de custódia reforça a credibilidade da prova digital, garantindo que ela não foi alterada, substituída ou contaminada, o que é especialmente relevante em processos judiciais onde a prova digital pode ser decisiva.

2.6 Aspectos éticos e legais: desafios na proteção da privacidade

A análise forense digital em dispositivos móveis está sujeita a regulamentações que visam proteger a privacidade dos usuários. A Lei Geral de Proteção de Dados (LGPD) no Brasil estabelece diretrizes rigorosas sobre o acesso e o tratamento de dados pessoais, impondo desafios adicionais para as investigações forenses. Segundo SILVA, "Qualquer violação das normas de privacidade pode resultar em implicações legais severas, afetando tanto os investigadores quanto as instituições envolvidas no processo de coleta e análise de evidências digitais." (SILVA 2021).

Além disso, a questão ética de proteger os dados de indivíduos inocentes é um tópico frequentemente debatido, principalmente quando a análise envolve dispositivos compartilhados ou usados para fins profissionais e pessoais.

2.7 A Lei Geral de Proteção de Dados Pessoais (LGPD) e a análise forense

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi criada com o objetivo de regular o tratamento de dados pessoais no Brasil, estabelecendo direitos aos titulares dos dados e responsabilidades para aqueles que os utilizam. Na análise forense digital, especialmente em dispositivos móveis, é essencial observar os princípios e requisitos impostos pela LGPD, a fim de garantir a legalidade e a ética do processo investigativo.

2.7.1 Autorização legal

A LGPD exige que o tratamento de dados pessoais, incluindo coleta, armazenamento e análise, seja realizado com base em fundamentos legais claros. Para a análise forense em dispositivos móveis, é necessário obter uma autorização prévia, como uma ordem judicial ou o consentimento do titular dos dados, salvo exceções previstas em lei.

Conforme o Art. 7º da LGPD, o tratamento de dados é permitido para o cumprimento de obrigação legal ou regulatória ou quando necessário para a execução de uma investigação criminal ou judicial. Dessa forma, é imprescindível que a autorização para acesso aos dados esteja documentada, garantindo a legalidade da análise.

2.7.2 Preservação da integridade das evidências

Durante a coleta e análise de dados em dispositivos móveis, é fundamental preservar a integridade das evidências digitais. Qualquer alteração nos dados pode comprometer a validade do processo investigativo. Para isso, é necessário utilizar ferramentas certificadas e técnicas forenses adequadas, como hashes criptográficos, para assegurar que os dados analisados permaneçam inalterados.

Conforme recomendado por Casey (2011) "a integridade das evidências digitais deve ser mantida desde o momento de sua coleta até sua apresentação em tribunal". Tal princípio é reforçado pela LGPD, que estabelece em seu Art. 6º os princípios da segurança e prevenção como pilares do tratamento de dados.

2.7.3 Documentação detalhada

A documentação detalhada é um aspecto essencial do processo forense. Todas as etapas da investigação devem ser registradas de forma minuciosa, incluindo:

- Data e hora da coleta dos dados;
- Ferramentas utilizadas;
- Procedimentos adotados;
- Resultados obtidos.

Essa documentação não apenas garante a transparência do processo, mas também assegura conformidade com o princípio da responsabilidade, previsto no Art. 6º, inciso X, da LGPD.

2.7.4 Respeito à privacidade

A LGPD estabelece a proteção da privacidade como um de seus fundamentos (Art. 2º). Na análise forense, é essencial minimizar a exposição de dados não relevantes para a investigação. Deve-se garantir que apenas informações diretamente relacionadas às questões investigadas sejam acessadas e analisadas.

2.7.5 Confidencialidade

A confidencialidade das informações deve ser mantida durante todo o processo investigativo. Isso inclui a proteção dos dados contra acessos não autorizados e a adoção de medidas como criptografia e controle de acesso. O Art. 46 da LGPD prevê que os agentes de tratamento adotem medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais. Assim, a segurança da informação deve ser uma prioridade.

2.7.6 Conformidade com regulamentações

O cumprimento das regulamentações é essencial para garantir a validade legal e ética da análise forense. Além da LGPD, devem ser observadas outras leis e normas aplicáveis, como:

- O Marco Civil da Internet (Lei nº 12.965/2014);
- O Código Penal Brasileiro (Decreto-Lei nº 2.848/1940);
- Normas internacionais, como a ISO/IEC 27037, que orienta a coleta e preservação de evidências digitais.

2.7.7 Cuidados éticos e legais

Durante a análise forense em dispositivos móveis, os seguintes cuidados éticos e legais devem ser observados:

- ***Consentimento informado*:** sempre que possível, obter o consentimento do titular dos dados;
- ***Minimização de dados*:** tratar apenas os dados estritamente necessários para a investigação;
- ***Imparcialidade*:** realizar a análise de forma objetiva, sem manipular resultados;
- ***Treinamento*:** garantir que os profissionais envolvidos sejam qualificados e capacitados para lidar com dados pessoais de maneira ética e segura.

A LGPD trouxe avanços significativos para a proteção de dados pessoais no Brasil, impondo diretrizes que devem ser rigorosamente seguidas durante a análise forense em dispositivos móveis. A observação de cuidados legais e éticos não apenas garante a validade das investigações, mas também contribui para a proteção dos direitos dos indivíduos, promovendo um equilíbrio entre a segurança e a privacidade.

3 TRABALHOS RELACIONADOS

Neste capítulo, serão apresentados estudos que analisam a aplicação da análise forense digital em dispositivos móveis, abordando casos práticos e desafios enfrentados na extração e recuperação de dados. Os trabalhos relacionados foram encontrados em bases acadêmicas como ScienceDirect, Forensic Science International e Journal of Digital Forensics, além de características técnicas de ferramentas forenses amplamente utilizadas no mercado, como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective. Para um melhor entendimento, os estudos analisados foram organizados em três tópicos principais:

- ***Investigação de fraudes financeiras em dispositivos Android*:** descreve um caso de fraude bancária em que a análise forense de um smartphone Android permitiu a extração de transações suspeitas;
- ***Recuperação de mensagens excluídas no iOS*:** aborda um caso de assédio virtual onde técnicas de análise forense digital foram aplicadas para recuperar comunicações deletadas de um iPhone;
- ***Análise forense de aplicativos de mensagens em investigações criminais*:** discute um caso de tráfico de drogas em que mensagens criptografadas de WhatsApp e Telegram foram extraídas e analisadas.

Cada seção explora um caso prático relevante, detalhando as metodologias aplicadas e as ferramentas utilizadas para a extração e análise de evidências digitais. Além disso, será realizada uma discussão sobre as limitações enfrentadas e as soluções propostas nesses estudos, relacionando-as com os desafios e contribuições da presente pesquisa.

3.1 Descrição do caso 1: investigação de fraudes financeiras em dispositivos Android

Al-Khasawneh et al. (2021) analisaram um caso de fraude bancária envolvendo um dispositivo Android utilizado para realizar transações financeiras suspeitas. O proprietário do smartphone negava envolvimento, alegando que sua conta havia sido acessada indevidamente.

A investigação teve como objetivo recuperar registros de acesso, identificar aplicativos suspeitos e verificar a existência de malware que pudesse ter comprometido a segurança da conta. Os investigadores utilizaram um método baseado na extração lógica e física do dispositivo. A extração lógica foi aplicada para obter acesso a dados do usuário sem comprometer o sistema, enquanto a extração física foi necessária para recuperar informações deletadas e setores ocultos do armazenamento interno:

***Extração lógica*:** Utilização de técnicas de desbloqueio do smartphone para acessar registros de navegação, aplicativos bancários e logs do sistema;

***Extração física*:** Recuperação de setores inteiros do armazenamento usando ferramentas avançadas para analisar vestígios de atividades suspeitas.

O Magnet AXIOM foi a principal ferramenta utilizada para análise forense neste caso. Ele é uma solução de ponta desenvolvida para examinar dispositivos móveis, computadores e serviços em nuvem. Suas principais funcionalidades incluem:

- Recuperação de arquivos apagados de sistemas de armazenamento;
- Análise detalhada do histórico de navegação, chamadas e mensagens;
- Extração de dados criptografados de aplicativos financeiros e redes sociais.

A ferramenta permitiu aos investigadores reconstruírem a linha do tempo das transações financeiras e identificar um malware que estava interceptando credenciais bancárias. A partir dessa descoberta, foi possível relacionar as atividades fraudulentas a um grupo criminoso que utilizava técnicas de keylogging e phishing para roubar informações bancárias.

3.2 Descrição do caso 2: recuperação de mensagens excluídas no iOS

Schaefer et al. (2022) documentaram uma investigação em que um iPhone foi apreendido em um caso de assédio virtual. A vítima recebeu mensagens ameaçadoras e, após a denúncia, o suspeito tentou deletar as conversas para ocultar as evidências. A análise forense foi realizada para recuperar essas mensagens e estabelecer uma conexão entre o dispositivo do suspeito e os envios das ameaças.

O método aplicado foi baseado em três etapas principais. A primeira foi a criação de uma imagem forense do iPhone: A cópia bit a bit do dispositivo foi gerada para evitar modificações nos dados originais, depois foi feita a extração de backups no iCloud, como as mensagens excluídas que podem permanecer armazenadas em backups automáticos, a análise dos arquivos do iCloud foram essenciais para o sucesso da perícia e por último foi realizada a recuperação de arquivos deletados. Técnicas especializadas foram utilizadas para restaurar dados apagados do banco de dados SQLite do iOS.

A ferramenta utilizada foi a Cellebrite UFED, uma das ferramentas forenses mais avançadas para análise de dispositivos móveis. Suas principais capacidades incluem:

- Desbloqueio e extração de dados de iPhones protegidos por senha;

- Análise de backups do iCloud para recuperar dados apagados;
- Extração de mensagens, registros de chamadas, dados de GPS e histórico de navegação.

A partir da análise realizada com o Cellebrite UFED, os investigadores conseguiram restaurar mensagens excluídas no iMessage, além de metadados que indicavam o horário exato das ameaças. Isso foi suficiente para implicar o suspeito e reforçar as acusações no processo judicial.

3.3 Descrição do caso 3: análise forense de aplicativos de mensagens em investigações criminais

Mastroianni (2022), analisou um caso de tráfico de drogas em que os suspeitos utilizavam WhatsApp e Telegram para se comunicar e coordenar as operações ilícitas. A investigação teve como objetivo recuperar conversas, identificar membros do grupo criminoso e extrair registros de geolocalização associados às mensagens.

O método aplicado na análise incluía a extração lógica de mensagens do banco de dados SQLite do WhatsApp, a recuperação de metadados de conversas no Telegram armazenadas em cache e análise de imagens e documentos trocados nos aplicativos para obter pistas adicionais. A ferramenta utilizada nesse caso foi a Oxygen Forensic Detective, que se destacou na investigação por oferecer funcionalidades especializadas para análise de aplicativos de mensagens como:

- Descriptografia de conversas armazenadas no WhatsApp e Telegram;
- Extração de tokens de autenticação para acessar mensagens remotamente;
- Recuperação de mídias trocadas em conversas criptografadas.

A investigação revelou mensagens comprometedoras que detalhavam transações de drogas e forneciam informações cruciais sobre a logística do grupo criminoso.

3.4 Discussão: semelhanças e diferenças entre os trabalhos relacionados

Com base nas observações feitas nos estudos apresentados, é possível identificar tanto as semelhanças quanto as particularidades de cada pesquisa e como elas contribuem para a análise forense digital em dispositivos móveis. Cada estudo de caso abordou um contexto

específico de investigação, utilizando diferentes ferramentas e metodologias para extrair e analisar evidências digitais.

Entre as principais semelhanças, destacam-se o uso de ferramentas especializadas para extração e análise de dados, pois ambos os estudos utilizaram softwares forenses amplamente reconhecidos, demonstrando a importância dessas ferramentas na investigação. A recuperação de dados deletados nos três casos apresentaram cenários em que os investigados tentaram apagar informações para ocultar atividades ilícitas.

Isso reforça a relevância da análise forense para restaurar e interpretar registros apagados e abordagem baseada em extração lógica e física visto que em todos os estudos, as análises começaram pela extração lógica de dados, como backup do iCloud ou histórico de aplicativos, seguida pela extração física nos casos em que era necessário recuperar informações mais profundas ou ocultas. Por outro lado, também foram identificadas diferenças significativas, conforme destacado abaixo:

Quadro 1 - Comparativo das principais características dos trabalhos relacionados

CRITÉRIO	**CASO 1 fraudes financeiras (Android)**	**CASO 2 recuperação de mensagens (iOS)**	**CASO 3 análise de mensagens criptografadas**
Objetivo principal	Identificar malware e transações suspeitas	Recuperar mensagens apagadas para investigação de assédio	Extrair mensagens criptografadas de redes criminosas.
Sistema operacional analisado	Android	IOS	Android e iOS
Ferramenta principal utilizada	Magnet AXIOM	Cellebrite UFED	Oxygen Forensic Detective
Método de extração	Extração lógica e física	Extração de backups do iCloud e base de dados SQLite	Extração de tokens de autenticação e descriptografia
	Criptografia do	Proteção de backup	Mensagens

Dificuldades encontradas	Secure Folder e proteção do Android 6.0+	no iCloud e autenticação biométrica	criptografadas e resistência a recuperação de dados

Fonte: elaborada pelo autor, 2025.

A partir dessa análise, percebe-se que, apesar das semelhanças na abordagem metodológica, cada caso exigiu estratégias específicas devido às características do sistema operacional e do tipo de dados analisados. No caso das fraudes financeiras, foi necessária uma análise profunda da memória do dispositivo para identificar malwares e suas atividades. Já na recuperação de mensagens no iOS, a extração de backups na nuvem foi essencial. Por fim, a análise de aplicativos de mensagens criptografadas exigiu técnicas avançadas para contornar a proteção dos dados.

Dessa forma, os estudos apresentados reforçam a importância de uma abordagem flexível na análise forense digital em dispositivos móveis, considerando os desafios impostos por cada plataforma e pelo tipo de evidência investigada.

4 DETALHANDO CADA FERRAMENTA

A análise forense digital em dispositivos móveis tem se tornado uma parte fundamental na investigação de crimes cibernéticos e na recuperação de provas digitais. Para realizar uma investigação eficaz, é necessário o uso de ferramentas especializadas que possibilitem a coleta, análise e preservação de dados de dispositivos móveis, sem comprometer a integridade das informações. Entre as ferramentas mais destacadas no cenário forense digital estão o Magnet AXIOM, o Cellebrite UFED e o Oxygen Forensic Detective.

Cada uma dessas soluções oferece recursos únicos que atendem às diversas demandas de investigação, desde a extração de dados até a análise aprofundada de informações criptografadas e ocultas. Este tópico aborda as características, funcionalidades e vantagens de cada uma dessas ferramentas, além de comparar suas capacidades no contexto da análise forense em dispositivos móveis.

4.1 Introdução sobre a Cellebrite

Figura 1 - Logotipo Cellebrite

Fonte: LIBLOGO, 2025.

A Cellebrite é uma empresa israelense fundada em 1999, especializada em tecnologias de extração, decodificação e análise de dados digitais para aplicações forenses. Sua principal área de atuação é a investigação criminal e forense digital, sendo amplamente utilizada por forças policiais, agências governamentais e empresas privadas ao redor do mundo.

A empresa fornece soluções que permitem recuperar informações de dispositivos móveis, incluindo mensagens, registros de chamadas, arquivos de mídia, dados de aplicativos e informações apagadas.

4.1.1 Soluções propostas pela Cellebrite

A Cellebrite tem uma gama de produtos voltados para a investigação digital, sendo o Cellebrite UFED (Universal Forensic Extraction Device) um dos mais conhecidos. Ele se destaca em relação a outras ferramentas similares, como a GrayKey e a Oxygen Forensics, devido à sua ampla compatibilidade com dispositivos móveis e à capacidade de realizar extrações tanto físicas quanto lógicas.

Sua popularidade decorre do suporte contínuo a novos modelos de smartphones e da capacidade de acessar dados que outras soluções forenses podem não conseguir extrair. Suas soluções incluem:

- UFED Touch / UFED 4PC: ferramentas para extração de dados de dispositivos móveis;
- UFED Cloud Analyzer: análise de dados armazenados na nuvem;
- Cellebrite Pathfinder: ferramenta para análise e visualização de dados extraídos;
- UFED Premium: solução avançada para desbloqueio e extração de dispositivos de alta segurança.

4.1.2 Análise detalhada do Cellebrite UFED

4.1.2.1 Extração de dados

O Cellebrite UFED pode realizar diferentes tipos de extração, sendo compatível com uma ampla gama de dispositivos, incluindo modelos da Apple (iPhone 6 ao iPhone 14), Samsung (Galaxy S8 ao S23), Google Pixel, Motorola e alguns dispositivos chineses como Xiaomi e Huawei.

***Física*:** a extração física cria uma cópia bit a bit da memória do dispositivo, capturando todos os dados, incluindo os excluídos e áreas não visíveis ao usuário. Isso oferece uma investigação mais profunda, ao contrário da extração lógica, que só coleta dados acessíveis ao usuário;

***Lógica*:** a extração lógica coleta apenas os dados acessíveis ao usuário, como arquivos, mensagens, registros de chamadas e aplicativos instalados. Esse processo é mais rápido e menos invasivo que a extração física, mas não captura dados excluídos ou áreas não visíveis da memória, oferecendo um nível de investigação mais superficial;

***Arquivo de backup*:** a extração por arquivo de backup consiste em recuperar dados a partir de backups feitos pelo dispositivo, como aqueles armazenados em serviços na nuvem

(iCloud, Google Drive) ou backups locais. Esse método permite acessar dados como fotos, mensagens e configurações, mas depende da existência de um backup recente e não captura dados que não foram incluídos nesse backup;

***Extração por nuvem*:** a extração por nuvem envolve recuperar dados armazenados em serviços de nuvem, como iCloud, Google Drive ou outros, sem precisar do dispositivo físico. Esse método permite acessar informações como fotos, mensagens e documentos, desde que o usuário tenha feito o backup. No entanto, ele depende do acesso à conta do usuário e não captura dados que não foram sincronizados com a nuvem;

***Peculiaridade*:** em dispositivos iOS, a ferramenta pode acessar backups criptografados desde que a senha seja conhecida ou obtida por engenharia reversa. Vale destacar, que ao realizar esse tipo de abordagem, é importante considerar as implicações legais e éticas, pois a engenharia reversa em sistemas de criptografia pode violar leis de privacidade e proteção de dados.

4.1.2.2 Decodificação de dados

Após a extração, o Cellebrite UFED permite decodificar:

- Mensagens de texto e chamadas;
- Mídia (fotos, vídeos, áudios);
- Dados de aplicativos como WhatsApp, Telegram, Signal;
- Metadados de arquivos.

4.1.2.3 Bypass de senhas e criptografia

O Cellebrite UFED Premium é capaz de contornar bloqueios em certos modelos de smartphones. No entanto, dispositivos modernos têm camadas avançadas de segurança, tornando a extração mais difícil.

4.1.3 Falhas e possíveis melhorias

Apesar da robustez do Cellebrite UFED, existem desafios e pontos de melhoria. Por exemplo, um estudo conduzido pelo National Institute of Standards and Technology (NIST) demonstrou que a ferramenta possui dificuldades na extração completa de dados de dispositivos com criptografia avançada. Além disso, casos judiciais, como o caso envolvendo a extração de dados do iPhone de um suspeito em 2021, evidenciaram que a Cellebrite enfrenta obstáculos para acessar conteúdos protegidos por criptografia de ponta a ponta, limitando sua eficácia em determinados cenários.

4.1.4 Limitações na quebra de senhas

- Problema: Nem todos os dispositivos podem ser desbloqueados;
- Melhoria: Investimento em técnicas de engenharia reversa e exploração de vulnerabilidades de firmware.

4.1.5 Suporte a dispositivos novos

- Problema: Modelos recentes de smartphones são mais protegidos;
- Melhoria: Parcerias com fabricantes para otimizar processos de análise.

4.1.6 Decodificação de apps criptografados

- Problema: Apps como Signal dificultam a extração de mensagens;
- Melhoria: Desenvolvimento de inteligência artificial (IA) para análise preditiva e interseção de dados armazenados temporariamente.

4.1.7 Extração de dados em tempo real

- Problema: Algumas operações demoram e não permitem acesso dinâmico aos dados;
- Melhoria: Implementação de ferramentas para captura em tempo real.

O Cellebrite UFED é uma ferramenta poderosa para investigação forense, possibilitando extração e análise de dados de dispositivos móveis. No entanto, ainda enfrenta

desafios como dispositivos altamente criptografados e novas formas de armazenamento seguro. Melhorias futuras podem incluir IA para previsão de senhas, novos métodos de engenharia reversa e suporte mais avançado a dispositivos modernos.

4.2 Introdução à Magnet Forensics

Figura 2 - Logotipo Magnet Forensics

Fonte: MAGNET FORENSICS, 2019.

A Magnet Forensics é uma empresa canadense fundada por Jad Saliba, um ex-investigador de crimes digitais. A empresa se especializa em ferramentas de investigação forense digital, ajudando polícias, instituições governamentais e empresas privadas a recuperar e analisar evidências digitais.

4.2.1 Soluções propostas pelo Magnet AXIOM

O Magnet AXIOM é uma das principais ferramentas da empresa, focada na análise forense digital. Ele oferece soluções para:

***Extração de dados*:** permite a coleta de dados de dispositivos móveis, computadores e armazenamentos em nuvem. O AXIOM pode acessar informações armazenadas na memória do dispositivo, bem como dados criptografados, dependendo do nível de acesso e permissão. Ele suporta a extração lógica, física e em nuvem, o que possibilita uma abordagem abrangente na coleta de evidências;

***Recuperação de arquivos apagados*:** identifica e restaura arquivos deletados, incluindo mensagens, imagens e históricos de navegação. Ele utiliza técnicas avançadas de análise de clusters e fragmentação de dados, permitindo a recuperação de arquivos que não

foram sobrescritos pelo sistema. Além disso, consegue extrair evidências de aplicativos de mensagens como WhatsApp, Telegram e Facebook Messenger;

***Análise de dados estruturada*:** fornece ferramentas para organização e correlação de evidências digitais. O AXIOM apresenta visualizações interativas, permitindo que os investigadores identifiquem rapidamente padrões e conexões entre eventos e usuários. Ele também oferece recursos como linha do tempo, mapeamento geográfico e análise de rede, auxiliando na reconstrução de eventos;

***Geração de relatórios*:** exporta evidências de forma organizada e legível para processos judiciais. Os relatórios gerados podem ser personalizados e exportados em diversos formatos, como PDF, CSV e HTML. Além disso, permitem a inclusão de capturas de tela e anotações, tornando a apresentação das evidências mais clara para tribunais e equipes de investigação.

4.2.2 Pontos fortes e melhorias necessárias

4.2.2.1 Pontos fortes

- Interface intuitiva e de fácil navegação;
- Suporte a uma ampla gama de dispositivos e sistemas;
- Recuperação eficaz de arquivos deletados;
- Integração com outras ferramentas forenses.

4.2.2.2 Possíveis melhorias e como implementá-las

A seguir segue uma tabela expondo as limitações, sugestões de melhoria e como implementá-las:

Quadro 2 - Falhas e limitações, sugestões de melhorias e implementação

FALHA/LIMITAÇÃO	SUGESTÃO DE	IMPLEMENTAÇÃO

	MELHORIA	
Tempo de processamento alto	Melhorar algoritmos de indexação	Implementar IA para filtrar dados irrelevantes antes da análise
Suporte Limitado a alguns Apps	Atualização contínua do banco de dados	Criar um sistema de atualização modular com plugins
Falta de integração avançada com Cloud	Melhor sincronização com serviços na nuvem	Adicionar suporte nativo para APIs de grandes provedores (Google, Apple, etc.)

Fonte: Fonte: elaborada pelo autor, 2025.

O Magnet AXIOM é uma ferramenta essencial para investigações forenses digitais, oferecendo funcionalidades robustas para extração, análise e geração de relatórios. Apesar de suas forças, algumas melhorias poderiam torná-lo ainda mais eficiente.

4.3 Introdução à Oxygen Forensics

Figura 3 - Logotipo Oxygen Forensics

Fonte: FOURINC, 2025.

A Oxygen Forensics é uma empresa especializada no desenvolvimento de soluções forenses digitais para investigação criminal e segurança cibernética. Fundada em 2000, a empresa tem se destacado no mercado por oferecer ferramentas avançadas para a extração,

análise e investigação de dados provenientes de dispositivos móveis, serviços em nuvem, drones e dispositivos IoT.

A missão da Empresa é buscar e fornecer soluções de ponta para auxiliar profissionais de segurança pública e investigadores forenses a coletar evidências digitais de forma rápida e eficaz. A empresa investe constantemente em pesquisa e desenvolvimento para acompanhar as evoluções tecnológicas dos dispositivos móveis e dos sistemas operacionais.

4.3.1 Soluções oferecidas pelo Oxygen Forensic Detective

O Oxygen Forensic Detective é uma suíte forense digital que permite a extração e análise de dados de diversas fontes, incluindo:

4.3.1.1 Dispositivos móveis

- Extração de dados de dispositivos iOS e Android;
- Métodos de bypass para contornar bloqueios de tela e criptografia;
- Extração lógica, física e via backup de dados.

4.3.1.2 Aplicativos de mensagens e redes sociais

- Suporte para recuperação de mensagens de aplicativos como WhatsApp, Telegram, Facebook Messenger, Instagram, Signal, WeChat, entre outros;
- Decodificação e análise de bancos de dados SQLite;
- Extração de mensagens apagadas ou ocultas.

4.3.1.3 Serviços em nuvem

- Acesso a dados armazenados no Google Drive, iCloud, OneDrive, Facebook, Twitter, Dropbox e outros;
- Extração utilizando credenciais, tokens ou ataques de força bruta.

4.3.1.4 Análise de arquivos e metadados

- Recuperação de arquivos excluídos;
- Análise de imagens e vídeos;
- Extração de metadados de arquivos (localização, data de criação, modificações).

4.3.1.5 Reconstrução de cenários e linha do tempo

- Mapeamento de atividades e interações entre usuários;
- Criação de linha do tempo com eventos organizados cronologicamente;
- Visualização de conexões entre contatos, chamadas e movimentações geográficas.

4.3.1.6 Drones e dispositivos IoT

- Extração e análise de logs de drones DJI e Parrot;
- Investigação de dispositivos IoT para recuperação de dados sensíveis (assistentes virtuais, dispositivos de saúde ou dispositivos de segurança).

4.3.2 Possíveis falhas ou limitações

Apesar da sua robustez, o Oxygen Forensic Detective possui algumas limitações e desafios, incluindo:

4.3.3 Suporte a dispositivos recentes

O avanço contínuo da segurança em dispositivos móveis, como criptografia avançada e novos métodos de bloqueio, torna mais difícil a extração de dados de dispositivos recém-lançados. Sugestão de melhoria: investir em parcerias com fabricantes e em pesquisa para aprimorar métodos de desbloqueio sem necessidade de root ou jailbreak.

4.3.4 Análise de aplicativos criptografados

Aplicativos como Signal e Telegram usam criptografia de ponta a ponta, dificultando a recuperação de mensagens. Sugestão de melhoria: implementar técnicas de captura de memória volátil e engenharia reversa para analisar processos em execução.

4.3.5 Interface e usabilidade

Embora poderosa, a interface pode ser complexa para usuários iniciantes. Sugestão de melhoria: criar um modo "assistente" para guiar os usuários menos experientes durante as etapas da análise forense.

4.3.6 Tempo de processamento

Algumas análises podem ser demoradas, especialmente em dispositivos com grande volume de dados. Sugestão de melhoria: implementação de processamento em nuvem para acelerar a análise de dados massivos.

4.3.7 Curiosidades sobre o Oxygen Forensic Detective

A ferramenta é utilizada por agências de segurança em mais de 150 países. É capaz de recuperar dados de drones, sendo uma das poucas ferramentas do mercado com esse suporte. Suas técnicas avançadas permitem reconstruir conversas e atividades mesmo após exclusão dos dados.

A conclusão foi que a ferramenta Oxygen Forensic Detective é uma das mais poderosas para investigação digital. No entanto, como qualquer tecnologia, há espaço para melhorias. A adoção de técnicas avançadas de extração, otimização de processamento e aprimoramento da usabilidade pode torná-la ainda mais eficiente.

5 METODOLOGIA

Esta pesquisa possui uma natureza aplicada, pois busca contribuir com o entendimento e a prática da análise forense digital em dispositivos móveis. Seu objetivo não é apenas ampliar o conhecimento teórico sobre o tema, mas também fornecer subsídios para profissionais da área forense e da segurança da informação, identificando desafios, avaliando ferramentas e propondo melhorias nos processos investigativos.

A abordagem utilizada é descritiva, pois tem como foco a documentação e análise das técnicas, ferramentas e desafios enfrentados na análise forense digital de dispositivos móveis. A pesquisa descritiva permite uma investigação das características técnicas dos sistemas operacionais Android e iOS, bem como das ferramentas utilizadas para extração e análise de dados.

Os dados obtidos nesta pesquisa referem-se à análise das ferramentas forenses utilizadas no mercado, suas capacidades e limitações. Serão considerados aspectos como:

- Métodos de extração de dados (lógica e física);
- Barreiras de segurança impostas pelos sistemas Android e iOS;
- Eficiência das ferramentas no tratamento de dados criptografados;
- Desafios operacionais enfrentados na coleta e preservação das evidências digitais.

Os dados foram coletados por meio de pesquisa bibliográfica e análise documental. A pesquisa bibliográfica será realizada em bases de dados acadêmicas, como IEEE Xplore, ScienceDirect e Google Scholar, priorizando materiais publicados entre 2010 e 2024. Além disso, foram analisados manuais técnicos, relatórios de fabricantes de ferramentas forenses (como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective) e estudos de caso documentados na literatura especializada.

Este estudo não envolve coleta de dados de uma população específica por meio de experimentação direta. A amostra utilizada consiste na seleção de artigos científicos, livros, relatórios técnicos e manuais de ferramentas forenses. A escolha das fontes considerou a relevância e a atualidade dos materiais, priorizando aqueles que abordam metodologias forenses aplicáveis a dispositivos móveis. Para a análise qualitativa, serão seguidos os seguintes passos:

***Identificação e categorização das capacidades das ferramentas forenses*:** Será realizada uma análise detalhada das funcionalidades específicas de cada ferramenta, como

Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective, comparando suas abordagens para extração física e lógica de dados;

***Definição de critérios de comparação*:** As ferramentas serão avaliadas com base em critérios como compatibilidade com sistemas Android e iOS, eficiência na recuperação de dados criptografados, facilidade de uso e tempo de processamento. Esses critérios serão extraídos da literatura e de relatórios técnicos;

***Análise de estudos de caso*:** A partir de casos práticos documentados, será feita uma análise de como as ferramentas foram aplicadas, identificando os principais desafios enfrentados e as soluções implementadas;

***Correlações entre desafios e soluções*:** Os desafios identificados na análise de dispositivos móveis, como a fragmentação do sistema Android e as barreiras de segurança do iOS, serão correlacionados com as estratégias sugeridas na literatura para superá-los;

***Geração de recomendações práticas*:** Com base nos dados coletados e analisados, serão propostas estratégias para otimizar o uso das ferramentas e superar as limitações tecnológicas e operacionais na análise forense digital.

Ao seguir essa metodologia, espera-se obter uma compreensão abrangente das capacidades e limitações das ferramentas forenses e fornecer contribuições práticas e teóricas para o campo da análise forense digital em dispositivos móveis.

5.1 Procedimentos metodológicos

Este capítulo descreve os procedimentos metodológicos adotados na realização desta pesquisa, com foco em fornecer uma abordagem estruturada para a investigação sobre análise forense digital em dispositivos móveis. O método descrito visa garantir a organização, confiabilidade e validade dos dados e dos resultados obtidos, orientando as atividades necessárias para o alcance dos objetivos propostos.

5.2 Tipo de pesquisa

A pesquisa caracteriza-se como de natureza aplicada, uma vez que busca resolver problemas específicos relacionados à análise forense digital em dispositivos móveis, fornecendo subsídios teóricos e práticos para profissionais da área. Trata-se de uma pesquisa de natureza descritiva, pois tem como foco a compreensão detalhada das ferramentas, métodos e desafios envolvidos nesse campo. Além disso, a abordagem metodológica é

predominantemente qualitativa, pois prioriza a análise interpretativa das informações coletadas.

5.3 Etapas da pesquisa

5.3.1 Revisão bibliográfica

A primeira etapa consiste em uma revisão bibliográfica ampla sobre análise forense digital, dispositivos móveis e ferramentas especializadas, como Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective. Foram consultadas bases de dados acadêmicas, como IEEE Xplore, ScienceDirect e Google Scholar, além de manuais técnicos das ferramentas analisadas. Essa revisão visa identificar os principais conceitos, desafios e boas práticas no campo da forense digital.

5.3.2 Análise documental

Documentos técnicos e estudos de casos publicados por fabricantes das ferramentas forenses foram analisados para compreender as funcionalidades, limitações e aplicações práticas dessas soluções. Essa etapa é fundamental para avaliar criticamente as capacidades dessas ferramentas no processo de extração e análise de dados.

5.3.3 Estudo comparativo

Com base nos dados obtidos, será realizado um estudo comparativo entre as ferramentas Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective. Foram definidos critérios de comparação, como:

- Capacidade de extração de dados: física, lógica e baseada em nuvem;
- Compatibilidade: suporte a diferentes sistemas operacionais (Android e iOS) e versões;
- Eficiência em dados criptografados: avaliação das capacidades para acessar dados protegidos;
- Facilidade de uso: interface intuitiva e curva de aprendizagem.

Os critérios foram selecionados com base na literatura e na documentação das ferramentas, buscando identificar vantagens e limitações.

5.3.4 Coleta de dados

Os dados serão coletados de forma indireta, através de fontes secundárias, como artigos acadêmicos, relatórios técnicos, estudos de caso e manuais. Essa coleta teve como objetivo fornecer informações suficientes para a análise das ferramentas e dos métodos empregados na análise forense de dispositivos móveis.

5.3.5 Análise qualitativa

A análise qualitativa foi conduzida através da triangulação dos dados coletados, permitindo uma interpretação detalhada das capacidades das ferramentas e dos desafios enfrentados na análise de dispositivos móveis. Essa análise possibilitou a geração de recomendações para superar limitações e otimizar os processos investigativos.

5.4 Considerações éticas

Todas as informações coletadas e analisadas serão obtidas de fontes públicas ou disponíveis mediante permissão dos fabricantes. Não haverá coleta direta de dados sensíveis ou intervenção com participantes humanos. Ademais, as implicações éticas da utilização das ferramentas forenses foram consideradas, com ênfase no respeito à privacidade e à integridade das evidências digitais.

6 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A presente pesquisa teve como objetivo analisar as principais ferramentas e métodos utilizados na análise forense digital em dispositivos móveis, especialmente em relação aos sistemas operacionais Android e iOS, bem como avaliar seus desafios e limitações. A partir da revisão teórica, estudo comparativo e análise documental, foram obtidos resultados que permitem responder às hipóteses inicialmente propostas e discutir criticamente as práticas vigentes na área.

6.1 Relação com os objetivos e hipóteses da pesquisa

A investigação confirmou que as ferramentas Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective se destacam como as soluções mais utilizadas no mercado forense digital, cada uma com suas potencialidades e limitações específicas. Assim, respondeu-se à primeira hipótese, identificando as principais barreiras enfrentadas na análise forense de dispositivos móveis, entre elas:

- A fragmentação do sistema Android, dificultando a aplicação uniforme de técnicas de extração de dados.
- As robustas barreiras de segurança do iOS, como o Secure Enclave, que limitam o acesso mesmo por ferramentas avançadas.
- A criptografia ponta a ponta em aplicativos de mensagens, especialmente em apps como Signal e Telegram, que dificultam ou impedem a recuperação de comunicações.

Esses fatores confirmam que o contexto técnico é altamente desafiador, exigindo atualizações constantes das ferramentas e aperfeiçoamento dos métodos utilizados.

Em relação à segunda hipótese, verificou-se que as técnicas de extração física e lógica permanecem como as mais eficazes, complementadas pela extração de dados em nuvem, que representa uma tendência crescente no cenário forense, dado o volume significativo de informações armazenadas remotamente. Além disso, a recuperação de dados deletados, a análise de metadados e a reconstrução de linhas do tempo são práticas consolidadas e essenciais.

No que tange à terceira hipótese, os cuidados éticos e legais são indispensáveis, especialmente com o advento da LGPD, que reforça a necessidade de:

- Minimização na coleta de dados.

- Garantia da integridade e confidencialidade das informações.
- Documentação minuciosa de todas as etapas da investigação.

  Esses cuidados foram sistematicamente abordados e reforçados ao longo do estudo.

6.2 Eficiência e limitações das ferramentas estudadas

A análise detalhada das três principais ferramentas demonstrou que:

- ✓ **Cellebrite UFED**:

  Ponto forte: vasta compatibilidade com dispositivos e capacidade de realizar desbloqueios em modelos antigos.

  Limitação: dificuldade crescente para acessar dispositivos com criptografia avançada, especialmente os mais recentes da Apple.
- ✓ **Magnet AXIOM**:

  Ponto forte: eficiência na recuperação de dados apagados e integração com diversas fontes, incluindo computação em nuvem.

  Limitação: tempo de processamento elevado e suporte limitado a certos aplicativos menos populares.
- ✓ **Oxygen Forensic Detective**:

  Ponto forte: ampla cobertura de aplicativos de mensagens e capacidade de extrair dados de dispositivos IoT e drones, o que amplia sua aplicabilidade.

  Limitação: dificuldades na extração de dados de aplicativos com criptografia ponta a ponta e desafios no suporte a dispositivos recém-lançados.

A comparação entre os casos analisados evidenciou que nenhuma ferramenta é universalmente superior; ao contrário, cada uma atende melhor a contextos específicos de investigação.

6.3 Estratégias para superar as limitações identificadas

Com base na análise comparativa, algumas estratégias podem ser sugeridas para contornar as limitações apontadas:

- Investimento contínuo em pesquisa e desenvolvimento pelas fabricantes de ferramentas, especialmente em técnicas de engenharia reversa e análise de memória volátil.

- Desenvolvimento de métodos que explorem vulnerabilidades zero-day, desde que em consonância com normas éticas e legais.
- Ampliação da integração entre ferramentas forenses e plataformas de computação em nuvem, para potencializar a coleta de dados remotos.
- Capacitação permanente de peritos forenses, visando o domínio das mais recentes tecnologias e a atualização sobre as legislações aplicáveis.

6.4 Impactos práticos e científicos da pesquisa

Os resultados obtidos neste estudo possuem significativa relevância prática, pois contribuem para a orientação de profissionais que atuam com investigação forense digital, indicando as ferramentas mais adequadas para cada tipo de cenário e os cuidados necessários para garantir a legalidade das operações.

Cientificamente, o estudo fortalece a compreensão sobre as limitações técnicas atuais, apontando direções para o desenvolvimento de soluções mais eficazes e seguras. Além disso, destaca a importância da intersecção entre aspectos técnicos, legais e éticos na análise forense digital, especialmente com a crescente complexidade dos dispositivos móveis e o reforço das legislações sobre privacidade de dados. Como demonstrado no Quadro 4, cada ferramenta possui vantagens e limitações específicas que orientam sua escolha conforme o contexto investigativo.

Quadro 3 - Comparativo das Ferramentas Forenses Estudadas

Critério	**Cellebrite UFED**	**Magnet AXIOM**	**Oxygen Forensic Detective**
Tipo de extração	Física, lógica e nuvem	Física, lógica e nuvem	Física, lógica, nuvem, IoT e drones
Ponto forte	Ampla compatibilidade com dispositivos móveis	Recuperação avançada de dados deletados e integração com nuvem	Suporte amplo a aplicativos de mensagens e análise de dispositivos IoT
Limitação	Dificuldade crescente com criptografia avançada e novos dispositivos	Tempo elevado de processamento e suporte limitado a alguns apps	Desafios com criptografia ponta a ponta e suporte a dispositivos mais

			recentes
Usabilidade	Interface robusta, mas pode ser complexa para iniciantes	Interface intuitiva com boas visualizações	Interface poderosa, porém, complexa para novos usuários
Aplicabilidade	Perícias criminais, desbloqueio de dispositivos e análise de backups	Análise detalhada de arquivos deletados e metadados	Investigações que envolvem múltiplos dispositivos e fontes, como IoT e nuvem
Evolução necessária	Melhorias em engenharia reversa e bypass de novos bloqueios	Otimização do tempo de processamento e maior suporte a APIs	Avanços na extração de dados criptografados e na integração com novos dispositivos

Fonte: elaborada pelo autor, 2025.

6.5 Considerações sobre a evolução tecnológica e os desafios futuros

A análise revelou que o principal desafio da área reside na velocidade com que novas barreiras de segurança são implementadas nos sistemas operacionais e aplicativos. A criptografia por padrão, a autenticação biométrica e os sistemas de armazenamento seguro dificultam cada vez mais o trabalho forense.

Neste contexto, a pesquisa aponta para a necessidade de um esforço multidisciplinar, envolvendo especialistas em segurança da informação, engenharia reversa, direito digital e políticas públicas, com vistas a desenvolver ferramentas mais eficazes, sem comprometer os direitos fundamentais dos cidadãos. Dentre os desafios futuros destacados, é possível visualizar algumas propostas de pesquisa, conforme sistematizado no Quadro 5.

Quadro 4 - Desafios futuros e propostas de pesquisa na análise forense em dispositivos móveis

Desafio Futuro	**Proposta de Pesquisa/Desenvolvimento**
Aumento das barreiras criptográficas nos sistemas Android e iOS	Investimento em técnicas legais de engenharia reversa, pesquisa em análise de memória volátil e modelagem forense preditiva
Popularização de novos dispositivos com segurança reforçada (ex.: criptografia por padrão, autenticação biométrica)	Desenvolvimento de soluções forenses capazes de realizar extrações não-invasivas e pesquisa em vulnerabilidades zero-day de forma ética

Crescente uso de aplicativos com criptografia ponta a ponta	Pesquisa em métodos de análise de metadados, análise de rede e engenharia reversa de processos em execução
Armazenamento massivo de dados em nuvem	Fortalecimento da integração das ferramentas com APIs de provedores de nuvem e padronização de procedimentos forenses em ambientes cloud
Necessidade de respeitar leis de proteção de dados (LGPD, GDPR)	Desenvolvimento de frameworks forenses alinhados com legislações de privacidade, reforçando boas práticas éticas e legais na coleta e análise de dados
Falta de profissionais capacitados para atuar com ferramentas e técnicas avançadas	Ampliação de programas de capacitação, certificações e cursos especializados em forense digital aplicada a dispositivos móveis e ambientes em nuvem

Fonte: elaborada pelo autor, 2025.

7 CONCLUSÃO

A análise forense digital em dispositivos móveis é um campo de investigação cada vez mais relevante e desafiador no contexto da segurança da informação e da justiça criminal. Ao longo deste trabalho, foi possível realizar uma investigação aprofundada sobre os principais métodos, ferramentas e desafios inerentes à análise forense de dispositivos móveis, com foco especial nos sistemas operacionais Android e iOS.

Os resultados obtidos confirmam que as ferramentas Cellebrite UFED, Magnet AXIOM e Oxygen Forensic Detective, são atualmente as soluções mais consolidadas e amplamente utilizadas no mercado. Contudo, a pesquisa também evidenciou que, apesar dos avanços tecnológicos, persistem significativas limitações relacionadas à fragmentação do Android, às barreiras de segurança implementadas pelo iOS e às criptografias ponta a ponta presentes em aplicativos de comunicação.

Dessa forma, a principal contribuição deste estudo reside na sistematização das vantagens e limitações das ferramentas forenses, bem como na proposição de estratégias e direções para pesquisas futuras, com vistas a superar os obstáculos tecnológicos e legais que permeiam essa área. Além disso, reforçou-se a necessidade de que as práticas forenses sejam sempre pautadas pela ética e pelo respeito às legislações vigentes, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD).

Como limitação desta pesquisa, destaca-se a natureza exclusivamente bibliográfica e documental, sem a realização de experimentações práticas em laboratório ou com dispositivos reais. Embora essa abordagem tenha permitido um panorama amplo e atualizado do tema, investigações futuras podem ampliar o escopo do estudo, com testes práticos das ferramentas analisadas e avaliação de sua eficácia em cenários reais de investigação.

Para pesquisas futuras, recomenda-se explorar temas como: o desenvolvimento de técnicas mais eficazes de extração de dados criptografados; a padronização de procedimentos forenses em ambientes de computação em nuvem; e o estudo do impacto das legislações de privacidade no cotidiano das investigações forenses.

Por fim, este trabalho pretende contribuir com a formação e atuação de profissionais da área de perícia digital, fornecendo subsídios teóricos e práticos para a compreensão dos desafios atuais e das tendências futuras no campo da análise forense digital em dispositivos móveis, consolidando-se como uma referência para novos estudos e para o aprimoramento das práticas forenses.

8 CRONOGRAMA DE EXECUÇÃO

As etapas da pesquisa foram planejadas conforme o cronograma a seguir:

Quadro 5 - Cronograma de execução

Etapa	Período	Atividade	Descrição
1	Até 09 de maio	Correções iniciais	Ajustes conforme revisões da banca examinadora do TCC1.
2	12 a 16 de maio	Aprofundamento teórico e prático	Ampliação da fundamentação teórica e melhorias no projeto prático, com revisão da Introdução e Justificativa.
3	19 a 25 de maio	Execução final do projeto ou pesquisa	Conclusão de experimentos, coleta ou implementação.
-	26 a 31 de maio	Período de recuperação	Tempo reservado para eventuais atrasos ou ajustes pendentes da etapa anterior.
4	02 a 20 de junho	Análise crítica dos resultados	Interpretação dos resultados obtidos, vinculando-os aos objetivos e hipóteses. Revisão das seções de Análise e Discussão.
-	23 a 27 de junho	Período de recuperação	Tempo extra para possíveis pendências da etapa 4.
5	02 a 06 de julho	Finalização do texto	Revisão geral, incluindo elementos pré e pós-textuais, apêndices e referências.
6	09 a 13 de julho	Preparação e defesa final	Elaboração dos slides e preparação para a apresentação pública.

Fonte: elaborada pelo autor, 2025.

Esse cronograma será ajustado conforme a necessidade durante o andamento da pesquisa, garantindo a conclusão das atividades dentro do prazo previsto.

Os procedimentos metodológicos descritos neste capítulo asseguram uma abordagem sistemática e confiável para a investigação sobre análise forense digital em dispositivos móveis, contribuindo para a validade dos resultados e sua relevância para o campo de estudo.

REFERÊNCIAS

AL-KHASAWNEH, A.; et al. **Mobile Forensics**: Challenges and Future Directions. Digital Investigation, v. 36, p. 301-315, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR 6023:2023**: Guia para elaboração de referências - Informação e Documentação – Referências. Rio de Janeiro, 2023.

BACKLINKO. **iPhone vs Android**: Estatísticas. Disponível em: https://backlinko.com. Acesso em: 20 dez. 2024.

CASEY, Eoghan**. Digital Evidence and Computer Crime**. Academic Press, 2011.

CAVALLI, F.; OLIVEIRA, L. M. **Análise Forense em Dispositivos Móveis**: Desafios e Ferramentas. Revista Brasileira de Computação Aplicada, v. 12, n. 3, p. 45-60, 2023.

CELLEBRITE. UFED Series **– Universal Forensic Extraction Device**. Disponível em: https://www.cellebrite.com. Acesso em: 9 fev. 2025.

FOURINC. **Logo Blue PNG [imagem]**. Disponível em:https://www.fourinc.com/imager/images/26192/logo_blue_png_a1f0d52ff9b54f3b1a5b1f3bdf9e76ef.png . Acesso em: 10 fev. 2025.

GARCIA, J.; Lima, R. **Forense Digital**: Princípios e Práticas. 2. ed. São Paulo: Novatec, 2020.

KASPERSKY. **Mobile Cyberthreats in 2023**: Analysis and Statistics. Moscou: Kaspersky Lab, 2023. Disponível em: https://www.kaspersky.com. Acesso em: 20 jan. 2024.

KLINCZAK, Marjori Naiele Mocelin. **Uma Revisão das Técnicas Forenses Aplicadas aos Dispositivos Móveis**. São Paulo: ICoFCS, 2018. Disponível em: http://dx.doi.org. Acesso em: 21 jan. 2025.

KRUSE, W. G.; HEISER, J. G. **Computer Forensics**: Incident Response Essentials. Addison-Wesley, 2002.

LIBLOGO. **Cellebrite Logo [imagem]**. Disponível em: <https://www.liblogo.com/img-logo/ce8812c365-cellebrite-logo-cellebrite-wins-significant-open-source-intelligence-solutions.png>. Acesso em: 10 fev. 2025.

MAGNET FORENSICS. **Magnet AXIOM**. Disponível em: https://www.magnetforensics.com. Acesso em: 10 fev. 2025.

MAGNET FORENSICS. **MF Blog AXIOM 3.0 Timeline [imagem]**. Disponível em: https://www.magnetforensics.com/wpcontent/uploads/2019/03/MF_Blog_AXIOM_3.0_Timeline.jpg. Acesso em: 10 fev. 2025.

MASTROIANNI, M. **Forensic Analysis of Mobile Devices**. Journal of Digital Forensics, 2022.

NIST – National Institute of Standards and Technology. **Mobile Device Forensic Tool Testing Program**. Disponível em: https://www.nist.gov. Acesso em: 9 fev. 2025.

O'SHOUGHNESSY, P.; SAPPENFIELD, J. **Android Forensics**: A Practitioner's Guide. Cambridge: Elsevier, 2018.

POLLITT, M. **Computer Forensics**: An Approach to Evidence in Cyberspace. In: National Information Systems Security Conference, 1995, Baltimore. Anais [...]. Baltimore: NIST, 1995. p. 487-491.

PORTAL DA SEGURANÇA. **Casos de estelionato no Brasil atingem recorde em 2022**. Disponível em: https://www.portaldaseguranca.com.br. Acesso em: 20 dez. 2024.

SALIBA, J. **Digital Forensics with Magnet AXIOM**. Toronto: Magnet Press, 2021.

SCHAEFER, R.; et al. **Trends in Mobile Forensic Investigations**. Forensic Science International, v. 338, p. 111-422, 2022. Disponível em: https://www.sciencedirect.com. Acesso em: 20 jan. 2024.

SILVA, T. **Direito Digital e a Privacidade no Brasil**. Revista de Direito e Tecnologia, 2021.

STATISTA. **Sistema operativo móvil com maior participação de mercado por país**. Disponível em: https://es.statista.com. Acesso em: 20 dez. 2024.

GLOSSÁRIO

Análise forense digital: área que aplica métodos técnicos e científicos para identificar, preservar, extrair e analisar dados digitais como evidências em investigações.

Android (sistema operacional): sistema operacional open-source usado em dispositivos de diversas marcas, como Samsung e Xiaomi.

Bypass de senha: métodos técnicos para contornar ou ignorar sistemas de bloqueio por senha em dispositivos.

Cellebrite UFED: ferramenta usada para extrair e analisar dados de dispositivos móveis, incluindo mensagens e arquivos apagados.

Cloud computing (computação em nuvem): tecnologia que permite o armazenamento e processamento de dados em servidores remotos.

Confidencialidade de informações: proteção contra acessos não autorizados às informações analisadas.

Consentimento informado: permissão explícita do usuário para acesso aos seus dados, essencial em investigações éticas.

Criptografia avançada: métodos de proteção de dados que garantem a segurança ao codificá-los, acessíveis apenas com chaves específicas.

Data protection API: interface usada para proteger dados sensíveis em dispositivos, como arquivos e chaves de criptografia.

Descriptografia: processo de decodificar dados criptografados para torná-los legíveis.

Extração lógica e física: métodos para acessar dados de dispositivos: a lógica recupera dados visíveis; a física acessa todo o conteúdo armazenado, incluindo apagados.

Extração por nuvem: recuperação de dados armazenados em serviços online (iCloud, Google Drive), sem necessidade do dispositivo físico.

Força bruta (ataque): técnica que tenta todas as combinações possíveis de senhas para acessar um sistema protegido.

Fragmentação de sistema: diversidade de versões e customizações em sistemas operacionais, dificultando a análise uniforme.

Hashes criptográficos: assinaturas digitais únicas usadas para verificar a integridade dos dados.

Imagem forense: cópia bit a bit de um dispositivo digital que preserva os dados originais para análise.

Integridade de dados: garantia de que os dados analisados não foram alterados desde sua coleta.

iOS (sistema operacional): sistema operacional da Apple usado em dispositivos como iPhones e iPads.

IoT (internet das coisas): rede de dispositivos conectados à internet que compartilham dados, como drones e assistentes virtuais.

ISO/IEC 27037: norma internacional que orienta a coleta, preservação e análise de evidências digitais.

Keylogging: técnica que registra todas as teclas digitadas em um dispositivo, usada em ataques maliciosos.

Lei Geral de Proteção de Dados (LGPD): lei brasileira que regula o uso de dados pessoais, protegendo a privacidade dos usuários.

Linha do tempo de atividades: representação cronológica das ações realizadas em um dispositivo, usada para reconstruir eventos.

Magnet AXIOM: software especializado na recuperação e análise de dados digitais de dispositivos móveis, computadores e serviços em nuvem.

Marco civil da internet: legislação brasileira que estabelece direitos e deveres no uso da internet, incluindo privacidade e segurança.

Metadados: informações sobre dados, como data de criação, local ou autor, que ajudam na análise forense.

Minimização de dados: prática de coletar apenas os dados necessários para uma investigação, preservando a privacidade.

Oxygen Forensic Detective: ferramenta para análise detalhada de aplicativos, redes sociais, serviços em nuvem e dispositivos IoT.

Pathfinder (Cellebrite): solução para visualização e análise de dados extraídos de dispositivos, identificando padrões e conexões.

Phishing: golpe que tenta enganar usuários para fornecerem dados pessoais, como senhas e informações bancárias.

Sacos de faraday: ferramentas que bloqueiam sinais de rádio para evitar a alteração remota de dados em dispositivos durante uma investigação.

Secure boot: tecnologia que impede a execução de sistemas ou softwares não autorizados durante a inicialização de dispositivos.

Secure enclave: coprocessador nos dispositivos iOS que gerencia dados criptográficos de forma isolada e segura.

SQLite (banco de dados): banco de dados leve e amplamente usado em dispositivos móveis para armazenar informações como mensagens e registros.

Token de autenticação: credenciais digitais que permitem o acesso a sistemas ou serviços em nuvem.

UFED Cloud Analyzer: ferramenta da Cellebrite para análise de dados armazenados em serviços de nuvem.

UFED Premium: versão avançada da Cellebrite que permite desbloqueios e extrações de dispositivos com alta segurança.