Fontes Abertas de Inteligência (OSINT): Estratégias para Garantir a Integridade e Admissibilidade em Investigações Forenses Digitais.

Lucas da Silva Souza – lucassouza.py@gmail.com
Computação Forense e Segurança da Informação
Instituto de Pós-Graduação - IPOG
Vilhena, RO, 26/02/2024

Resumo
Este estudo explora as técnicas e fontes de coleta de informações em fontes abertas de inteligência (OSINT) e as estratégias necessárias para garantir sua integridade e admissibilidade como prova pericial em processos judiciais. A pergunta central desta pesquisa é: como assegurar a integridade das informações obtidas por OSINT para que possam ser aceitas como evidências digitais? A hipótese sugere que a aplicação de protocolos rigorosos de preservação e verificação, como o uso de ferramentas especializadas e a adesão a normas internacionais e à legislação brasileira, pode garantir a integridade e credibilidade dessas informações. Para alcançar os objetivos, foi realizada uma revisão bibliográfica de literaturas especializadas e foram analisados os principais métodos de coleta de OSINT, utilização de técnicas de preservação baseadas na norma ISO/IEC 27037, como o uso ferramentas técnicas de captura e preservação, como a Verifact. Os resultados indicam que a implementação de práticas de coleta seguras, aliada ao uso de ferramentas certificadas, fortalece a credibilidade das evidências digitais, garantindo sua validade em tribunais. O estudo conclui que a adoção dessas estratégias contribui para uma justiça mais eficaz e confiável no uso de provas digitais.

***Palavras-chave**: OSINT. Fontes abertas. Provas digitais. Integridade. Admissibilidade.*

1. Introdução

A crescente digitalização da sociedade e o avanço das tecnologias da informação têm proporcionado um acesso sem precedentes a uma vasta quantidade de informações disponíveis online. Nesse contexto, as fontes abertas de inteligência (OSINT), surgem como uma ferramenta fundamental para a coleta de dados relevantes em diversas áreas, incluindo a investigação criminal e a perícia forense. No entanto, a utilização dessas informações como prova pericial requer cuidados especiais para garantir sua integridade e admissibilidade em processos judiciais.

Este trabalho se propõe a investigar algumas das muitas técnicas de coleta de informações em fontes abertas de inteligência (OSINT) e as metodologias utilizadas para assegurar a integridade dessas informações como prova pericial. O objetivo principal é propor estratégias que garantam a confiabilidade e a admissibilidade das evidências digitais coletadas em fontes abertas de inteligência (OSINT) em processos judiciais.

A pesquisa está estruturada em três partes. No primeiro, será feita uma contextualização do tema, delimitando o escopo do estudo e apresentando os diferentes tipos de fontes e inteligência, abordando em seguida a relevância do uso

de fontes abertas de inteligência (OSINT) em processos judiciais. Em seguida, será apresentado diferentes técnicas e casos em que o OSINT pode ser aplicado durante uma investigação. E finalizando, será abordado o problema de pesquisa, centrado na questão de como garantir a integridade das evidencias digitais obtidas em fontes abertas de inteligência para seu uso como prova pericial. As hipóteses levantadas sugerem que a aplicação de métodos de verificação de fontes e protocolos de preservação de evidências digitais são fundamentais para alcançar o objetivo de garantir a integridade e admissibilidade das informações coletadas.

A escolha desse tema se justifica pela sua relevância e impacto na área da segurança digital e da justiça. Com o aumento do uso de evidências digitais em processos judiciais, torna-se essencial compreender e aprimorar as práticas de coleta e preservação dessas informações. A metodologia adotada será uma revisão de literaturas especializadas em OSINT e provas digitais, Serão utilizados métodos de verificação de fontes e protocolos de preservação de evidências digitais, com base no referencial teórico de segurança digital e perícia forense.

2. Desenvolvimento

Método Adotado

A pesquisa proposta, se trata de uma abordagem exploratória, da qual foi adotada uma metodologia que combinou a revisão bibliográfica especializadas em fontes abertas de inteligência (OSINT) e provas digitais, somado ao estudo de casos judiciais dos quais utilizam essas fontes como meio de coleta de evidências.

Em relação à coleta de dados, foram utilizadas fontes bibliográficas, incluindo artigos científicos, livros, teses e dissertações, disponíveis em bases de dados acadêmicas e em bibliotecas virtuais. Os critérios de inclusão dos estudos foram a relevância para o tema proposto e a atualidade das informações apresentadas.

Quanto aos tipos de pesquisa, esta investigação se enquadra como uma pesquisa bibliográfica e documental, uma vez que se baseia na análise de fontes secundárias para abordar o problema de pesquisa proposto. Os instrumentos utilizados incluíram análise de conteúdo para identificar as principais abordagens e perspectivas relacionadas ao tema, bem como técnicas de verificação de fontes para avaliar a credibilidade e a confiabilidade das informações coletadas. A amostra utilizada consistiu em uma seleção de estudos relevantes encontrados durante a revisão das literaturas.

Os dados foram coletados ao longo de um período determinado, utilizando-se recursos online, acesso a bancos de dados acadêmicos e bibliotecas virtuais. A análise dos dados consistiu em uma avaliação qualitativa das informações coletadas, buscando identificar padrões, conceitos, causas e consequências no conhecimento existente sobre o tema.

Os resultados foram apresentados de forma clara e organizada, utilizando-se tabelas e citações diretas e indiretas dos estudos revisados. A interpretação dos dados foi guiada pelo referencial teórico adotado, destacando-se as principais conclusões e contribuições para o campo da segurança digital e da perícia forense.

3. Fundamentação Teórica

Inteligência

Antes de mergulharmos no problema de pesquisa, é importante estabelecer uma base sólida em relação a alguns conceitos e definições pertinentes ao tema central deste trabalho. Um exemplo fundamental é a exploração dos conceitos e definições de inteligência, do qual, segundo CEPIK (2003, p. 27):

> Uma definição ampla diz que inteligência é toda informação coletada, organizada ou analisada para entender as demandas de um tomador de decisões qualquer. Para a ciência da informação, inteligência é uma camada específica de agreção e tratamento analítico em uma pirâmide informacional, formada, na base por dados brutos e, no vértice, por conhecimentos reflexivos.

Outra definição pode ser observada na Doutrina da Atividade de Inteligência, DNISP (2023, p. 44) “A inteligência é o ramo da atividade de inteligência voltado para a função informacional.” Dessa forma, podemos constatar uma equiparação entre as definições na qual ambas empregam a inteligência ao propósito informacional, que tem por objetivo a tomada de decisão, seja ela qual for. Como por exemplo, na defesa dos objetivos fundamentais do Estado, como complementado na DNISP (2023, p. 44):

> Seus profissionais são responsáveis por obter, processar e difundir dados, informações e conhecimentos relativos a fatos, eventos, situações ou fenômenos que se constituam ou indiquem oportunidades e ameaças aos objetivos fundamentais do Estado.

Logo, entende-se que, inteligência é o estado da informação analisada de forma criteriosa, com o objetivo de justificar uma ação, ou seja, a tomada de decisão com base em dados coletados, analisados e interpretados.

Fontes de Inteligência

Observamos anteriormente que, durante o processo de inteligência para a tomada de decisão, é crucial a disponibilidade de dados e informações para análise. Portanto, é fundamental entender o conceito de fontes de inteligência e suas diferentes classificações para que a coleta desses dados e informações possa ocorrer de maneira eficaz.

> Pode-se definir fonte como qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais, e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos, federais, estaduais e municipais). (BARRETO; WENDT; CASELLI, 2017 p. 27)

Uma outra definição, segundo CARVALHO et al. (2023, p. 36) “podemos dizer que fonte é a origem de uma informação. Qualquer dado ou conhecimento que interessa ao profissional de inteligência ou de investigação para a produção de conhecimentos e/ou provas admitidas em juízo.” Esta definição é clara e direta, destacando a origem da informação e sua relevância para profissionais de inteligência ou investigação.

Ambas as definições generalizam a qualidade do dado ou conhecimento obtido de uma fonte, logo, podemos dizer que fonte é qualquer origem que emita dados e informações. De fato, entretanto, de acordo com a DNISP (2023, p. 48) “A classificação pela origem do dado diferencia a produção do conhecimento pelas características das fontes de onde provêm os dados.”

Nesse trecho podemos observar a importância de se classificar as fontes de inteligência de modo que possa tornar compreensível a natureza das informações obtidas no processo de produção de conhecimento, até mesmo para a sua qualificação como uma fonte segura de dados íntegros. Sendo assim, toda fonte pode e deve ser classificada durante um processo de tomada de decisão.

Classificação de Fontes

Referente aos tipos de fontes de inteligência "Podemos classificar as fontes como fechadas (protegidas) ou abertas." (CARVALHO et al., 2023, p. 36). De acordo com essa definição, de maneira bem direta as fontes podem ser divididas entre esses dois tipos, conforme mencionado por Barreto e Wendt (2020, p. 29):

> As chamadas fontes abertas são aquelas de livre acesso, sem obstáculos à obtenção de dados e conhecimentos. [...] fontes fechadas são aquelas cujos dados são protegidos ou negados. O dado protegido é aquele que necessita de credenciamento para acesso. O dado negado é aquele que necessita de uma operação de busca para sua obtenção.

Entretanto de maneira mais abrangente e técnica, a Doutrina da Atividade de Inteligência categoriza as fontes em três, sendo elas, Inteligência de Fontes Humanas, Inteligência de Fontes Técnicas e Inteligência de Fontes Abertas. (DNISP, 2023, p. 48). E ela as define da seguinte maneira.

> A Inteligência de Fontes Humanas (Human Intelligence – Humint) é a inteligência realizada com base em dados obtidos de pessoas. Reúne dados, informações, conhecimentos e percepções originados de relatos feitos por indivíduos de fora do órgão de inteligência ou trazidos por eles.
> [...] A Inteligência de Fontes Técnicas (Technical Intelligence – Techint) é a inteligência realizada com base em dados obtidos por meios técnicos. Reúne informações e dados originados do emprego de equipamentos, que requerem perícia em seu manuseio. Apoia-se em técnicas próprias para análise de cada tipo de insumo obtido. [...] É composta por diversos tipos, cada qual com suas metodologias e técnicas próprias de coleta e processamento de dados. Em um rol não exaustivo de tipos temos: Sigint (Signals Intelligence): Imint (Imagery Intelligence); Geoint (Geospatial Intelligence; e Masint (Measurement Intelligence).
> [...] A Inteligência de Fontes Abertas (Open Source Intelligence – Osint) é a inteligência realizada com base em dados disponíveis, ou seja, de livre acesso. O termo Osint adquiriu relevância com o advento da Internet, mas inclui também outras formas públicas de obtenção de dados. (DNISP, 2023, p. 48)

Nesse ponto, podemos observar que as definições de Carvalho et al. (2023) e Barreto e Wendt (2020) se divergem das classificações de fontes da DNISP, da qual se demonstra mais abrangente proporcionando uma compreensão mais profunda das diferentes metodologias e técnicas envolvidas na coleta de inteligência.

Entretanto, observa-se que, as diferentes definições se complementam ao citar as fontes abertas, da qual, conforme interpretado podemos concluir que se trata de uma fonte sem controles para acesso as informações ou aos dados disponíveis livremente. E é nesse ponto que chegamos ao que conhecemos como OSINT ou Inteligência de Fontes Abertas.

Inteligência de Fontes Abertas (OSINT)

Relacionado a citação anterior, conforme definido pela Doutrina da Atividade de Inteligência, OSINT – Open Source Intelligence ou Inteligência de fontes abertas, é a produção de conhecimento com base em dados públicos e de livre acesso (DNISP, 2023, p. 48).

Pode-se dizer que OSINT é um apanhado de métodos, técnicas e ferramentas de livre acesso, empenhadas a extração e coleta de informações oriundas de fontes abertas aplicadas a produção de inteligência. Essas fontes cuja principal característica é a disponibilidade publica, podendo ser, mídias televisivas, bancos de dados, comerciais, informações bibliográficas, entre outras. Um exemplo que pode ser citado, seria uma simples pesquisa no Google, isso se caracteriza como uma busca de dados via OSINT (LOPES, 2019, p. 12).

Analisando dessa forma, pode se concluir que a Inteligência de Fontes Abertas é algo muito mais comum em nossas vidas do que imaginamos. “O que pode passar despercebido, entretanto é que OSINT significa essencialmente reunir, analisar e disseminar informações. E que essas atividades estão no âmago do que significa ser humano” (CARVALHO et al., 2023, p. 39).

O processo de inteligência para tomada de decisão baseada em informações de fontes abertas está rotineiramente em nossas vidas, pois temos a necessidade de realizar pesquisas e buscas por informações públicas, seja para aprender uma nova habilidade, escolher qual eletrodoméstico tem o melhor custo-benefício ou definir qual é a rota com menos trânsito durante algum percurso. Esses são alguns exemplos que contextualiza a prática de OSINT como uma habilidade essencial em uma sociedade cada vez mais orientada pela informação.

Provas Digitais

O Código de Processo Civil (CPC) define prova como o conjunto de maneiras legalmente aceitáveis e moralmente justificadas pelas quais as partes demonstram a veracidade dos fatos que sustentam seus pedidos ou defesas, influenciando diretamente o convencimento do juiz, (BRASIL, 2015, Art. 369). O CPC regulamenta uma variedade de tipos de provas:

1. **Documental** (BRASIL, 2015, Art. 405 a 429);
2. **Testemunho** (BRASIL, 2015, Art. 442 a 463);
3. **Pericial** (BRASIL, 2015, Art. 464 a 480);
4. **Depoimento pessoal das partes** (BRASIL, 2015, Art. 385 a 388);
5. **Confissão** (BRASIL, 2015, Art. 389 a 395);
6. **Inspeção judicial** (BRASIL, 2015, Art. 481 a 484).

Cada um desses métodos tem suas próprias características quanto à forma de produção, admissibilidade e valor probatório, das quais são essenciais para a instrução adequada do processo e a busca pela verdade dos fatos. Porém, com o advento da internet e todas as novas tecnologias que a acompanha, como redes sociais e aplicativos de mensageria instantânea, as provas passaram a possuir uma nova característica, não mais sendo somente físicas e analógicas, mas também de aspectos intangíveis e digitais, das quais passaram a ser comumente utilizadas e aceitas em processos judiciais.

“No ambiente digital o que se manipula são dados (bits), em geral intangíveis, imateriais e longe do alcance dos modelos analógicos de percepção e de conhecimento da realidade.” (SOUZA; CARVALHO; MUNHOZ, 2023, p. 8).

Provas digitais pode ser definida como “Instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais, ou, se fora deles, esses sirvam como instrumento para sua demonstração” (SOUZA; CARVALHO; MUNHOZ, 2023, apud THAMAY; TAMER 2020 p. 23). Já de acordo Pinheiro:

> É o conjunto de evidências e arquivos eletrônicos que representam a relação e/ou obrigação gerada, acordada ou contratada por uma via digital. O mais importante é que, nessa hipótese, o arquivo original é o digital, sendo qualquer versão impressa cópia, uma vez que não permite perícia. (PINHEIRO, 2021, p. 377)

Conforme podemos observar, para Thamay e Tamer (2020) as de provas digitais possuem semelhanças com as provas tradicionais. Entretanto, o meio digital traz consigo duas situações, a primeira, que uma prova digital pode ser utilizada para a apuração de um fato ocorrido em meios digitais, a segunda, diz que uma prova digital pode ser utilizada para averiguar uma ação não ocorrido necessariamente por meios digitais, mas tem esse como um elemento na apuração dos fatos.

Pinheiro (2021) acrescenta uma importante observação em relação as provas digitais, mencionando devidamente o meio digital como a fonte originaria de uma prova dessa característica, que no âmbito jurídico e das ciências forenses expressa uma gigante significância no saber identificar e preservar a originalidade da prova, garantindo assim a possibilidade da perícia adequada e rigorosa.

4. Resultados e Discussões

Os resultados desta pesquisa foram obtidos a partir de uma revisão bibliográfica, fundamentada em obras de autores especializados em provas digitais, perícia forense computacional e técnicas de investigação que utilizam métodos de coleta de dados baseados na inteligência de fontes abertas.

Este trabalho apresenta e discute os resultados obtidos a partir das revisões bibliográficas, buscando responder à pergunta-problema desta pesquisa: Quais técnicas são utilizadas para a coleta de informações em fontes abertas de inteligência (OSINT), e como garantir a admissibilidade dessas informações como prova pericial durante o processo de investigação digital?

Inicialmente, são exploradas alguns dos principais métodos, técnicas e ferramentas de OSINT identificadas nas literaturas, com ênfase em suas aplicações práticas no contexto de investigações digitais. Em seguida, a discussão se volta para os critérios e métodos que asseguram a admissibilidade dessas informações como prova pericial, destacando os desafios enfrentados e as melhores práticas recomendadas por especialistas. Por fim, a análise crítica dos resultados relaciona as técnicas descritas com a prática forense, sugerindo estratégias para garantir a integridade e confiabilidade das provas digitais oriundas de fontes abertas.

Técnicas de Coleta de Informações em OSINT

As técnicas de OSINT (Open Source Intelligence ou Inteligência de Fontes Abertas) são métodos, procedimentos e ferramentas utilizadas para coletar, analisar e interpretar informações oriundas de fontes públicas. As técnicas apresentadas demonstram de forma clara a capacidade de desenvolvimento de inteligência baseando-se em informações abertamente acessíveis.

Segundo George Kennan (apud. CARVALHO et al., 2023, p. 51) “Eu diria que algo em torno de 95% do que nós precisamos saber poderia muito bem ser obtido por um estudo cuidadoso e competente de fontes perfeitamente legítimas de informações abertas e disponíveis para nós [...]”.

Conforme mencionado por Souza, Carvalho e Munhoz (2023, p.191), diariamente investigadores digitais, desenvolvedores e especialistas em OSINT criam novas soluções. Assim, o número de ferramentas é imensurável. Devido a essa expressiva quantidade, não será possível detalhar todas neste trabalho. Portanto, selecionamos alguns dos principais métodos, técnicas e ferramentas utilizadas durante um processo de inteligência pensadas para reunir informações públicas sobre pessoas e empresas.

Coleta de Inteligência em Fontes Oficiais do Governo

O governo atua como um grande centralizador de dados e informações, muitas das quais podem ser acessadas abertamente através de seus portais oficiais. Essas informações são de extrema importância para a sociedade, incluindo registros de documentos pessoais. Conforme descrito por Carvalho et al. (2023, p. 290):

> O governo cria e mantém registros dos cidadãos que nasceram, vivem ou residem em solo brasileiro. Tomando como base o cidadão brasileiro (nascido no Brasil), entendemos que todos possuem (ou deveriam possuir) documentos nacionais como o Cadastro de Pessoa Física (CPF).

Um exemplo de coleta de inteligência por meio de fontes oficiais do governo seria a necessidade de obter informações sobre um indivíduo a partir de seu CPF. Nesse caso, um método eficaz e confiável de OSINT seria utilizar bases de dados governamentais, como a Receita Federal ou o Portal da Transparência. Essa abordagem permite a coleta de dados relevantes e verificáveis sobre o indivíduo.

Uma das ferramentas disponíveis para essa verificação é o site da Procuradoria Geral da Fazenda Nacional, que permite a consulta e emissão de uma certidão negativa de débitos relativos aos tributos federais e à dívida ativa da União. Através dessa certidão, é possível obter o nome completo da pessoa associada ao CPF, fornecendo uma fonte legítima de identificação.

Ainda utilizando os portais oficiais do governo, poderíamos também realizar buscas sobre empresas, por meio do site Situação Cadastral de Pessoa Jurídica, que nas palavras de Souza, Carvalho e Munhoz (2023, p.196), “Esta página tem como objetivo permitir a emissão do Comprovante de Inscrição e de Situação Cadastral de Pessoa Jurídica pela Internet em consonância com a Instrução Normativa RFB n° 1.863/2018.”

Coleta de Inteligência em Mídias Sociais

As redes sociais desempenham um papel significativo na coleta de informações sobre rotinas, familiares, relacionamentos e muitos outros dados, devido à sua profunda integração com a vida cotidiana e o grande volume de dados gerados diariamente que podem ser úteis para investigadores. Carvalho et al. (2023, p. 393) enfatizam que, devido à ampla conectividade global proporcionada por essas plataformas, o uso de mídias sociais é altamente recomendado para investigações em fontes abertas.

Dentro do contexto das investigações de fontes abertas, a coleta de informações em mídias sociais é denominada SOCMINT (Social Media Intelligence). Como descrevem Carvalho et al. (2023, p. 48), SOCMINT envolve o uso de técnicas e tecnologias para monitorar sites de redes sociais, incluindo a análise de conteúdo como mensagens, imagens e outros dados gerados durante o uso dessas plataformas. Esse tipo de inteligência abrange diversas formas de interação, sejam elas públicas ou privadas, e inclui comunicações entre indivíduos, grupos ou ambos.

Uma das técnicas de Open Source Intelligence (OSINT) amplamente utilizada é a correlação de usernames, também conhecidos como "arrobas" ou nomes de usuários em plataformas digitais. Esta técnica envolve a pesquisa e análise de nomes de usuário para identificar perfis em diferentes redes sociais e plataformas online que compartilham o mesmo nome de usuário.

Uma ferramenta relevante para essa técnica é o WhatsMyName Web, descrito por Souza, Carvalho e Munhoz (2023, p.192) como uma plataforma de busca de nomes de usuários. Esta ferramenta permite verificar a existência de contas em redes sociais e a disponibilidade de nomes de usuários em mais de 200 plataformas diferentes. É utilizada para facilitar a correlação de *usernames* e a identificação de perfis conectados através de diferentes serviços online.

Ainda dentro do contexto de coleta de informações em redes sociais, o Linkedin se destaca como uma plataforma voltada para a atuação profissional, com o objetivo de conectar pessoas e empresas, de acordo com Carvalho et al. (2023, p. 401). O Linkedin é uma ferramenta poderosa para mapear pessoas e suas posições dentro de uma empresa, facilitando a identificação de estruturas organizacionais e conexões profissionais.

Além disso, o Linkedin permite a coleta de dados corporativos valiosos, como informações de contato, incluindo e-mails e números de telefone. Essa capacidade torna a plataforma uma fonte rica para investigações OSINT, especialmente em cenários onde é necessário identificar e conectar informações profissionais e corporativas de indivíduos e organizações.

Coleta de Inteligência em Mecanismos de Buscas

É impossível falar de inteligência em fontes abertas sem mencionar os motores de busca, e lógicamente o mais famoso dentre eles, o Google. Como descrito por Carvalho et al. (2023, p. 313), esses buscadores são ferramentas projetadas para procurar palavras-chave informada por uma pessoa durante uma consulta por documentos, sites, notícias e muito mais.

> Para maior compreensão, segue abaixo o funcionamento: A ferramenta possui “rastreadores” que varrem a web à procura de novos conteúdos ou atualização deles em páginas indexadas. Esses rastreadores podem ser chamados de web crawlers, spider ou bots. Ao identificar as informações, capturam o conteúdo e cadastram os links encontrados em sua base de dados. Em seguida, a página visitada (e rastreada) é indexada no site de busca, podendo ser localizada por qualquer usuário a partir de seu navegador. (CARVALHO et al., 2023 p. 313)

E devido justamente a esse comportamento de varrer a web, identificar e indexar conteúdos que as ferramentas de busca também se tornam fontes para coleta de inteligência, e para otimizar essas consultas podemos utilizar de operadores, conhecidos como Dorks, capazes de filtrar os resultados de maneira inteligente e direta.

> A maior parte das pessoas utilizam os navegadores apenas para buscas simples. Porém, podemos muitas vezes realizar buscas mais complexas e objetivas que nos auxiliem nos processos de OSINT. Esse processo usa operadores para otimizar as buscas [...] (CARVALHO et al., 2023 p. 313)

Os operadores avançados de busca no Google são ferramentas poderosas para refinar consultas e obter resultados específicos de forma mais eficiente. Aqui estão alguns dos mais conhecidos:

1. **intext:** - Esse operador é usado para retornar apenas resultados que contenham o termo especificado no conteúdo da página. Por exemplo, a consulta "intext:OSINT" traria páginas que mencionam a palavra "OSINT" no texto do conteúdo.
2. **intitle:** - Utilizado para filtrar termos que aparecem no título da página. Diferente do intext, que retorna resultados com o termo dentro do conteúdo, intitle:OSINT retornaria apenas páginas onde "OSINT" aparece no título.
3. **filetype:** - Com este operador, é possível buscar por extensões de arquivos específicas, sendo comumente utilizado para identificar vazamentos de arquivos indexados pelo Google. Por exemplo, "filetype:pdf" retornaria apenas documentos em PDF.
4. **inurl:** - Utilizado para filtrar links de sites, esse operador retorna apenas resultados onde o termo especificado está presente na URL. Por exemplo, "inurl:login" mostraria páginas com "login" na URL.
5. **site:** - Esse operador realiza buscas dentro de um domínio específico. A consulta "site:ipog.com.br" retornaria apenas os resultados indexados dentro do domínio "ipog.com.br".

Uma característica interessante é que esses operadores podem ser combinados para criar buscas ainda mais precisas. Por exemplo, a consulta "site:ipog.com.br filetype:pdf intext:CPF" teoricamente retornaria resultados onde arquivos de extensão PDF hospedados no domínio "ipog.com.br" e que contenham o termo "CPF" no conteúdo, desde que estejam indexados.

Os operadores de busca avançada no Google, junto com outras técnicas descritas, são ferramentas valiosas em investigações digitais e na coleta de informações. Eles oferecem métodos eficazes para explorar e filtrar vastas quantidades de dados disponíveis na web, permitindo que investigadores digitais e especialistas em OSINT obtenham insights precisos e relevantes de fontes abertas. A habilidade de combinar esses operadores para refinar consultas e direcionar buscas específicas aumenta significativamente a eficiência e a profundidade das investigações, tornando-os indispensáveis no arsenal de ferramentas de qualquer analista de inteligência.

Admissibilidade das Informações de OSINT como Prova Pericial

Critérios de Admissibilidade Jurídica

Os critérios de admissibilidade jurídica são fundamentais para a aceitação de qualquer prova no âmbito judicial, incluindo aquelas obtidas por meio de OSINT (Open Source Intelligence). Segundo Carvalho et al. (2023 p. 127 apud Oliveira 2019) “[...] em virtude da fragilidade da evidência digital, é necessário padronizar o seu tratamento a fim de garantir sua integridade e autenticidade”.

A autenticidade refere-se à confirmação da origem e autoria das informações, assegurando que os dados realmente provêm da fonte alegada. Para isso, é necessário validar a procedência das informações e associá-las corretamente ao autor ou à entidade responsável. Como destacado por Souza, Carvalho e Munhoz (2023, p. 53), é fundamental documentar a origem digital da prova, como um site, com argumentos que sustentem a confiança em seu conteúdo e eliminem qualquer dúvida quanto à manipulação das informações antes de sua coleta e preservação.

Já a integridade envolve a preservação da completude, imutabilidade, temporalidade e credibilidade das provas. Isso significa que as informações devem estar completas, não alteradas, e que possam ser verificadas em relação ao momento em que foram coletadas. A credibilidade é fundamental para assegurar que os dados são confiáveis e pertinentes ao caso.

A técnica conhecida para assegurar a integridade de uma evidência é por meio de códigos HASH, que funciona como uma “impressão digital” única de uma evidência e que deve ser aplicada no momento da coleta. Funções de hash são capazes de assegurar que determinada prova não foi adulterada após sua coleta, sendo um método confiável e amplamente aceito.

> O código HASH é o resultado de um algoritmo matemático que produz uma sequência de caracteres pequena (normalmente de 32 a 256 caracteres) com base no conteúdo de um determinado arquivo. Caso seja feita qualquer alteração desse conteúdo, a sequência de caracteres sofre uma mudança drástica em seu conteúdo. No que se refere ao seu uso para evidências digitais, também é importante que o algoritmo seja seguro contra “colisões”, que consiste na possibilidade de você ter dois arquivos de conteúdos

> diferentes como o mesmo código gerado. (SOUZA; CARVALHO; MUNHOZ, 2023, p. 61)

Cadeia de Custódia

Para que as informações coletadas de fontes abertas sejam admitidas como provas periciais, elas devem demonstrar clara conexão com o caso, serem apresentadas em seu formato original e sem adulterações, e atender aos padrões legais vigentes. A cadeia de custódia, que garante que as provas foram coletadas, manipuladas, e preservadas de maneira apropriada, também desempenha um papel crucial na determinação da admissibilidade.

A norma ISO/IEC 27037:2013 é um padrão internacional que estabelece diretrizes para a identificação, aquisição e preservação de evidências digitais. Conforme destacado por Carvalho et al. (2023, p. 128), essa norma "tem por finalidade padronizar o tratamento de evidências digitais, para preservar a integridade dos materiais, contribuindo com sua admissibilidade e força probatória". A ISO/IEC 27037:2013 foca em padrões para investigações digitais, servindo como uma referência essencial para garantir a integridade e a admissibilidade das evidências digitais em processos judiciais e investigações.

> Dentro do escopo de documentação de fatos digitais temos como uma das maiores referências a ABNT NBR ISO/IEC 27037:2013, que reúne uma série de recomendações e procedimentos que visam a padronizar o tratamento de evidências digitais para contribuir para sua admissibilidade, força probatória e confiança da apresentação dos fatos. Esses métodos práticos são aceitos mundialmente para padronizar os passos à evidência digital, desde sua coleta da fonte original, passando pelo seu exame e análise, até sua apresentação. (SOUZA; CARVALHO; MUNHOZ, 2023, p. 57)

Por outro lado, na legislação brasileira temos a Lei Nº 13.964, também conhecida como “Lei Anticrime”, que introduziu diversas alterações no Código de Processo Penal brasileiro, algumas das quais são relevantes para a área de investigação digital. Nela está definido os princípios da cadeia de custódia apontada em dez passos específicos para garantir a admissibilidade de uma prova no processo legal.

> Na legislação brasileira há pouca referência direta aos requisitos de uma prova obtida a partir da realidade, sobretudo em relação a provas digitais. Entretanto, podemos considerar os princípios da cadeia de custódia listados no artigo 158-A do CPP, que propõem etapas essenciais para a manutenção da autenticidade de prova [...] (SOUZA; CARVALHO; MUNHOZ, 2023, p. 57)
>
> [...] Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (CARVALHO et. al. 2023 p. 129 apud Lei Nº 13.964, 2019 s/n)

Dentre os dez passos definidos para manter a confiança da prova durante o processo legal, destacam-se as cinco primeiras, sendo elas essencialmente utilizadas na coleta e preservação de provas digitais, conforme descrito por Carvalho et al (2023 p. 129):

> Nesta lei são descritos dez passos relativos ao caminho da prova para manter sua confiança durante o processo legal, sendo os cinco primeiros conceitos associados à coleta e preservação da prova, que também podem ser aplicáveis às provas digitais:
>
> Reconhecimento: ato de distinguir quais elementos com maior interesse para a produção da prova pericial;
> **Isolamento:** a preservação do fato original, ou seja, evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato e relacionado aos vestígios e local de crime;
>
> **Fixação:** referente à descrição detalhada do vestígio, listando sua origem, posição, estado e diversos outros detalhes que confirme seu contexto.
> Coleta: refere-se ao ato de recolher o vestígio, respeitando suas características e natureza;
>
> **Acondicionamento:** procedimento de embalagem da evidência, de forma adequada a preservar suas características até o momento de sua análise, identificando o autor e o momento da coleta.

Ao nos aprofundarmos na ISO/IEC 27037:2013 e a Lei Nº 13.964 é possível observar como ambas se relacionam em três etapas essenciais no processo de documentação de provas digitais, sendo eles o isolamento, coleta e preservação das evidências.

Isolamento	Coleta	Preservação
Garantir a integridade da evidência durante a coleta para que se evite contaminações antes da preservação.	Captura detalhada e sistemática das evidências de modo que possam ser reproduzidas e auditadas posteriormente.	Assegurar a guarda da evidência de maneira integra e imutável.

Tabela 1 - Etapas para obtenção de provas digitais confiáveis para uso judicial, conforme método científico, baseadas em normas forenses e legislação
Fonte: CARVALHO et al. 2023, p. 131

Ambos os documentos, a norma ISO/IEC 27037:2013 e a Lei Nº 13.964, reconhecem a importância de um processo estruturado e rigoroso para o manejo de evidências digitais, ainda que de perspectivas diferentes – a norma com um enfoque técnico e a lei com um enfoque legal. Juntos, eles oferecem um quadro abrangente para a admissibilidade de provas digitais, que envolve o isolamento, coleta e preservação adequadas dessas evidências, garantindo que sejam confiáveis e utilizáveis em processos judiciais.

Integridade e Autenticidade das Provas

Sob a ótica dos requisitos descritos anteriormente, discutiremos a seguir alguns dos principais métodos utilizados para o isolamento, coleta e preservação de evidências digitais, analisando suas confiabilidades no asseguramento da integridade e autenticidade das provas. Entre eles, estão a captura de tela, Blockchain, ata notarial e as ferramentas de captura técnica. Esta última representa um meio moderno que segue padrões internacionais e a legislação brasileira para a documentação adequada de provas digitais, proporcionando maior confiabilidade em termos de preservação e validade jurídica.

Captura de Tela

Capturas de tela ou “Print Screen” se trata de um método básico, porém, muito utilizado para documentar evidências digitais de forma visual. Entretanto, essa maneira de se coletar e documentar evidências possuem duas situações que implicam em sua impugnação em processos judiciais, sendo eles a possibilidade de manipulação e o contexto limitado.
Uma imagem pode facilmente ser um material forjado para que seja implantada em um cenário investigado, como por exemplo, manipulando o conteúdo de um site por meio do inspecionar elemento do navegador ou por meio de uso de softwares capazes de criar conversas e contextos em telas idênticas a aplicativos de mensageria instantânea.

> Um designer com boas noções de UX é igualmente capaz de recriar um diálogo com o mesmo visual do WhatsApp, do Telegram ou do Instagram. Podemos dizer que: seja por meio de aplicativos específicos, seja por meio de softwares de edição de imagens, é relativamente simples criar diálogos que nunca existiram [...] (SOUZA; CARVALHO; MUNHOZ, 2023, p. 73)

Uma evidência registrada por meio de captura de tela também pode ter uma compreensão limitada de seu contexto, uma vez que a imagem apresentada não consegue fornecer uma visão completa dos assuntos ou cenários investigados. Isso significa que a captura de tela pode representar apenas uma parte do contexto, sem revelar todos os detalhes necessários para uma análise abrangente.

Observando a fácil capacidade de adulteração e manipulação das evidências por meio de capturas de tela, bem como a dificuldade de se validar sua autenticidade, considera-se que essa técnica representa um meio de baixíssima confiança como método de documentação de evidências. Conforme apresentado no quadro abaixo, a captura de tela não oferece garantias robustas sobre a integridade dos dados representados, o que compromete sua confiabilidade como prova.

Etapa	Isolamento	Coleta	Preservação
Confiança	Baixíssima	Baixíssima	Baixíssima

Tabela 2 - Avaliação de Confiaça – Captura de Tela
Fonte: SOUZA; CARVALHO; MUNHOZ, 2023, p. 75

Blockchain

A Blockchain, tecnologia que opera como um registro de dados de forma descentralizada e distribuída entre diversos computadores (nós) na rede. Como descrito por Carvalho et al. (2023 p. 138) “A tecnologia Blockchain consiste em um encadeamento de blocos compartilhados que cria um “livro razão imutável de dados”. Ou seja, sua estrutura garante a integridade e a imutabilidade das informações registradas, proporcionando maior transparência e confiança no processo de armazenamento e rastreamento de evidências digitais, podendo ser uma ferramenta eficaz para documentar toda a cadeia de custódia de uma evidência.

Entretanto, como mencionado por Carvalho et al. (2023 p. 138) “[...] esta tecnologia não faz juízo de valor sobre os materiais inseridos, ou seja, aceita informações falsas e/ou verdadeiras, a depender da intenção do emissor”. O que faz a blockchain ser confiável não é uma validação automática de que os dados são verdadeiros,

mas sim as características que garantem integridade e rastreabilidade. Dado esses atributos, considera-se que a tecnologia possui os princípios ideais para a preservação de uma evidência digital, assegurando que uma vez registrada, a evidência não possa ser adulterada ou removida sem que haja um rastro claro dessas modificações.

Etapa	Isolamento	Coleta	Preservação
Confiança	Baixa	Baixa	Alta

Tabela 3 - Avaliação de Confiança - Blockchain
Fonte: SOUZA; CARVALHO; MUNHOZ, 2023, p. 77

Ata Notarial

O registro e validação de evidências por meio de cartório, através de um tabelião com fé pública, é uma ferramenta histórica amplamente utilizada. De acordo com Brandelli (2004 apud Carvalho et al. 2023, p. 137), “a ata notarial é um instrumento público através do qual o notário capta, por seus sentidos, uma determinada situação, um determinado fato, transladando-o para os seus livros de notas ou para outro documento.” O notário, com base em seus sentidos humanos, é responsável por captar e documentar aquilo que testemunha.

Entretanto, vale ressaltar que esse profissional não tem a responsabilidade de possuir o entendimento técnico necessário para lidar com evidências geradas no ambiente digital, o que pode levar ao registro de provas manipuladas ou que não representem todo o contexto dos fatos.

> [...] o mero testemunho do fato digital sem o uso de conhecimentos técnicos adequados não são suficientes para avaliar um fato digital, afinal, a internet é meio volátil, facilmente falsificável e manipulável. Por isso, o conteúdo visto e ouvido na tela pode não corresponder ao que realmente está em determinada página. Com o uso de alguns recursos técnicos é possível “simular” uma situação de modo imperceptível a um leigo. (CARVALHO et. al., 2023, p. 138)

O uso isolado desse método, sem uma validação técnica, não é suficiente, de acordo com os métodos forenses, para garantir a integridade e autenticidade das provas. Como afirmam Souza, Carvalho e Munhoz (2023, p. 78), 'O cenário ideal de uso da ata notarial para a documentação de provas digitais envolveria a atuação de um perito técnico associado à fé pública do tabelião'. Dessa forma, a presunção de imparcialidade e a capacidade técnica seriam complementares, garantindo que as evidências digitais fossem registradas de maneira precisa e adequada, atendendo tanto aos requisitos legais quanto aos critérios técnicos necessários para sua validação em processos judiciais.

Etapa	Isolamento	Coleta	Preservação
Confiança SEM perícia técnica	Baixa ou Média	Baixa	Alta
Confiança COM perícia técnica	Alta	Alta	Alta

Tabela 4 - Avaliação de Confiança – Ata Notarial
Fonte: SOUZA; CARVALHO; MUNHOZ, 2023, p. 79

Ferramentas de Captura Técnica

As ferramentas de captura técnicas são plataformas que seguem padrões internacionais e a legislação brasileira, aderindo os critérios da cadeia de custódia. Nesse tópico iremos nos ater a solução atestada tecnicamente por órgãos públicos, a *Verifact*.

> A Verifact permite o registro desassistido de fatos digitais online a partir de uma tecnologia que atende de maneira efetiva as 3 etapas expostas anteriormente para se ter confiança no registro do fato digital. A plataforma se baseou em normas forenses internacionais para criar seu procedimento, possui meios efetivos para se evitar a fraude no registro e está em conformidade com a legislação brasileira. (CARVALHO et al., 2023, p. 142)

A solução tem como objetivo ser uma ferramenta de fácil acesso e baixo custo, garantindo, ao mesmo tempo, a integridade das informações coletadas. Seu funcionamento ocorre por meio da criação de um ambiente virtualizado, onde o perito pode, através da emulação de um navegador, acessar conteúdos como redes sociais, aplicativos de mensagens ou qualquer outro site cuja informação seja relevante para compor seu relatório de evidências.

> A navegação no conteúdo ocorre em um ambiente seguro que roda nos servidores da solução, evitando tentativas de manipulação citadas anteriormente como engenharia reversa, interceptação de conexão de internet e outras, comprovada por laudo de empresa de cibersegurança independente. (CARVALHO et al., 2023, p. 142)

Isso assegura que as informações registradas pela solução estavam realmente expostas na fonte específica, preservando sua autenticidade e validade para fins de comprovação, como mencionado por Souza, Carvalho e Munhoz (2023, p.191).

> A empresa afirma que seu procedimento permite embasar argumentos de conteúdos disponíveis na internet quanto à sua integridade, anterioridade, origem, contexto e ausência de adulteração durante e após o processo de coleta. Ou seja, permite afirmar que determinado conteúdo estava publicado em determinado site, em determinado momento, tal qual se apresenta nos conteúdos captados, havendo meio eficaz de se evitar interferências indevidas.

Ao finalizar todo o procedimento de evidenciação, a plataforma gera um relatório técnico preservado por meio da Certificação Digital ICP/Brasil, responsável por atestar a autoria do relatório utilizando o eCNPJ da Verifact. O documento também é associado a um carimbo de tempo certificado, que registra a data exata de fechamento do documento, garantindo a integridade temporal das informações coletadas (CARVALHO et al., 2023, p. 142).

Em suma, ferramentas como a Verifact desempenham um papel fundamental na garantia da admissibilidade e integridade das evidências digitais em processos judiciais, do qual nas palavras de Grazella (2020 apud CARVALHO et al., 2023, p. 142) “Pode ser usada por órgãos públicos, força policial, advogados e até pelas próprias vítimas de crimes virtuais, criando um material de alta confiança probatória quanto a sua existência, origem e autenticidade.” Sendo assim uma solução viável para que investigadores digitais possam assegurar que seus métodos de coleta e análise sejam robustos e respeitem os mais altos padrões éticos e legais.

Etapa	Isolamento	Coleta	Preservação
Confiança	Alta	Alta	Alta

Tabela 5 - Avaliação de Confiança - Ferramentas de Captura Técnica
Fonte: SOUZA; CARVALHO; MUNHOZ, 2023, p. 80

A seguir, temos um comparativo entre os métodos abordados anteriormente. Nele, podemos observar as diferentes abordagens para coleta de provas digitais e como cada uma delas atende aos critérios essenciais para gerar provas confiáveis. Ferramentas como o print de tela, Blockchain, ata notarial e a Verifact são comparadas em aspectos como agilidade, auditoria, integridade das informações, e conformidade com normas técnicas como a ISO 27037:2013 e a Lei 13.964/2019, que trata da coleta e preservação de evidências dentro da cadeia de custódia.

Figura 1 - Meios de coleta de provas digitais mais utilizados
Fonte: CARVALHO et al., 2023, p. 144

5. Conclusão

Os resultados obtidos neste trabalho demonstram que a utilização de técnicas de coleta de informações em fontes abertas de inteligência (OSINT) apresenta um papel crucial em investigações digitais. A pesquisa buscou responder à pergunta-problema, que aborda as técnicas empregadas para a coleta de dados e a admissibilidade das informações como prova pericial.

Dessa forma, cada objetivo foi alcançado. Primeiramente, foi possível identificar as principais técnicas de OSINT descritas na literatura especializada e sua aplicação no contexto de investigações forenses. Além disso, a pesquisa destacou os critérios necessários para assegurar a admissibilidade das provas coletadas, abordando a preservação da integridade e confiabilidade das evidências, conforme as melhores práticas recomendadas por especialistas.

A hipótese central de que é possível garantir a integridade e admissibilidade das informações obtidas por meio de OSINT, desde que seguidas as práticas adequadas de coleta, isolamento e preservação, como discutido ao longo do trabalho.

Entretanto, uma das limitações encontradas durante a pesquisa foi a escassez de literatura acadêmica voltada exclusivamente para a combinação de técnicas de OSINT com a legislação específica brasileira, o que sugere a necessidade de novos estudos nessa área. Assim, futuros trabalhos podem explorar mais profundamente a integração entre tecnologias emergentes e as práticas legais, visando contribuir para o aprimoramento dos métodos de coleta e análise de provas digitais.

Em suma, este estudo confirma a viabilidade da utilização de OSINT como ferramenta auxiliar nas investigações forenses, desde que os métodos de coleta e preservação respeitem os padrões éticos e legais, assegurando a confiabilidade das informações no processo judicial.

6. Referências

BARRETO, Alessandro Gonçalvez; WENDT, Emerson; CASELLI, Guilherme. **Investigação Digital em Fontes Abertas.** 2. ed. Rio de Janeiro: Brasport Livros e Multimídias Ltda, 2017.

BARRETO, Alessandro Gonçalvez; WENDT, Emerson. **Inteligência e Investigação Digital em Fontes Abertas.** 3. ed. Rio de Janeiro: Brasport Livros e Multimídias Ltda, 2020.

BRASIL. **Código de Processo Civil. Lei n.º 13.105, de 16 de março de 2015.** Brasília: Senado Federal, 2015.

BRASIL. **Doutrina Nacional de Inteligência de Segurança Pública (DNISP).** 1. ed. Brasília: Coordenação de Comunicação Social / ABIN, 2023.

BRASIL. **Emissão de Comprovante de Inscrição e de Situação Cadastral.** Disponível em: https://solucoes.receita.fazenda.gov.br/servicos/cnpjreva/cnpjreva_solicitacao.asp. Acesso em: 15 mar. 2024.

BRASIL. **Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União.** Disponível em: https://solucoes.receita.fazenda.gov.br/Servicos/certidaointernet/PF/EmitirPGFN. Acesso em: 15 mar. 2024.

Busca Por Nomes de Usuários. Disponível em: https://whatsmyname.app/. Acesso em: 3 jun. 2024.

CEPIK, Marco A. C. **Espionagem e Democracia.** 1. ed. Rio de Janeiro: Editora FGV, 2003.

LOPES, Pedro. **Investigação Cibernética Usando OSINT.** 2019.

PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

ROMULLO, Carvalho et al. **OSINT do Zero à Investigação Profissional.** 1. ed. Literando Editora, 2023.

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual Prático de Provas Digitais.** 1. ed. São Paulo: Thomson Reuters, Revista dos Tribunais, 2023.