

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Título do Artigo: Aplicações da Inteligência Artificial na Perícia Digital voltada à Investigação de Crimes Digitais.

Autores: Rodrigo Pecorari dos Santos Junior
rodrigopsjr98@gmail.com

Orientador: Hélio Luís Da Silva Rodrigues
helio.rodrigues@cps.sp.gov.br

Resumo

O crescente uso digital na sociedade impulsiona o aumento dos crimes cibernéticos, tornando a perícia digital uma atividade essencial para a identificação, preservação e análise de evidências digitais. Por isso, este trabalho analisa as aplicações da Inteligência Artificial (IA) na perícia digital voltada à investigação de crimes digitais, destacando suas contribuições, limitações e impactos no processo investigativo. A pesquisa foi desenvolvida por meio de uma abordagem exploratória e descritiva, com revisão bibliográfica, análise documental e estudo de caso, envolvendo ferramentas forenses e tecnologias de IA. Foram analisadas aplicações relacionadas à análise automatizada de grandes volumes de dados, detecção de fraudes, reconhecimento de padrões, análise de logs e de redes, processamento de linguagem natural e recuperação de evidências digitais. Como resultado, verificou-se que a IA pode aumentar significativamente a eficiência das investigações, reduzindo o tempo necessário para a análise de evidências e auxiliando na identificação de comportamentos suspeitos. Além disso, o estudo demonstrou a viabilidade da integração entre ferramentas forenses e modelos de linguagem por meio do protocolo MCP, ampliando as capacidades analíticas dos peritos. Porém, também foram identificados desafios relacionados à privacidade, à transparência, à cadeia de custódia e à conformidade legal, evidenciando a necessidade de supervisão humana e uso responsável dessas tecnologias.

Palavras-chave: Inteligência Artificial; Perícia Digital; Crimes Cibernéticos; Computação Forense; Investigação Digital.

**CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO**

Abstract

The increasing digitalization of society has driven the growth of cybercrime, making digital forensics an essential activity for the identification, preservation, and analysis of digital evidence. Therefore, this study examines the applications of Artificial Intelligence (AI) in digital forensics focused on the investigation of cybercrimes, highlighting its contributions, limitations, and impacts on the investigative process. The research was developed through an exploratory and descriptive approach, using a literature review, document analysis, and a case study involving forensic tools and AI technologies. Applications related to the automated analysis of large volumes of data, fraud detection, pattern recognition, log and network analysis, natural language processing, and digital evidence recovery were examined. The results showed that AI can significantly increase the efficiency of investigations by reducing the time required for evidence analysis and assisting in the identification of suspicious behaviors. Furthermore, the study demonstrated the feasibility of integrating forensic tools with language models through the MCP protocol, expanding the analytical capabilities of forensic experts. However, challenges related to privacy, transparency, chain of custody, and legal compliance were also identified, highlighting the need for human oversight and the responsible use of these technologies.

Keywords: Artificial Intelligence; Digital Forensics; Cybercrime; Computer Forensics; Digital Investigation.

1. INTRODUÇÃO

O avanço da tecnologia e a crescente digitalização da sociedade transformaram não somente as formas de comunicação e de armazenamento de informações, mas também as práticas criminosas, que passaram a ocorrer com frequência em ambientes digitais. Nesse contexto, a perícia digital tornou-se fundamental para a identificação, preservação e análise de evidências relacionadas a atividades ilícitas.

Entretanto, o grande volume e a complexidade dos dados digitais representam um desafio para os métodos tradicionais de investigação. A necessidade de maior agilidade e precisão na análise dessas informações evidencia a importância da adoção de novas tecnologias.

A Inteligência Artificial (IA), por meio de técnicas como *machine learning* (Aprendizagem de Máquina) e *deep learning* (Aprendizado Profundo), apresenta-se como uma ferramenta eficaz para automatizar processos, identificar padrões e auxiliar na detecção de comportamentos suspeitos. Contudo, sua aplicação também envolve desafios técnicos, éticos e legais que devem ser considerados.

Dessa forma, este trabalho propõe analisar as aplicações da IA na perícia digital voltada à investigação de atividades ilícitas, destacando seus benefícios, limitações e contribuições para o fortalecimento das práticas forenses.

2. REFERENCIAL TEÓRICO

2.1 Forense Computacional e Investigação de Crimes Cibernéticos

A Forense Computacional, também conhecida como forense digital ou perícia digital, reúne técnicas científicas e metodológicas para a identificação, coleta, preservação, análise e apresentação de evidências digitais. Segundo Oettinger (2021), o termo "computação forense" foi o padrão no passado; o conceito atualmente se expandiu para abranger a recuperação de dados de qualquer dispositivo de armazenamento, mantendo o foco na integridade da informação.

2.1.1 A Essência e o Processo de análise

No universo de tecnologias que podem passar por perícia, podemos pontuar que tudo o que mantém alguma informação, seja ela processada de forma sistêmica e armazenada digitalmente em formato binário, pode ser periciado. Seguindo esta premissa, podemos incluir neste grupo de tecnologias.

- Computadores (desktops, workstations e notebooks)
- Servidores
- Mobile (smartphones, tablets)
- Memórias Ram

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

- Unidades de armazenamento massivo (pendrives, discos rígidos, SSD, cartões de memória, entre outros)
- Sites
- Dispositivos de IoT
- Servidores virtuais e ambientes em Cloud

A análise forense pode ser dividida em duas modalidades: a Online (Live Forensics) e a Post-mortem:

- **Online:** feita com o sistema em execução para capturar dados voláteis como a memória RAM,
- **Post-mortem:** realizada após o desligamento do sistema.

Para viabilizar esse trabalho, utilizam-se bloqueadores de escrita (*write blockers*) para manter a integridade dos dados armazenados nas mídias e em softwares renomados como EnCase, FTK e Autopsy. No cenário brasileiro, destaca-se o IPED (Indexador e Processador de Evidências Digitais), desenvolvido pela Polícia Federal para o processamento de grandes volumes de dados (BRASIL, 2024).

Independentemente da ferramenta ser comercial ou de código aberto, Oettinger (2021) defende que o ponto crucial é a expertise do profissional em validar os métodos e explicar a confiabilidade dos resultados. O desfecho de todo esse trabalho é o Laudo Pericial, um documento que deve ser claro, objetivo e tecnicamente fundamentado, utilizando o cálculo de hash para blindar os arquivos contra contestações de adulteração.

Conforme destaca Paula ([s.d.], p. 4), o princípio da documentação "é baseado na Cadeia de Custódia da prova material, ou seja, toda amostra deve ser cuidadosamente documentada desde o momento em que aparece no local do crime até sua análise em exames complementares, a fim de garantir e estabelecer um histórico completo de sua origem".

A integridade é reforçada pelo uso de funções hash — uma espécie de "carimbo digital" — e pela clonagem bit a bit (imagens forenses). Oettinger (2021) avisa que o perito nunca analisa a evidência original, mas sim uma cópia, para assegurar que o material fonte permaneça intocado. A integridade do laudo pericial depende diretamente da preservação dos elementos colhidos, pois qualquer falha na custódia do vestígio pode comprometer a idoneidade da prova e levar à sua nulidade judicial (PAULA, [s.d.]).

2.1.2 Forense Criminal

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

O propósito principal desta área não é somente encontrar artefatos, mas realizar uma análise formal que possa sustentar ou refutar acusações em juízo. Como destaca Oettinger (2021, p. 18), o exame serve para "provar que o acusado cometeu a violação ou refutar essa acusação". Assim, o papel do perito vai além da busca pela culpabilidade; ele atua na descoberta da verdade dos fatos, podendo inclusive produzir evidências que inocentem o investigado.

Diferente da investigação tradicional, que lida com elementos tangíveis como impressões digitais físicas, a investigação digital enfrenta a volatilidade dos dados. Enquanto a primeira foca em locais de crime físicos, a digital exige o rastreamento de logs, atividades online e o manejo de dados que podem ser facilmente alterados, demandando um rigor técnico superior na preservação.

"O Princípio da Observação diz que 'todo contato deixa uma marca'. Este princípio é a base da Criminalística e da própria investigação criminal." (PAULA, [s.d.], p. 8).

2.1.3 Procedimentos Técnicos

Para uma evidência ser aceita legalmente, a extração deve seguir protocolos rigorosos. Temos como modelos normas técnicas e frameworks, que estabelecem principalmente uma metodologia de análise e aquisição de evidências, preservando ao máximo a integridade dos dados que serão avaliados e posteriormente apresentados em relatórios.

Como base, temos normas/procedimentos padrão para o processo forense, aceitos mundialmente e especificados na Tabela 1.

Framework/Norma	Foco Principal	Publico-Alvo	Diferencial Científico
ISO/IEC 27037	Identificação, coleta, aquisição e preservação de evidências digitais.	Primeiros Respondentes (First Responders) e Peritos de Campo.	Estabece os princípios de auditabilidade, repetibilidade e reprodutibilidade global.
NIST SP 800-86	Integração de técnicas forenses na resposta a incidentes de segurança.	Equipes de Resposta a Incidentes (CSIRTs) e Administradores de TI.	Abordagem holística e corporativa sem comprometer a continuidade do negócio.
DFRWS	Fundamentação teórica e formalização da ciência forense digital.	Pesquisadores acadêmicos e Desenvolvedores de ferramentas forenses.	Primeira matriz conceitual linear separando classes de evidências de tecnologias.
SWGDE	Garantia de qualidade, práticas laboratoriais e cadeia de custódia.	Laboratórios forenses, Examinadores digitais e Sistema jurídico.	Rigor procedural em padrões de qualidade e validação legal de ferramentas.

Tabela 1: Normas e Frameworks para procedimento forense. Fonte: Elaborada pelo autor com auxílio de IA (2026).

O processo, acima de tudo, visa às melhores práticas envolvendo desde a coleta física, identificação e extração, antes mesmo de se avaliar qual ferramenta será utilizada em cada fase. É recomendado o uso de mídias externas de inicialização com sistemas operacionais periciais, forçando o equipamento a ignorar o sistema nativo via alterações na BIOS, impedindo a

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

corrupção de dados originais. Um pilar indispensável desse processo é a Cadeia de Custódia, que garante a idoneidade dos vestígios desde o isolamento e coleta até o descarte (Brasil, 2013).

A figura 1 ilustra todo o processo metodológico de uma análise forense computacional, seguindo a norma ISO 27037 (2012). Este processo é criterioso e metódico, no qual são pontuados, acima de tudo, o processo envolvido, seus riscos e boas práticas que devem ser seguidas para manter a integridade do resultado. Sequencialmente, como boas práticas, o perito deve:

- Identificar a estrutura que será analisada
- Efetuar a sua coleta (física)
- Efetuar a aquisição lógica (extração dos dados)
- Preservar os dados adquiridos
- Indexar e analisar os dados adquiridos, não mais os dados originais.
- Apresentar os resultados

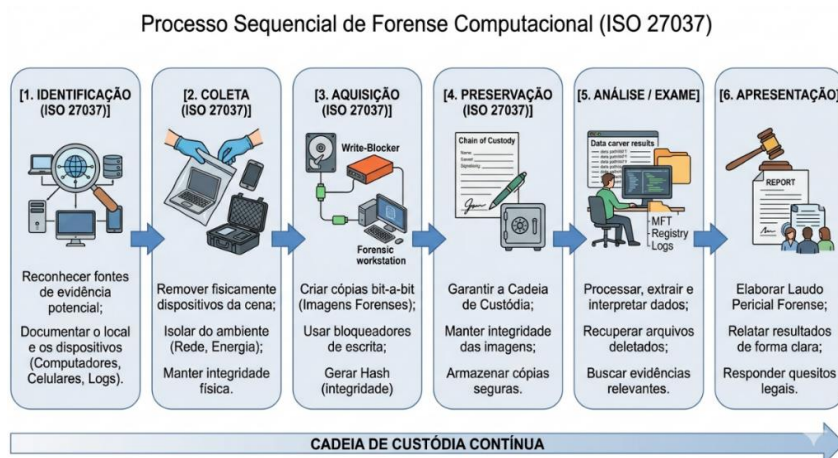


Figura 1: Baseado na ISO 27037. Fonte: Elaborada pelo autor com auxílio de IA (2026).

- **Desafios e ferramentas forenses**

O ambiente digital abriga desde crimes contra sistemas (hacking, DDoS) e pessoas (cyberbullying, extorsão) até fraudes financeiras complexas (phishing, lavagem de dinheiro). Contudo, o perito enfrenta obstáculos severos, como o volume massivo de dados e o anonimato proporcionado por VPNs e pela rede Tor.

A criptografia também surge como uma barreira, mas as diretrizes nacionais permitem o uso de métodos como força bruta, dicionários e *rainbow tables* para tentar o acesso aos dados (BRASIL, 2024). No fim, o maior desafio

permanece sendo a identificação do autor, como define Oettinger (2021, p. 19): “Fator humano como origem da falha”, associando a evidência digital a um indivíduo específico.

2.2 Inteligência Artificial e Machine Learning

- **Conceito de Inteligência Artificial**

A Inteligência Artificial (IA) é a capacidade de sistemas computacionais realizarem tarefas que simulam a inteligência humana, como raciocínio, aprendizado e tomada de decisão. Nesse sentido, trata-se de uma área da computação voltada para o desenvolvimento de sistemas inteligentes capazes de resolver problemas de forma autônoma (COZMAN; PLONSKI; NERI, 2021).

De acordo com Cozman, Plonski e Neri (2021, p. 15), a IA envolve diferentes abordagens, podendo ser compreendida como sistemas que “agem como humanos” ou que “agem racionalmente”. Essa definição evidencia a diversidade conceitual presente na área.

Atualmente, a IA pode ser dividida em dois grandes grupos: a IA fraca, voltada para tarefas específicas, e a IA forte, que busca simular a cognição humana. No entanto, a literatura aponta que a IA forte ainda se encontra em nível teórico e distante de aplicações práticas (BRANCO; TEFFÉ, 2022).

- **Machine Learning (ML)**

O Machine Learning (ML), ou aprendizado de máquina, é um dos principais campos da Inteligência Artificial, sendo responsável pelo desenvolvimento de algoritmos capazes de aprender padrões a partir de dados. Dessa forma, os sistemas tornam-se capazes de melhorar seu desempenho sem a necessidade de programação explícita para cada tarefa (COZMAN; PLONSKI; NERI, 2021).

No aprendizado supervisionado, os algoritmos são treinados com dados previamente rotulados, permitindo a construção de modelos capazes de prever resultados futuros.

Conforme destacado por Cozman, Plonski e Neri (2021, p. 42), trata-se de um processo no qual o sistema aprende “uma função que mapeia entradas em saídas desejadas”.

Além disso, existem outros processos, como o aprendizado não supervisionado, que busca identificar padrões ocultos nos dados, e o semi-supervisionado, que combina pequenas quantidades de dados rotulados com grandes volumes de dados não rotulados, aumentando a eficiência do aprendizado.

- **Técnicas importantes**

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

O desenvolvimento de sistemas de IA depende da aplicação de diversas técnicas de aprendizado e análise de dados. Essas técnicas vão desde métodos estatísticos tradicionais até abordagens mais avançadas, como redes neurais artificiais e deep learning.

Segundo Cozman, Plonski e Neri (2021), o avanço dessas técnicas possibilita desenvolver sistemas cada vez mais sofisticados, capazes de reconhecer padrões complexos e realizar tarefas antes restritas aos seres humanos.

Nesse contexto, o uso de redes neurais profundas tem se destacado por sua capacidade de processar grandes volumes de dados e identificar relações complexas entre variáveis. Como afirmam os autores, essas tecnologias ampliam significativamente o potencial da Inteligência Artificial em diversas áreas do conhecimento.

- **Processamento de dados**

O funcionamento da Inteligência Artificial está diretamente relacionado ao uso de grandes volumes de dados. O conceito de Big Data refere-se à capacidade de coletar, armazenar e processar grandes quantidades de informações em alta velocidade e variedade (BRANCO; TEFFÉ, 2022).

De acordo com Branco e Teffé (2022, p. 28), o Big Data caracteriza-se pela “produção massiva e contínua de dados”, exigindo novas formas de processamento e análise.

Nesse cenário, a mineração de dados (Data Mining) desempenha um papel fundamental ao permitir a extração de conhecimento relevante a partir de dados brutos. Esse processo possibilita identificar padrões e tendências que auxiliam na tomada de decisão e no aprimoramento dos sistemas inteligentes.

- **Vantagens e limitações.**

A Inteligência Artificial apresenta diversas vantagens, como a automação de processos, aumento da eficiência e capacidade de análise em larga escala. No entanto, também enfrenta limitações importantes.

Um dos principais desafios é o viés algorítmico, que ocorre quando os sistemas reproduzem preconceitos presentes nos dados de treinamento. Segundo Branco e Teffé (2022), algoritmos podem gerar decisões discriminatórias quando baseados em dados enviesados, impactando diretamente a sociedade.

Além disso, a falta de transparência nos sistemas de IA, conhecida como problema da “caixa preta”, dificulta a compreensão de como as decisões são tomadas. Isso reforça a necessidade de maior controle, ética e governança no desenvolvimento dessas tecnologias.

2.3 Aplicações da IA na Perícia Digital

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

A Inteligência Artificial (IA) amplia as possibilidades da perícia digital ao automatizar a análise de dados, identificar padrões suspeitos e otimizar investigações cibernéticas. Essas tecnologias contribuem para tornar os processos investigativos mais rápidos e precisos, principalmente diante do grande volume de informações digitais. Segundo Norte Filho et al., a IA “possibilita o tratamento automatizado de grandes volumes de informações, contribuindo para a identificação de comportamentos suspeitos”. Dessa forma, a IA se consolida como uma importante ferramenta de apoio à perícia digital e à investigação de crimes cibernéticos.

- **Análise de dados**

A Inteligência Artificial (IA) aplicada à análise de dados permite o processamento de grandes volumes de informações, filtrando evidências relevantes e reduzindo o tempo de investigação. Nesse contexto, a perícia digital tem como objetivo “identificar, coletar e examinar/analisar os dados digitais” (OETTINGER, 2021, s.p.), evidenciando a importância de tecnologias que auxiliem na triagem dessas informações.

Segundo Branco e Teffé (2022), a IA consiste em um conjunto de técnicas que permite “processar grandes volumes de dados para projetar tarefas de processamento computacional muito complexas”.

Além disso, segundo Oettinger (2021), o investigador deve “filtrar e excluir dados que não são pertinentes à sua investigação” (OETTINGER, 2021, s.p.), demonstrando, indiretamente, como a IA pode otimizar esse processo ao automatizar a seleção de dados relevantes.

- **Deteção de fraudes**

A IA contribui significativamente para a deteção de fraudes ao identificar padrões anômalos e atividades suspeitas. Conforme destaca Oettinger (2021), a análise das evidências digitais é essencial para “provar que o acusado cometeu a violação ou refutar essa acusação” (OETTINGER, 2021, s.p.).

Assim, segundo Branco e Teffé (2022), essas funcionalidades permitem reduzir significativamente o tempo de investigação, tornando a perícia mais ágil. Dessa forma, sistemas inteligentes podem auxiliar na identificação de comportamentos fora do padrão, apoiando investigações antifraude de maneira mais eficiente.

- **Análise de logs e redes**

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

A análise de logs e redes com o auxílio da IA permite detectar intrusões e ataques cibernéticos. Segundo Oettinger (2021), as evidências digitais podem revelar “informações relacionadas às conexões de rede do host com outros hosts” (OETTINGER, 2021, s.p.), sendo fundamentais na investigação de invasões. Isso ocorre porque, segundo Branco e Teffé (2022), a tecnologia permite analisar dados de diferentes fontes e “identificar possíveis ajustes nos fluxos de trabalho”.

Assim, indiretamente, a IA possibilita a automação da análise dessas conexões, identificando atividades suspeitas com maior rapidez e precisão.

- **Reconhecimento de padrões**

O reconhecimento de padrões é uma das principais aplicações da IA na perícia digital, permitindo a identificação de comportamentos criminosos. Conforme afirma Oettinger (2021), os artefatos digitais são “pistas que levam à identidade da pessoa que conduziu a atividade ilegal” (OETTINGER, 2021, s.p.).

Nesse sentido, como dizem Branco e Teffé (2022), essa funcionalidade permite identificar comportamentos criminosos e perfis suspeitos com maior assertividade.

- **Processamento de Linguagem Natural (NLP)**

O uso de IA por meio do Processamento de Linguagem Natural (NLP) possibilita a análise de e-mails, mensagens e redes sociais. De acordo com Oettinger (2021), a investigação pode envolver grande volume de dados digitais, incluindo comunicações eletrônicas (OETTINGER, 2021, s.p.). Além disso, como destaca o autor, é necessário analisar tanto o emissor quanto o receptor das mensagens para uma investigação completa (OETTINGER, 2021, s.p.). Assim, o NLP automatiza essa análise, permitindo identificar conteúdos suspeitos e possíveis ameaças.

Nesse sentido, destaca-se que técnicas de linguagem natural ampliam as possibilidades de análise automatizada de dados textuais (BRANCO; TEFFÉ, 2022, p. 13)

- **Análise de imagens e vídeos**

A IA também pode ser aplicada na análise de imagens e vídeos, especialmente na identificação de conteúdos ilícitos. Segundo Lopes e Silva Filho, a análise de dados de celulares tornou-se um pilar nas investigações modernas, porém, a quantidade de informações contida nesses aparelhos representa um grande obstáculo.

Um único dispositivo pode armazenar dezenas de milhares de imagens, vídeos e mensagens, cuja análise manual é demorada, suscetível a erros e, muitas vezes, inviável em sua totalidade. (LOPES; SILVA FILHO, 2025). Dessa forma, algoritmos de IA podem automatizar o reconhecimento dessas imagens, tornando o processo investigativo mais ágil e eficaz.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

- **Recuperação de evidências**

A recuperação de evidências digitais pode ser aprimorada com o uso de IA, principalmente na organização e classificação automáticas de arquivos. Segundo Oettinger (2021), destacam-se técnicas como “recuperação de dados apagados” no processo de investigação.

Assim, a IA pode auxiliar na reconstrução de informações e na priorização de evidências relevantes para o caso. Esse processo está diretamente relacionado à automação de atividades rotineiras, característica central dessas tecnologias (BRANCO; TEFFÉ, 2022).

- **Análise preditiva**

A análise preditiva com IA permite antecipar possíveis crimes e apoiar a inteligência policial. Segundo Oettinger (2021), a análise das evidências digitais determinará se os fatos encontrados corroboram a ocorrência de um crime. Nesse sentido, a IA pode utilizar dados históricos para prever comportamentos suspeitos, contribuindo para ações preventivas.

Nota-se que o avanço da IA está diretamente ligado à disponibilidade de dados e à evolução da capacidade computacional, fatores que impulsionam sua adoção em diferentes áreas (BRANCO; TEFFÉ, 2022, p. 13)

3. METODOLOGIA

A pesquisa segue de modo exploratório e descritivo, ao buscar compreender e detalhar como técnicas de Inteligência Artificial vêm sendo aplicadas na perícia digital para investigação de atividades ilícitas.

Quanto à abordagem, será uma pesquisa qualitativa. A abordagem utiliza a análise de conceitos, técnicas e estudos de caso e a avaliação de desempenho de ferramentas de IA aplicadas à detecção de evidências digitais.

- **Coleta de Dados**

A coleta de dados foi realizada por meio de várias estratégias:

- **Pesquisa bibliográfica:** análise de artigos científicos, livros e publicações, abordando inteligência artificial e perícia digital.
- **Análise documental:** estudo de relatórios técnicos, normas e diretrizes relacionadas à computação forense.
- **Estudo de caso:** análise de cenários de investigação digital envolvendo crimes cibernéticos.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Os instrumentos utilizados incluem softwares de análise forense digital, bases de dados públicas e algoritmos de aprendizado de máquina.

- **Amostra**

A pesquisa compreende estudos, ferramentas e aplicações de Inteligência Artificial no contexto da perícia digital.

A amostra foi definida de forma não probabilística por conveniência, incluindo:

Artigos publicados nos últimos 3 a 5 anos;

Ferramentas de IA amplamente utilizadas ou relevantes;

Casos documentados de uso de IA em investigações digitais.

- **Análise de Dados**

Os dados coletados foram analisados por meio de:

- **Análise de conteúdo:** para interpretar os dados qualitativos provenientes da literatura e estudos de caso;
- **Estatística descritiva:** para avaliar métricas como precisão, acurácia e taxa de detecção dos modelos de IA;
- **Comparação de desempenho** entre diferentes técnicas de Inteligência Artificial aplicadas à perícia digital.

- **Procedimentos**

A pesquisa foi conduzida seguindo as etapas abaixo:

1. Definição do tema e do problema de pesquisa relacionados ao uso de Inteligência Artificial na perícia digital.
2. Levantamento bibliográfico em bases científicas relevantes.
3. Seleção e análise dos materiais com base em critérios de relevância e atualidade.
4. Identificação das principais técnicas de IA utilizadas na investigação digital (como aprendizado de máquina e redes neurais).
5. Coleta e organização dos resultados obtidos.
6. Análise e interpretação dos dados com base nos métodos definidos.
7. Elaboração das conclusões, destacando contribuições, limitações e possibilidades futuras.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Aplicações da IA na Análise Forense

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

A aplicação prática da IA não vai substituir o perito, que permanece central na investigação, mas sim dotá-lo de uma capacidade de resumir e de conexão sem precedentes e ágil. A função principal da ciência forense é a materialização da prova digital, e a IA potencializa essa missão em quatro frentes críticas:

1. Análise de Logs: Os logs são a "espinha dorsal" da investigação, mas sua interpretação é extremamente difícil devido ao estado bruto dos dados. Wendt e Jorge (2013, p. 130) comparam: "O log é o equivalente cibernético dos registros mantidos pela companhia telefônica, porém com uma leitura um pouco diferenciada, pois enquanto estes são apresentados organizadamente, os logs são apresentados de uma forma mais bruta e desorganizada, sendo necessário um esforço maior para serem interpretados." A IA permite cruzar logs de eventos de sistemas distintos (Windows, Apache, firewalls) para identificar padrões de invasão de forma instantânea.

2. Análise de Memória (RAM): Por ser volátil, a RAM guarda evidências que desaparecem no desligamento do sistema. Conforme Eleutério e Machado (2011, p. 27): "A memória RAM é volátil, e seus dados são perdidos quando o computador é desligado. Assim, caso o perito suspeite que evidências estejam contidas nesse tipo de memória, ferramentas próprias podem ser utilizadas para realizar tal cópia." A IA brilha ao identificar injeções de código e artefatos de malware escondidos em dumps de memória que ferramentas baseadas somente em assinaturas estáticas deixariam passar.

3. Análise de Tráfego de Rede: Através do monitoramento de pacotes, os sniffers capturam evidências em trânsito. Segundo Wendt e Jorge (2013, p. 34), eles "possuem a finalidade de monitorar todo o tráfego da rede, de modo que todos os dados transmitidos por ela possam ser interceptados e analisados." Modelos de IA podem traduzir arquivos PCAP complexos em descrições narrativas, apontando tentativas de exfiltração de dados por protocolos incomuns.

4. Interpretação e Correlação Automatizada: A IA atua como um "filtro inteligente", separando o ruído do sinal. Como descrevem Wendt e Jorge (2013, p. 215), "Desta forma, o perito tem condições de filtrar melhor as informações e gerar um laudo com mais resultados úteis." Ela consegue fazer a conexão de um arquivo deletado em um horário específico, possuindo ligação direta com um processo que rodou na memória minutos depois, facilitando a missão do perito que, segundo Soares (2019, p. 41), é a de "determinar toda a dinâmica da autoria dos ilícitos".

4.2 Utilização de Prompts e Automação de Investigação

Porém, a eficácia da IA generativa depende diretamente da qualidade da interação humano-máquina. Na perícia, essa interação começa com a formulação técnica dos quesitos. Wendt e Jorge (2013, p. 214) ressaltam: "Portanto, o importante que deve constar no encaminhamento de solicitação de forense é o seguinte: [...] Quesitos objetivos (na dúvida de elaboração, conversar previamente com o perito)."

Na automação, a engenharia de prompts tornou-se uma habilidade técnica essencial. Não basta solicitar uma análise; é preciso saber estruturar consultas que forcem a IA a seguir metodologias como a *Chain of Thought* (Cadeia de Pensamento). Isso permite configurar varreduras automatizadas em busca de persistência de malware ou análises contextuais de comandos PowerShell.

Um exemplo atual é a transcrição automatizada de mídias para facilitar a busca por palavras-chave. Conforme observado em decisões judiciais citadas por Costa e Feller (2025, p. 11):

"A fim de facilitar as buscas e a visualização do conteúdo das mensagens de voz dos aplicativos WhatsApp e WhatsApp Business, foi gerada, automatizadamente, uma transcrição aproximada dos arquivos de áudio com o uso de ferramentas baseadas em inteligência artificial."

Além disso, a IA surge como ferramenta de apoio à decisão judicial. Toledo (2021, p. 71–72) discute o uso de programas de IA para orientar o juiz na aplicação de penas, baseando-se em perfis de reincidência, embora sublinhe que "quem prolatou a sentença é o juiz". No entanto, a automação não retira o fator humano na reconstrução da narrativa. Como explicam Padilha et al. (2021, p. 112), "o papel do perito é reconstruir a narrativa do evento a partir dos dados organizados [...] tarefa dificultada pelo volume de dados que supera em muito a capacidade humana de análise."

4.2.1 Análise de evidências com prompt

- **Dump de processos de memória**

A análise forense de memória é uma técnica essencial para identificar processos ativos, comportamentos suspeitos e possíveis ameaças em sistemas computacionais. Foi utilizada a ferramenta Volatility para examinar a árvore de processos de um sistema Windows, visando detectar indícios de atividades maliciosas e compreender o estado do ambiente analisado.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

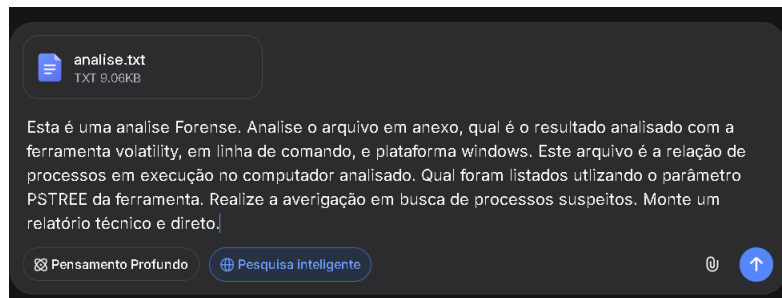


Figura 2: Prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Na figura 2, foi realizada uma análise forense digital utilizando um arquivo chamado “analise.txt”, com o objetivo de examinar os resultados obtidos pela Volatility no sistema operacional Windows. O texto apresenta que o arquivo contém uma relação de processos em execução no computador analisado, listados por meio do comando PSTREE. Esse comando é utilizado para organizar os processos em formato de árvore, permitindo visualizar a hierarquia entre eles. Essa atividade consiste em verificar possíveis processos suspeitos, identificando comportamentos incomuns ou indícios de malware. Além disso, é solicitado o desenvolvimento de um relatório técnico e direto com base nos resultados encontrados. A análise busca reconhecer processos ocultos, duplicados ou executados anormalmente.

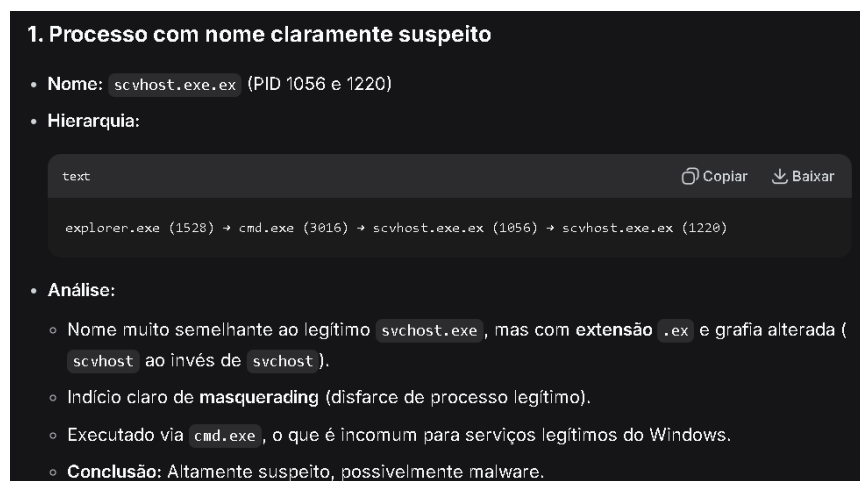


Figura 3: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Como na Figura 3, a IA mostra a identificação de um processo suspeito durante uma análise forense de memória. O processo possui o nome “scvhost.exe.ex” e está executado nos PIDs 1056 e 1220. A suspeita ocorre porque o nome é muito parecido com o processo legítimo do Windows chamado svchost.exe, técnica conhecida como masquerading, utilizada por malwares para

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

enganar usuários e analistas, disfarçando arquivos, processos ou programas maliciosos como se fossem legítimos. A hierarquia indica que o processo foi iniciado a partir do cmd.exe, algo incomum para serviços do Windows, iniciados pelo sistema operacional. O caminho mostrado na árvore de processos foi:

- **explorer.exe → cmd.exe → scvhost.exe.ex → scvhost.exe.ex.**

Além disso, a extensão “.ex” e a alteração na grafia (“scvhost” em vez de “svchost”) mostram um comportamento talvez malicioso e apontam que o processo é altamente suspeito e possivelmente um malware em execução no computador investigado.

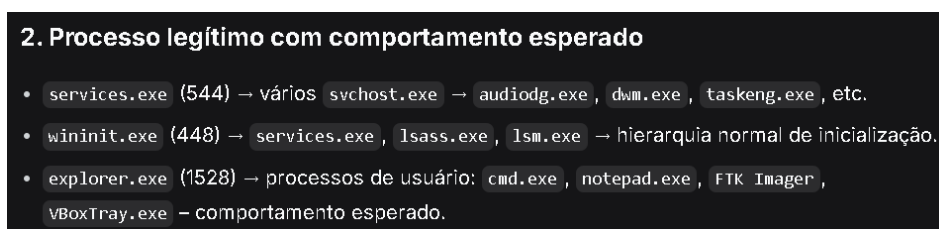


Figura 4: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Já a Figura 4 mostra exemplos de processos do Windows considerados normais durante uma análise forense, demonstrando como funciona a hierarquia padrão dos processos do Windows para diferenciar atividades legítimas de possíveis ameaças.

O processo `services.exe` aparece iniciando vários processos `svchost.exe`, assim como outros componentes comuns do sistema, como `audiodg.exe`, `dwm.exe` e `taskeng.exe`, mostrando o funcionamento esperado dos serviços do Windows.

Também é mostrada a sequência de inicialização do processo: `wininit.exe` → `services.exe`, `lsass.exe` e `lsim.exe`, a qual é uma hierarquia normal do processo de boot do Windows. Já na parte do usuário, o processo `explorer.exe` inicia aplicações comuns como `cmd.exe`, `notepad.exe`, `FTK Imager` e `VBoxTray.exe`, um comportamento típico de atividades normais do usuário e de ferramentas.

A análise conclui que esses processos não apresentam indícios suspeitos, ao seguirem padrões normais e esperados do sistema operacional.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Conclusão / Recomendações			
Processo	PID	Indício	Ação recomendada
svchost.exe.exe	1056, 1220	Nome enganoso, execução via cmd	Coletar binário, analisar conexões de rede, verificar persistência

Figura 5: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

E, por fim, na Figura 5, a IA recomenda que, sempre que desconfiar de um processo suspeito, coletar o arquivo para análise (ver se é vírus mesmo), verificar se tem conexões de rede (pode estar enviando dados ou recebendo comandos), e checar a persistência dele com o final do sistema operacional (se ele se reinstala sozinho ao reiniciar o PC).

- **Dump de rede (pcap)**

A análise de tráfego de rede permite identificar atividades suspeitas, tentativas de invasão e comportamentos anômalos em ambientes computacionais. Neste relatório, foi realizada uma investigação forense em um arquivo PCAP capturado pelo Wireshark, com foco na detecção de evidências de reconhecimento de rede e possíveis ataques cibernéticos.

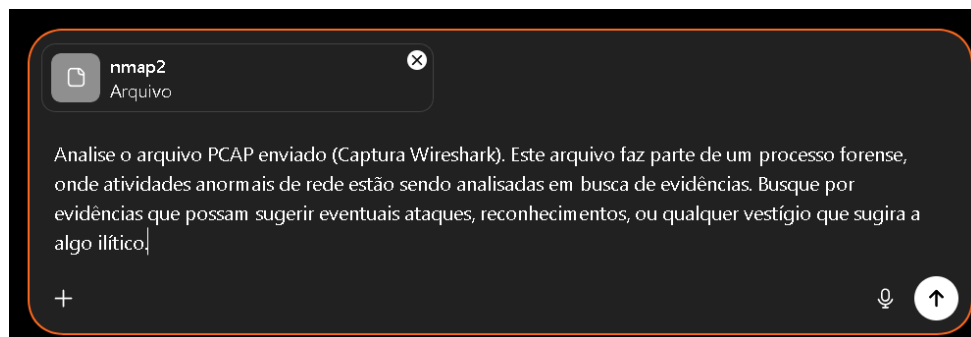


Figura 6: Prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Na Figura 6, foi solicitada pelo prompt uma análise de um arquivo PCAP capturado no Wireshark para realizar uma investigação forense de rede, buscando identificar atividades suspeitas ou possíveis ataques cibernéticos. O texto orienta a procurar evidências de reconhecimento de rede, comportamentos anormais e outros indícios relevantes para a investigação. Como um arquivo nmap2, é uma varredura de portas utilizando a ferramenta Nmap para detectar invasões, tentativas de exploração e movimentações suspeitas na rede.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Evidências Encontradas

1. Descoberta de Hosts via ARP

Foram observadas múltiplas requisições ARP:

Origem	Destino	Tipo
192.168.100.101	192.168.100.102	ARP Request
192.168.100.103	192.168.1.1	ARP Request repetitivo
192.168.100.103	192.168.100.102	ARP Request

Interpretação

Esse comportamento sugere:

- Descoberta de dispositivos ativos na rede;
- Enumeração local da sub-rede;
- Mapeamento de hosts disponíveis.

O volume repetitivo de ARP Requests pode indicar varredura automatizada.

Figura 7: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Já na figura 7, é apresentada uma análise forense de rede relacionada a requisições ARP. Foram identificados vários ARP Requests entre dispositivos da rede, como solicitações repetitivas vindas do IP 192.168.100.103, indicando atividade de descoberta de hosts e enumeração da sub-rede, utilizadas para identificar máquinas ativas. Essas ações podem representar a fase inicial de um possível ataque ou mapeamento da rede.

2. Pacotes TCP Sem Flags (NULL Scan)

Foram identificados pacotes TCP contendo:

- Flags TCP = 0x0000
- Sem SYN, ACK, FIN, RST ou PSH.

Exemplos:

Origem	Destino	Porta Destino
192.168.100.101	192.168.100.102	80
192.168.100.101	192.168.100.102	26114
192.168.100.101	192.168.100.102	26115
192.168.100.101	192.168.100.102	0

Figura 8: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

E na Figura 8, foram identificadas evidências de pacotes TCP sem flags, como um ataque do tipo NULL Scan, em que pacotes são enviados sem as flags TCP padrão, como SYN, ACK, FIN ou RST. É possível identificar portas abertas ou filtrar respostas do alvo, por exemplo, o IP 192.168.100.101 enviando pacotes para várias portas do host 192.168.100.102, incluindo a porta 80.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

3. Porta TCP 0

Foi identificado tráfego direcionado à:

- Porta TCP 0

Relevância

A porta 0 é reservada/inválida e normalmente não é utilizada em aplicações legítimas.

Seu uso costuma estar associado a:

- Testes de pilha TCP;
- Ferramentas de scanning;
- Fingerprinting;
- Atividade maliciosa/anômala.

Figura 9: Resposta do prompt utilizado na IA. Fonte: Elaborada pelo autor (2026).

Por fim, a Figura 9 mostra evidências de tráfego direcionado para a porta TCP 0, a qual é reservada e inválida em comunicações normais, o que é um tráfego não utilizado por aplicações legítimas e pode indicar atividades suspeitas. O uso da porta 0 está associado a testes de pilha TCP, ferramentas de varredura e técnicas de fingerprinting para identificar sistemas e serviços. Já em análises forenses, esse comportamento é tratado como um possível indício de reconhecimento de rede ou atividade maliciosa/anômala.

4.3 Integração de ferramentas forenses com IA

A computação forense atravessa um momento vindo de diversas evoluções e técnicas. A complexidade e o volume das ameaças atuais exigem que as instituições não sejam espectadoras, mas agentes ativos e em constante evolução. Como bem apontam Wendt e Jorge (2013, p. 13), "[...] os órgãos de segurança pública com a incumbência de promover a investigação criminal [...] devem ser instrumentalizados para enfrentar com eficiência e proatividade as ciberameaças e programar um planejamento estratégico [...]".

Este planejamento passa, obrigatoriamente, pela junção entre o rigor metodológico e a inovação tecnológica. A integração entre ferramentas periciais, como o Autopsy e o The Sleuth Kit, e modelos de linguagem de grande escala (LLMs), como ChatGPT e Claude, muda a dinâmica de investigação. O ponto de inflexão atual é o uso de protocolos como o MCP Server (Model Context Protocol). Através dele, o perito deixa de somente realizar tarefas manuais e gera um fluxo inteligente onde a IA "lê" o contexto dos artefatos.

Essa mudança foi necessária pelo grande volume de dados — o Big Data — que superou a capacidade humana. É aqui que a Inteligência Artificial se torna indispensável. Toledo (2021, p. 59) define a IA como um "ramo científico específico que tem por tarefa a simulação computacional da inteligência humana, entendida enquanto capacidade de apreender e organizar dados de uma situação". No fluxo de integração, a IA atua como um analista de nível 1, filtrando ruídos e identificando anomalias em uma

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

velocidade humanamente impossível. Norte Filho et al. (2026, p. 3) sintetizam esse papel:

"A inteligência artificial (IA) assume papel de destaque como instrumento potencialmente capaz de aprimorar a atuação estatal na persecução penal. Por meio de técnicas avançadas de análise de dados, aprendizado de máquina e reconhecimento de padrões, a IA possibilita o tratamento automatizado de grandes volumes de informações, contribuindo para a identificação de comportamentos suspeitos e para a articulação de dados provenientes de múltiplas fontes digitais."

Portanto, a integração não é uma escolha técnica, mas uma necessidade imposta pela evolução tecnológica, visando à eficiência que a justiça moderna exige.

4.4 Integração Autopsy e Claude com MCP

Como parte da apresentação de resultados, será apresentado o modelo de integração de ferramenta forense, com imagem indexada e IA em estado da arte. Com relação ao Procedimento Forense, como exposto no Tópico 2.1, altera-se o Passo 5, onde a IA é aplicada como ferramenta auxiliar no processo de Análise/Exame, em conjunto com as Ferramentas forenses já utilizadas. Esta alteração de sequência pode ser observada na Figura 10.



Figura 10: Baseado na ISO 27037. Fonte: Elaborada pelo autor (2026).

Para a apresentação de resultados, é utilizada como ferramenta forense o Autopsy, uma base de dados de estudos (container E01), integrada à IA Claude com MCP Server. Cada ponto de estudo será apresentado nos próximos tópicos.

4.4.1 Ambiente de testes

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Para o ambiente de testes de integração, a seguinte configuração foi utilizada, sendo processada 100% em ambiente Windows:

- Sistema Operacional: Windows 11 Education 25H2
- Autopsy versão 4.23.0
- Claude Desktop versão 1.5354.0
- Imagem Forense do Tipo E01

Utiliza-se o plano gratuito para o Claude, demonstrando que podemos ter resultados, mesmo que limitados, utilizando estes planos para validação de integrações, teste de resultados e de uso acadêmico. Limita-se, então, a quantidade de perguntas por sessão, mas este contador é zerado após 2 horas, podendo retomar o chat criado e dar continuidade ao processo de testes.

A Imagem Forense escolhida é um caso fictício disponível na internet, utilizado para treinamentos e ensino acadêmico. Não possuindo, assim, dados sigilosos que não poderiam ser compartilhados com uma IA pública, para o caso de processos investigativos em processo jurídico sendo julgado. Em um cenário real, não é indicada a integração em nuvem pública, sendo um cenário ótimo para a utilização de uma IA local como o Ollama.

4.4.2 MCP Server

O **Model Context Protocol (MCP)** foi desenvolvido pela Anthropic, empresa desenvolvedora da IA Claude, e disponibilizado ao público em novembro de 2024. É um padrão aberto que cria uma ponte segura e direta de via dupla entre fontes de dados e ferramentas de Inteligência Artificial.

Sua estrutura funciona de forma simples: desenvolvedores podem expor seus dados por meio de servidores MCP ou criar aplicações de IA (os clientes MCP) que se conectam a eles. A figura 11 demonstra as possibilidades utilizando o MCP Server como ponte integradora entre fontes externas e IA.

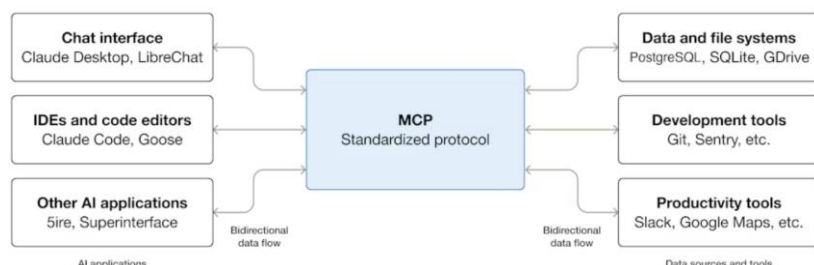


Figura 11: Gráfico de integração MCP (Fonte: <https://modelcontextprotocol.io/docs/getting-started/intro>)

4.4.3 Autopsy integrada ao Claude: Fluxo de Integração

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Na integração entre a ferramenta Autopsy e LLM Claude, temos um ambiente local formado por:

- Claude Desktop: Instalado localmente no equipamento forense e devidamente conectado e autenticado nos servidores da Anthropic. Também parametrizado para utilizar o MCP Server da Ferramenta Autopsy.
- Autopsy: Com o MCP Server ativo e configurado.
- Imagem Forense: Localmente no equipamento e previamente indexada à ferramenta Autopsy.

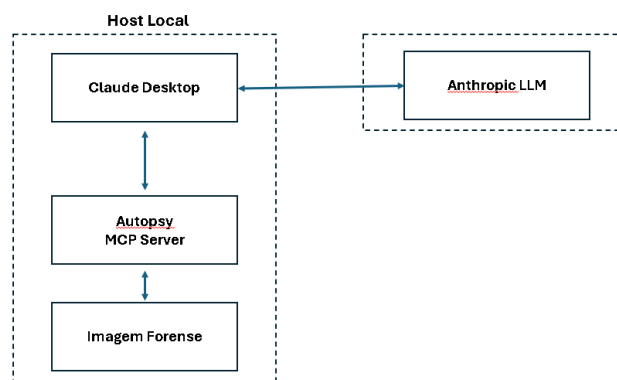


Figura 12: Adaptado de www.cybertriage.com
(Acessado em 23/05/2026)

A partir da versão 4.23.0 da Ferramenta Autopsy, é disponibilizada a integração via MCP com LLM que suporta a comunicação via MCP. É disponibilizado nas Opções de Configuração da Ferramenta o trecho em JSON que deve ser parametrizado na IA em questão.

Para os testes, iremos utilizar o Claude como LLM, que fará a leitura dos dados indexados pela ferramenta Autopsy. A opção de parâmetros é visualizada na figura 13, trecho da função Options da Ferramenta. Nesta tela, temos o trecho em JSON que deverá ser copiado e parametrizado na LLM utilizada.

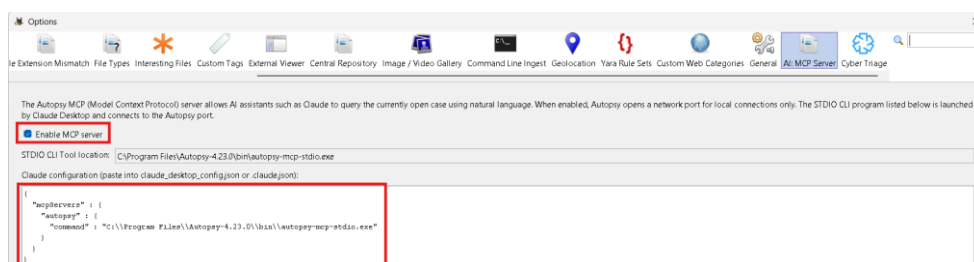


Figura 13: MCP server na Ferramenta Autopsy, e trecho do JSON qual aponta para a aplicação MCP. Fonte: Elaborada pelo autor (2026).

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Neste trecho de código, é apontado o local do executável **autopsy-mcp.stdio.exe**. Este aplicativo permite que uma LLM realize chamadas a uma aplicação. O Claude Desktop se comunica com a Autopsy via STDIO e ele atua como um meio de transporte entre o Claude Desktop e o aplicativo Autopsy em execução. Exemplifica-se a arquitetura na figura 12.

Este JSON é parametrizado em um arquivo chamado **claude_desktop_config.json** na aplicação Claude instalada no equipamento no qual está a imagem a ser analisada na Autopsy. E pode variar de acordo com a LLM utilizada. A localização do arquivo pode variar entre os sistemas operacionais utilizados. Este JSON aponta para um executável da ferramenta Autopsy, no caso, o **autopsy-mcp.stdio.exe**.

As chamadas que a LLM realiza no aplicativo **autopsy-mcp.stdio.exe**, no caso desta integração, permitem que a IA utilizada interaja com a aplicação, no caso o Autopsy, e é possível assim realizar consultas via prompt como:

- Quais são os usuários do sistema operacional analisado na imagem do Autopsy?
- Quantas unidades de disco são listadas?
- Na pasta Meus Documentos, existem arquivos relevantes para uma investigação criminal? O que pode ser considerado suspeito?
- Existem arquivos criptografados em alguma unidade?

A conexão é realizada através da porta 8743 (sleuthkit.org acessado em 23/05/2026), aberta pelo Autopsy caso esteja parametrizado para disponibilizar a porta automaticamente. É gerado um token criptográfico a cada conexão; conexões sem token são rejeitadas, mantendo a integridade da conexão (sleuthkit.org, acessado em 24/05/2026). É visualizado na Figura 14 o processo de integração.

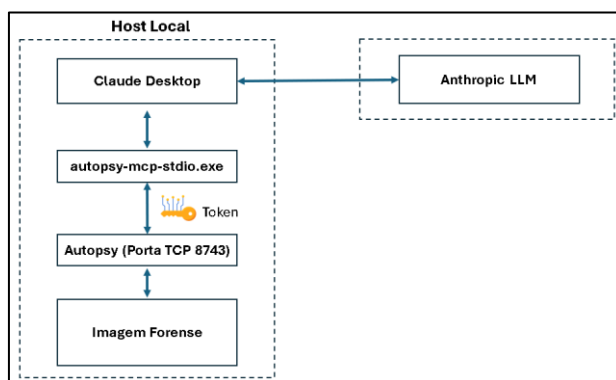


Figura 14: Processo de integração via MCP adaptado de www.cybertriage.com (2026)

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Realizados os parâmetros, estando a ferramenta Autopsy aberta, com a imagem em questão indexada, pode-se iniciar os prompts. A Figura 15 demonstra o prompt “Existe uma imagem aberta no Aplicativo Autopsy?” e o retorno do Claude solicitando a requisição de status da ferramenta, onde se pode sempre permitir, permitir somente uma vez ou negar.

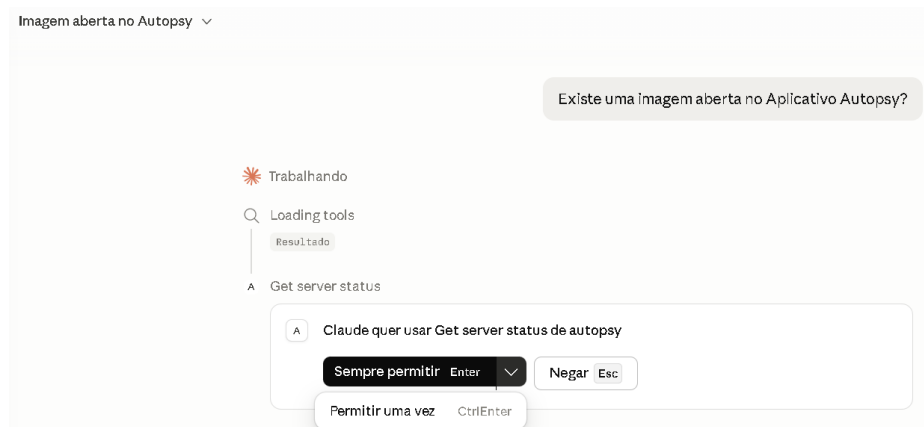


Figura 15: Solicitação de verificação da integração com MCP Server da Ferramenta. Fonte: Elaborada pelo autor (2026).

Permitindo o acesso, tem-se a primeira resposta positiva validando a integração da LLM com a ferramenta e a base de dados em questão, como demonstrado pela Figura 16. A partir deste ponto, é possível interagir com a base de dados a partir de prompts.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

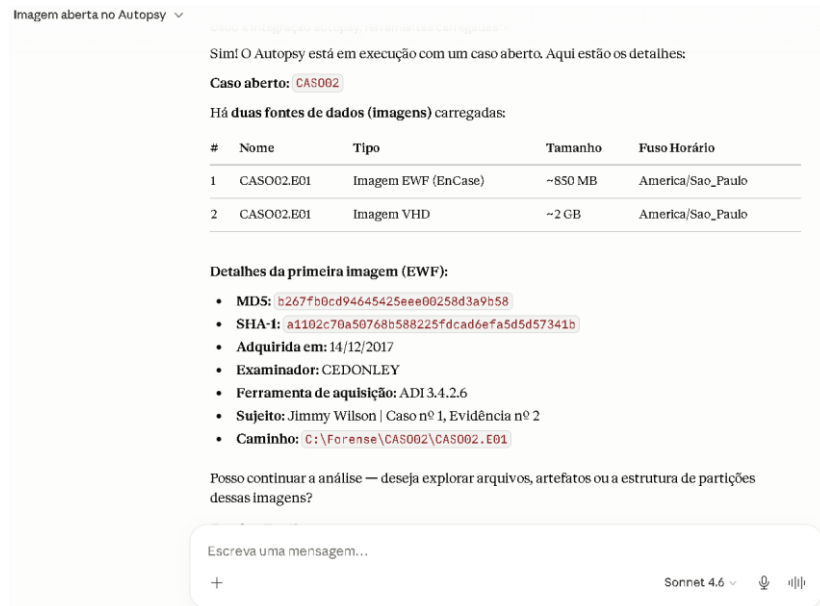


Figura 16: Resposta da verificação da Integração com MCP Server. Fonte: Elaborada pelo autor (2026).

Em outro teste, foi solicitada novamente à IA (Claude) a verificação sobre a conexão com a ferramenta Autopsy, e obtivemos outro tipo de retorno embasado em sugestões para interação com a imagem forense, como exposto na figura 17. Este tipo de sugestão auxilia o perito em questão com insights que podem ser praticados com a imagem em questão.

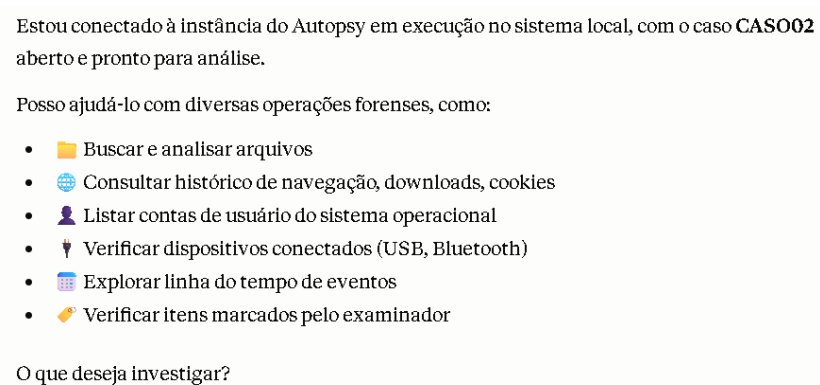


Figura 17: Insights da IA com relação a imagem a ser exploradas. Fonte: Elaborada pelo autor (2026).

Partindo para novos testes, sugeriu-se a partir do prompt da IA que fosse efetuada uma checagem das unidades de disco indexadas na Imagem Forense, bem como a quantidade de partições, dados sobre o sistema operacional e as datas de instalação e o último dia em que este sistema foi utilizado. Como demonstrado na figura 18.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Efetue uma checagem sobre as unidades disponíveis na imagem, quantidade de partições. Qual é o sistema operacional instalado e quando foi instalado. Também a data da última vez que foi ligado.

Figura 18: Prompt para investigação sobre dados do SO da imagem. Fonte: Elaborada pelo autor (2026).

Foi gerado um relatório gráfico, sem intervenção do usuário, com os dados solicitados, sendo complementado com mais informações pertinentes, correlacionando os prompts executados com procedimentos de perícia em sistemas operacionais, sendo demonstrado pelas figuras 19 e 20. As informações fornecidas pela IA complementam a necessidade do perito forense.

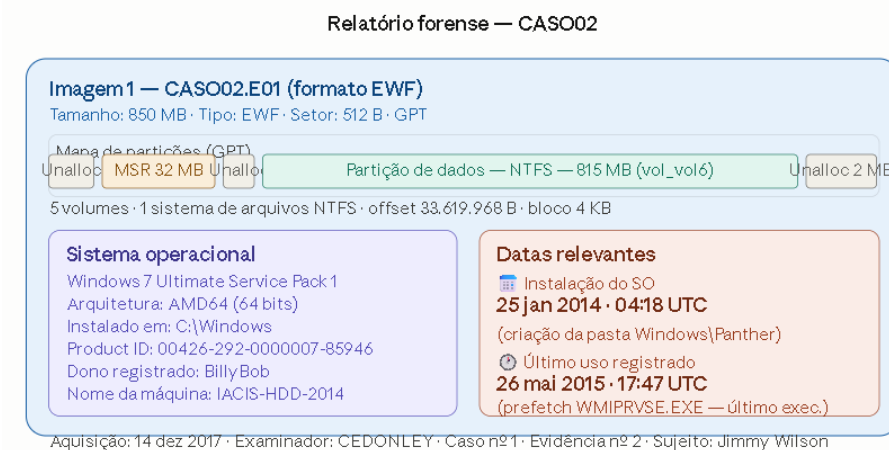


Figura 19: Relatório gráfico gerado pela IA. Fonte: Elaborada pelo autor (2026).

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

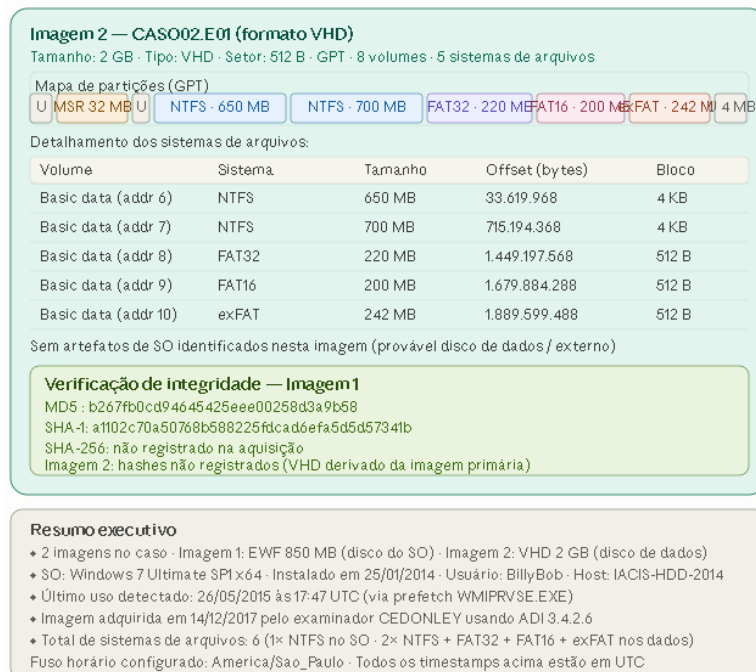


Figura 20: Relatório gráfico gerado pela IA. Fonte: Elaborada pelo autor (2026).

Como resumo, a IA ainda fornece mais dados sobre a imagem analisada, conforme a Figura 21, na qual se relata que foi realizada a aquisição da imagem em 2017 e que o equipamento foi utilizado pela última vez em 2015, havendo, assim, uma lacuna de tempo em que o equipamento não foi utilizado. Eliminando assim possíveis alterações de dados até a data da aquisição.

Estrutura de disco — duas imagens

O caso contém duas imagens derivadas do mesmo arquivo **CAS002.E01**. A primeira, em formato EWF (imagem forense clássica), tem 850 MB e é o disco do sistema operacional. A segunda, em formato VHD, tem 2 GB e parece ser um disco de dados/externo.

Sistema operacional

A Imagem 1 contém o Windows 7 Ultimate Service Pack 1, 64 bits, instalado em **C:\Windows**. O usuário registrado é **BillyBob** e o nome da máquina é **IACIS-HDD-2014**.

Data de instalação do SO — 25 de janeiro de 2014

Determinada pelo timestamp de criação da pasta **Windows\Panther** (diretório gerado exclusivamente durante o processo de instalação do Windows): **2014-01-25T04:18:02Z**.

Último uso registrado — 26 de maio de 2015 às 17:47 UTC

O prefetch do processo **WMIPRVSE.EXE** apresenta o timestamp mais recente de todo o caso. Também há intensa atividade no registro SYSTEM (**2015-05-26T13:05:11Z**) e em arquivos do NTFS nessa mesma data — consistente com o último boot e uso do sistema.

Vale observar que a imagem foi adquirida apenas em dezembro de 2017, ou seja, o sistema ficou armazenado sem uso por cerca de 2,5 anos antes da coleta forense.

Figura 21: Resumo sobre dados do equipamento. Fonte: Elaborada pelo autor (2026).

4.4.4 Resultados sobre dados de criação de usuários - Timeline

Alguns tipos de consultas serão exemplificados, demonstrando que a LLM consegue rapidamente trazer resultados e efetuar tentativas diferentes da primeira abordagem em busca dos resultados. Quais demandariam um esforço a mais do perito utilizando uma ferramenta padrão de indexação? No exemplo da Figura 22, foi questionado:

- *Quais são os usuários do sistema operacional em questão, sua data de criação, seu último logon, se possui senha e qual a frase de segurança para recuperação da senha?*

Alguns destes dados poderiam ser adquiridos mediante análise do Autopsy e análise dos arquivos de registro do Windows (NTUSER.DAT e UsrClass.dat), realizando a exportação e posterior leitura. A resposta da LLM trouxe todos os tópicos questionados, no exemplo das Figuras 22 e 23, e complementou com mais dados, como: quais eram os usuários administradores, quantidade de logons, se a senha expira, SID do usuário e Status da Conta.

Aqui está o levantamento completo dos usuários do sistema operacional encontrados no caso CASO02:

👤 Contas de Usuário (Relevantes para Investigação)					
Campo	administrator	guest	billybob	sgt. joe t. nameless	jimmy wilson
Nome Completo	—	—	—	Sgt. Joe T. Nameless	Jimmy Wilson
SID	...-500	...-501	...-1001	...-1003	...-1004
Criação da Conta	25/01/2014 04:24 UTC	25/01/2014 04:24 UTC	25/01/2014 01:27 UTC	25/01/2014 15:27 UTC	25/01/2014 15:30 UTC
Último Logon	21/11/2010 01:47 BRST	(sem logon)	20/02/2014 14:46 BRT	07/02/2014 15:34 BRST	19/02/2014 10:30 BRT
Qtd. de Logons	6	0	21	18	13
Senha Necessária	Não	Não	Não	Sim	Sim
Senha Expira	Não	Não	Não	Não	Não
Dica/Frase de Recuperação	(nenhuma)	(nenhuma)	"A NUMBER"	"Backward #"	"safeone"
Administrador	✅ Sim	❌ Não	✅ Sim	✅ Sim	✅ Sim
Status da Conta	Desabilitada	Desabilitada	Ativa	Ativa	Ativa

Figura 22: Retorno do prompt executado. Fonte: Elaborada pelo autor (2026).

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

 Destaques Forenses

- **billybob** é o usuário com **mais logons (21)** e o último acesso mais recente entre os três ativos, sendo potencialmente o usuário principal do sistema. A dica de senha é **"A NUMBER"**.
- **jimmy wilson** é justamente o sujeito identificado na aquisição da imagem. Sua dica de senha é **"safeone"**.
- **sgt. joe t. nameless** possui dica de senha **"Backward #"** e realizou 18 logons.
- As contas **administrator** e **guest** estão **desabilitadas**.
- Houve falha de autenticação registrada para **billybob** em 11/02/2014 e para **sgt. joe t. nameless** em 25/01/2014.

Figura 23: Resumo do prompt executado. Fonte: Elaborada pelo autor (2026).

Em um próximo teste, foi solicitado à LLM que analisasse as contas de usuário listadas posteriormente e indicou-se qual foi o usuário que criou as contas locais. Neste processamento de prompt, dados do sistema operacional foram lidos, e a LLM correlacionou datas de criação, apontando que o primeiro usuário a ser criado foi billybob. E que supostamente este criou os demais usuários. Como demonstrado na figura 24.

Usou a integração autopsy >

A resposta direta é: o usuário **billybob** criou as três contas.

Há duas evidências que apontam para isso:

1. Registro do Sistema Operacional (TSK_OS_INFO) O campo **TSK_OWNER** do Windows 7 Ultimate instalado na máquina aponta **BillyBob** como o proprietário registrado do sistema operacional. Isso significa que ele foi o primeiro usuário a configurar o sistema.

2. Correlação de timestamps As três contas foram criadas no dia **25/01/2014**, mesmo dia em que o sistema foi configurado. Analisando a sequência:

Conta	Data/Hora de Criação (UTC)
administrator e guest	25/01/2014 às 04:24 (contas padrão do Windows)
billybob	25/01/2014 às 01:27 (primeira conta criada — conta do proprietário)
homegroupuser\$	25/01/2014 às 01:27 (criada automaticamente junto com billybob)
sgt. joe t. nameless	25/01/2014 às 15:27
jimmy wilson	25/01/2014 às 15:30

Figura 24: Retorno do prompt executado. Fonte: Elaborada pelo autor (2026).

A figura 25 mostra a forma como os mesmos dados, ou parcialmente, são visualizados na ferramenta Autopsy. Somente algumas informações, como data de criação, SID e tipo de conta, são apresentadas. Neste sentido, a análise da

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

imagem pela LLM foi mais ampla, mesmo não solicitando dados a mais no prompt.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-67086987-2446681470-237959220-1000			0		CASO02.E01_1 Host	Local		
S-1-5-18				SYSTEM	CASO02.E01_1 Host	Local	NT AUTHORITY	
S-1-5-21-1171287513-3642516788-2358256967-500			0	administrator	CASO02.E01_1 Host	Local		2014-01-25 02:24:46 BRST
S-1-5-21-1171287513-3642516788-2358256967-501			0	guest	CASO02.E01_1 Host	Local		2014-01-25 02:24:46 BRST
S-1-5-21-1171287513-3642516788-2358256967-1001			0	billybob	CASO02.E01_1 Host	Local		2014-01-24 23:27:34 BRST
S-1-5-21-1171287513-3642516788-2358256967-1002			0	homegroupuser\$	CASO02.E01_1 Host	Local		2014-01-24 23:27:37 BRST
S-1-5-21-1171287513-3642516788-2358256967-1003			0	sgt. joe t. nameless	CASO02.E01_1 Host	Local		2014-01-25 13:27:41 BRST
S-1-5-21-1171287513-3642516788-2358256967-1004			0	jimmy wilson	CASO02.E01_1 Host	Local		2014-01-25 13:30:36 BRST
S-1-5-19				LOCAL SERVICE	CASO02.E01_1 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	CASO02.E01_1 Host	Local	NT AUTHORITY	

Figura 25: Dados vistos no Autopsy. Fonte: Elaborada pelo autor (2026).

A LLM sugere a possível cronologia de criação das contas, como especificado na Figura 26, indicando até mesmo o timestamp relativo ao intervalo de horas de criação. Neste ponto, somente foram analisados os dados de registro do Windows, sem aprofundar na leitura de logs de eventos como o Security.evtx.

Billybob foi a primeira conta de usuário criada no sistema (SID terminado em -1001), sendo o proprietário e administrador original. As contas de **Sgt. Joe T. Nameless** (15:27) e **Jimmy Wilson** (15:30) foram criadas sequencialmente cerca de 14 horas depois, em uma sessão logada com a conta **billybob**, que era a única conta ativa e com privilégios de administrador naquele momento.

Figura 26: Análise da LLM com relação as contas criadas. Fonte: Elaborada pelo autor (2026).

Comparando a resposta da LLM com a leitura manual do arquivo de log, por meio da extração do arquivo Security.evtx da Autopsy, e visualização dele no Visualizador de Eventos do Windows da máquina host. Comprova-se que, mesmo sem a leitura dos dados, a cronologia está correta, somente efetuando a leitura dos timestamps. As figuras 27, 28 e 29 demonstram a cronologia de criação de usuários, que estão no log Security.evtx da imagem analisada.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

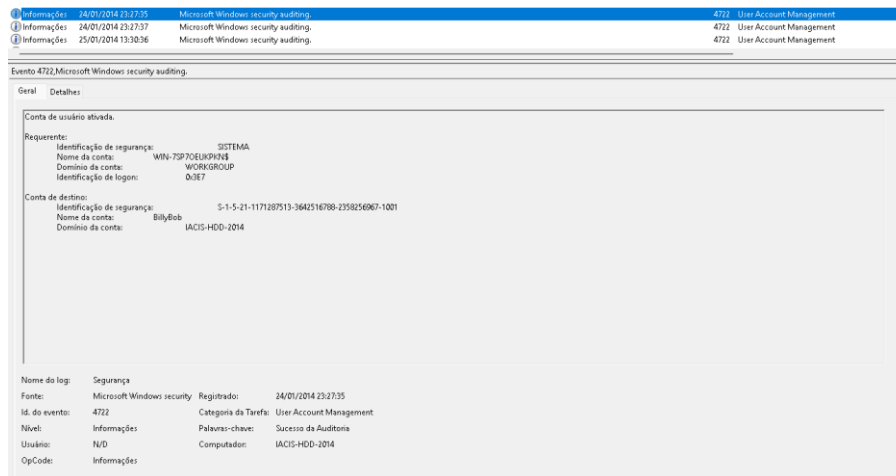


Figura 27: Criação do primeiro usuário BillyBob. Fonte: Elaborada pelo autor (2026).

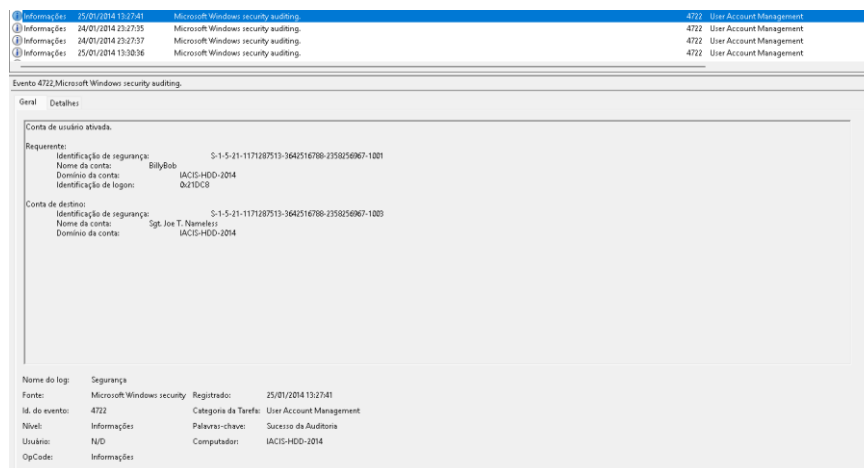


Figura 28: Criação do segundo usuário Sgt. Joe T Nameless por BillyBob. Fonte: Elaborada pelo autor (2026).

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

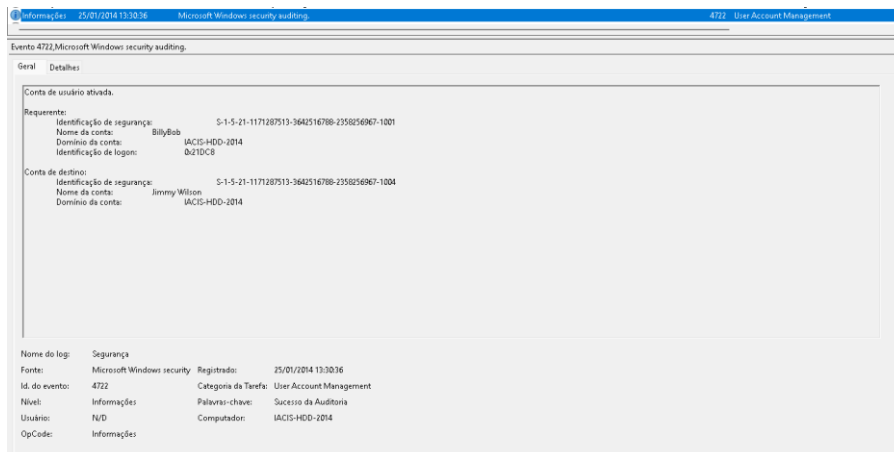


Figura 29: Criação do terceiro usuário, Jimmy Wilson, por Billy Bob.
Fonte: Elaborada pelo autor (2026).

4.4 Limitações, Segurança e Implicações Legais

A digitalização da prova traz uma fragilidade inerente: a facilidade de alteração. Soares (2019, p. 37-38) alerta que "documentos eletrônicos ou arquivos de informática são provas que podem ser modificadas facilmente [...] Há uma dificuldade imensa na comprovação da veracidade". Dessas dificuldades, três grandes desafios se impõem:

1. Privacidade e LGPD: O envio de evidências de IAs em nuvem pode violar a Lei Geral de Proteção de Dados e quebrar toda a cadeia de custódia. O resguardo do sigilo de dados é um direito instrumental importante para o Judiciário que, segundo Wendt e Jorge (2013, p. 125), visa "viabilizar a efetiva realização de direitos individuais relativos à incolumidade da intimidade e da vida privada."

2. O Fenômeno da "Caixa-Preta": A opacidade dos algoritmos desafia o princípio do contraditório. Se o funcionamento da IA é secreto, como contestar os seus resultados? Toledo (2021, p. 67) é enfático ao afirmar que, se os algoritmos e dados não forem acessíveis, "não há como garantir a sua ampla defesa nem o respeito ao contraditório, já que as partes não sabem nem do que se defender". Além disso, existe o risco do "viés algorítmico", onde o código herda preconceitos dos desenvolvedores, gerando resultados inconstitucionais (TOLEDO, 2021, p. 73).

3. Cadeia de Custódia: Para garantir a validade jurídica, o perito deve documentar cada passo. Soares (2019, p. 49) define o passo fundamental: "Um passo importante para o perito é realizar o que se chama de 'cadeia de custódia', sendo a documentação de toda e qualquer operação realizada no material apreendido". A integração da IA deve, portanto, ser acompanhada de uma lógica compreensível e transparente, pois, como reforçam Padilha et al. (2021, p. 128-

129), a limitação na interpretabilidade dos modelos reduz sua aplicação em cenários jurídicos.

5. CONSIDERAÇÕES FINAIS

O avanço da digitalização amplia as ocorrências de crimes cibernéticos, tornando a perícia digital uma atividade mais relevante para a identificação, preservação e análise de evidências eletrônicas. Nesse contexto, esta pesquisa teve como objetivo analisar as aplicações da Inteligência Artificial (IA) na perícia digital voltada à investigação de crimes digitais, identificando suas contribuições, limitações e impactos nos processos investigativos.

Com base na revisão bibliográfica, análise documental e estudo de caso realizado, foi possível verificar que os objetivos propostos foram alcançados. O estudo demonstrou que a Inteligência Artificial possui potencial para otimizar diversas etapas da investigação forense, especialmente na análise automatizada de grandes volumes de dados, detecção de fraudes, reconhecimento de padrões, processamento de linguagem natural, análise de logs e redes, recuperação de evidências digitais e apoio à análise preditiva. Além disso, a pesquisa demonstra que a integração entre ferramentas forenses e modelos de linguagem, pelo uso do protocolo Model Context Protocol (MCP), ajuda nas capacidades analíticas dos peritos e contribui para a redução do tempo necessário para a obtenção de informações.

Entre os principais pontos deste trabalho para a área de Segurança da Informação, destaca-se a demonstração prática de como ferramentas de Inteligência Artificial podem atuar como apoio ao processo pericial, sem substituir a atuação humana. Os resultados obtidos com a interação entre o Autopsy e a IA Claude mostraram que os modelos de linguagem conseguem interpretar dados indexados, correlacionar informações, sugerir linhas de investigação e apresentar resultados de forma mais acessível e organizada. Assim, a pesquisa evidencia o entendimento sobre o uso de tecnologias inteligentes na computação forense e incentiva novas iniciativas de modernização dos processos investigativos.

Na prática, os resultados obtidos indicam que profissionais da área de Segurança da Informação, peritos digitais, investigadores e organizações podem se beneficiar da adoção dessas tecnologias. A automação de tarefas repetitivas permite que os especialistas utilizem seus esforços em análises mais estratégicas e complexas, aumentando a produtividade e a eficiência das investigações. Além disso, a utilização de sistemas inteligentes pode auxiliar organizações na identificação de incidentes de segurança, no combate a fraudes e na resposta mais rápida aos ataques cibernéticos. Porém, a adoção desses sistemas deve ocorrer de forma responsável, observando requisitos de privacidade, proteção de dados, transparência e preservação da cadeia de custódia das evidências digitais.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Apesar dos benefícios, o estudo também identificou limitações importantes. Entre elas destacam-se a dependência da qualidade dos dados analisados, os riscos associados ao algoritmo, a dificuldade de interpretação de decisões geradas por modelos complexos e os desafios jurídicos relacionados à razão das evidências produzidas com auxílio da Inteligência Artificial. Tais fatores reforçam a supervisão humana e a validação dos resultados apresentados pelas ferramentas automatizadas.

Para sugestões para trabalhos futuros, recomenda-se realizar estudos experimentais envolvendo diferentes ferramentas forenses integradas a modelos de Inteligência Artificial, bem como a comparação entre soluções locais e serviços baseados em nuvem. Também são importantes pesquisas voltadas à aplicação de modelos de IA especializados em análise de malware, investigação de dispositivos móveis, análise de tráfego de rede em tempo real e identificação de deepfakes. Além disso, estudos sobre governança, ética, conformidade legal e preservação da cadeia de custódia em ambientes apoiados por Inteligência Artificial poderão contribuir para uma adoção mais segura e confiável dessas tecnologias na área forense.

Por fim, concluo que a Inteligência Artificial representa uma importante aliada da perícia digital moderna, oferecendo recursos capazes de ampliar a capacidade dos profissionais e enfrentar os desafios pelo crescente volume de dados presentes nas investigações digitais. Entretanto, sua utilização deve ocorrer como ferramenta complementar ao trabalho do perito, preservando os princípios técnicos, éticos e legais que garantem a confiabilidade das evidências e a efetividade da justiça.

REFERÊNCIAS

BRANCO, Sérgio; **TEFFÉ**, Chiara Spadaccini de (coords.). *Inteligência artificial e big data: diálogos da pós-graduação em direito digital*. Rio de Janeiro: Instituto de Tecnologia e Sociedade, 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. *Procedimentos operacionais padrão: perícia criminal – informática forense*. v. 5. Brasília: SENASP/MJSP, 2024.

COSTA, Mauir Victor da Silva; **FELLER**, Thiago de Almeida. O uso da inteligência artificial na investigação criminal. *Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)*, São Paulo, v. 11, n. 11, nov. 2025.

COZMAN, Fabio G.; **PLONSKI**, Guilherme Ary; **NERI**, Hugo (orgs.). *Inteligência artificial: avanços e tendências*. São Paulo: Instituto de Estudos Avançados da USP, 2021.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

ELEUTÉRIO, Pedro Monteiro da Silva; **MACHADO**, Marcio Pereira. *Desvendando a computação forense*. São Paulo: Novatec, 2011.

GOMES DA COSTA, Carlos Zoete; **ABREU**, Daniel Quintaneiro. O uso de inteligência artificial na análise de documentos forenses: uma revisão sistemática. *Revista Base Científica*, v. 2, p. 01-20, 2024.

MAIA, Francisco Sílvio. *Criminalística geral*. Fortaleza: [s.n.], 2012.

NORTE FILHO, Antônio Ferreira do et al. A aplicação da inteligência artificial na investigação de crimes cibernéticos: avanços tecnológicos e impactos no sistema jurídico-forense. *REMUNOM*, v. 13.05, 2026.

OETTINGER, William. *Aprenda computação forense: um guia para iniciantes para buscar, analisar e proteger evidências digitais*. Tradução de Lúcia A. Kinoshita. São Paulo: Novatec Editora, 2021.

PADILHA, Rafael et al. A Inteligência Artificial e os desafios da Ciência Forense Digital no século XXI. *Estudos Avançados*, v. 35, n. 101, 2021.

PAULA, Washington X. de. *Noções de criminalística*. [S.l.: s.n., s.d.].

PEDÁGIO. In: PEIXOTO, Fabiano Hartmann (org.). *Inteligência Artificial: Estudos de Inteligência Artificial*. Curitiba: Alteridade Editora, 2021. v. 4, p. 57-85. (Coleção Direito, Racionalidade e Inteligência Artificial).

SLEUTH KIT LABS. *Autopsy User Documentation 4.23.0 – Claude MCP Integration*. Disponível em: Sleuth Kit Documentation. Acesso em: 23 mai. 2026.

SLEUTH KIT LABS. *Cyber Triage*. Disponível em: Cyber Triage Official Website. Acesso em: 23 mai. 2026.

SOARES, Fábio Nunes. *Investigação: crimes cibernéticos e computação forense*. Rio de Janeiro: SESES, 2019.

WENDT, Emerson; **JORGE**, Higor Vinicius Nogueira. *Crimes cibernéticos: ameaças e procedimentos de investigação*. 2. ed. Rio de Janeiro: Brasport, 2013.