COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 09

Investigação em fontes abertas

Guia prático de OSINT para a investigação criminal



09

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Investigação em fontes abertas

Guia prático de OSINT para a investigação criminal

Métodos, ferramentas e cuidados jurídicos para transformar informações públicas em conhecimento verificável.

Coleção Investigação e Proteção na Era Digital
Volume 09

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge
Material educativo de distribuição gratuita.
Coleção Investigação e Proteção na Era Digital, volume 09.
www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.
Investigação em fontes abertas : guia prático de OSINT para a investigação criminal [recurso eletrônico] / Higor Vinicius Nogueira Jorge. -- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.
1 recurso online (84 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 9)

Formato: PDF.
Modo de acesso: World Wide Web: <www.higorjorge.com.br>.
Inclui referências e apêndices.
Publicação de distribuição gratuita.

1. Inteligência de fontes abertas. 2. Investigação criminal. 3. Internet. 4. Prova digital. 5. Cadeia de custódia. 6. Proteção de dados pessoais. I. Título. II. Série.

Sumário

Apresentação..... 5
Objetivos e público-alvo..... 7
1 Fundamentos da investigação em fontes abertas..... 9
2 Limites jurídicos e éticos da pesquisa aberta..... 14
3 Planejamento, segurança operacional e registro..... 18
4 Buscadores, pesquisa avançada e memória da web..... 21
5 Identidades digitais, nomes de usuário e redes sociais..... 25
6 Imagens, vídeos e geolocalização..... 31
7 Domínios, DNS, endereços IP e infraestrutura..... 35
8 Sites falsos, golpes e reputação..... 40
9 Metadados e documentos digitais..... 42
10 Empresas, registros públicos e dados governamentais..... 44
11 Criptoativos e vestígios financeiros públicos..... 47
12 Correlação, análise de vínculos e uso de inteligência artificial..... 49
13 Preservação, cadeia de custódia e relatório..... 51
14 Estudo de caso hipotético: a loja que não existia..... 55
15 Oficinas práticas e casos simulados..... 58
Considerações finais..... 62
Apêndice A. Consulta rápida: qual ferramenta escolher..... 63
Apêndice B. Ficha de planejamento da pesquisa..... 65
Apêndice C. Registro de consulta em fonte aberta..... 66
Apêndice D. Checklist antes de encaminhar os resultados..... 67
Apêndice E. Comandos locais de integridade e metadados..... 68
Apêndice F. Glossário..... 70
Apêndice G. Índice de ferramentas e endereços..... 72
Referências..... 77
Minicurrículo do autor..... 81
Para aprofundar o estudo..... 83
A coleção..... 84

Apresentação

Toda investigação começa com um fragmento. Às vezes é o nome de usuário de um anunciante, a fotografia de um perfil, o endereço de um site recém-criado, uma página que desapareceu da internet ou o número de CNPJ estampado no rodapé de uma loja virtual. Isolados, esses elementos dizem pouco. Submetidos a um método de pesquisa, preservação e análise, podem revelar relações, contradições, padrões de comportamento e caminhos seguros para as diligências seguintes.

A inteligência de fontes abertas, conhecida pela sigla inglesa OSINT (Open Source Intelligence), não se confunde com pesquisas casuais na internet. O que a distingue é a combinação de uma pergunta investigativa definida, fontes identificáveis, procedimentos reproduzíveis, avaliação crítica das informações e documentação de cada passo. O objetivo não é acumular páginas, capturas de tela ou relatórios extensos, mas transformar observações públicas em conhecimento verificável e juridicamente utilizável.

Este volume foi escrito para funcionar de duas maneiras. Em leitura contínua, apresenta os fundamentos teóricos, os limites jurídicos e as técnicas de cada tipo de fonte, sempre com exemplos aplicados. Como obra de consulta, permite localizar rapidamente a ferramenta adequada a cada necessidade, compreender sua finalidade e suas limitações e acessar diretamente o endereço oficial, pois todos os links são clicáveis. A formação se completa com um estudo de caso integrado, oficinas práticas, modelos de registro e listas de verificação.

A obra dialoga com o método da Investigação Criminal Tecnológica que desenvolvi no livro Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais, publicado pela Editora Juspodivm, estruturado em sete fases: identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação (Jorge, 2027). A técnica digital não substitui o raciocínio investigativo, o respeito aos direitos fundamentais nem o controle humano sobre hipóteses e conclusões. Quanto mais fácil se torna pesquisar, maior é a responsabilidade de distinguir o que a fonte revela, o que ela apenas sugere e o que depende de diligência formal.

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

Este guia se destina a Delegados de Polícia, policiais civis e federais, peritos, analistas de inteligência, membros do Ministério Público, advogados, estudantes e pesquisadores que utilizam ou pretendem utilizar fontes abertas na apuração de fatos. A linguagem foi pensada para quem não tem formação em tecnologia, sem abrir mão da precisão técnica que a atividade exige.

Ao concluir a leitura, o leitor deverá ser capaz de formular uma pergunta investigativa verificável, escolher fontes e ferramentas proporcionais ao objetivo, reconhecer os limites jurídicos da pesquisa aberta, preservar o material com rastreabilidade, distinguir identificador digital de identidade civil e redigir conclusões que separem observação, inferência e comprovação.

Como utilizar este guia

Há duas trilhas de leitura. Na trilha de consulta imediata, o profissional identifica o objeto da pesquisa (pessoa, perfil, imagem, site, endereço IP, documento, empresa ou transação), consulta o Apêndice A, acessa o capítulo correspondente, escolhe a ferramenta e segue o procedimento indicado, sem dispensar o registro da consulta. Na trilha de formação, o leitor percorre os fundamentos, executa as oficinas do capítulo 15 com dados de treinamento e conclui com um relatório simulado. Esta segunda trilha é recomendada para cursos de formação policial e capacitações de unidades de polícia judiciária.

Cada ferramenta aparece em um quadro próprio, com finalidade, condição de acesso, cautela principal e endereço oficial. A condição de acesso segue cinco categorias aproximadas: aberto (consulta sem cadastro em condições normais), cadastro (exige conta ou autenticação), instalação (programa local ou extensão de navegador), freemium (recursos gratuitos limitados) e restrito (depende de autorização ou elegibilidade específica). Fornecedores alteram planos, regras e interfaces com frequência. Por isso, confira o domínio exibido no navegador antes de usar qualquer serviço e trate a classificação como orientação inicial.

A presença de um serviço neste guia significa que sua finalidade foi identificada e que há endereço oficial ou repositório verificável. Não representa aprovação institucional, garantia de segurança ou validação de todos os resultados que a plataforma possa produzir.

CAPÍTULO 1

Fundamentos da investigação em fontes abertas

1.1 O que é investigar em fontes abertas

Investigar em fontes abertas é identificar, acessar, coletar, preservar, comparar e interpretar informações provenientes de fontes legalmente acessíveis, com finalidade definida e método documentado. A expressão "fonte aberta" diz respeito à forma de acesso à informação, e não à sua veracidade, autoria ou permanência. Um perfil aberto pode conter dados falsos; um registro tecnicamente correto pode conduzir a uma interpretação equivocada; uma página pública hoje pode desaparecer amanhã.

A pesquisa em fontes abertas apoia a verificação de fatos, a identificação de endereços digitais, a reconstrução de contextos, a localização de testemunhas e documentos e a formulação de hipóteses. Ela não estabelece, por si só, a identidade civil de quem controla uma conta, a autoria penal de uma conduta ou a localização física precisa de um aparelho. Essas conclusões exigem convergência de elementos e, muitas vezes, diligências que dependem de requisição ou de ordem judicial.

O termo inteligência, presente na sigla OSINT, merece cuidado. Na atividade de inteligência, o produto serve ao assessoramento e à decisão; na investigação criminal, o resultado precisa ingressar nos autos com origem identificada, possibilidade de contraditório e respeito às regras de prova. A mesma técnica atende às duas finalidades, mas o rigor da documentação é maior quando o resultado poderá fundamentar uma medida restritiva ou uma imputação.

> **Exemplo hipotético.** Uma vítima de estelionato informa o nome de usuário do vendedor e a página em que viu o anúncio. A pesquisa aberta confirma que o anúncio ainda está publicado, preserva a página com data e hash, localiza o mesmo usuário em outra plataforma de vendas e identifica o domínio para o qual o anúncio direciona. Nada disso, ainda, aponta quem é o golpista. O resultado orienta, porém, quais registros devem ser preservados e requisitados junto aos provedores.

1.2 O ciclo da pesquisa e o método em sete fases

O método da Investigação Criminal Tecnológica organiza o trabalho em sete fases conectadas, que se aplicam integralmente às fontes abertas (Jorge, 2027). Na identificação, a equipe delimita a pergunta, as hipóteses, os alvos informacionais e os riscos. Na preservação, registra a existência do conteúdo relevante antes que seja removido ou alterado. Na obtenção, acessa e coleta os dados compatíveis com o escopo e com a base jurídica da diligência. No tratamento, organiza formatos, horários, fontes e duplicidades sem modificar os originais. Na correlação, confronta dados independentes, cronologias, vínculos e inconsistências. Na interpretação, avalia hipóteses concorrentes, explicações alternativas e lacunas. Na apresentação, relata método, achados, limitações e conclusões proporcionais ao material.

Observe que a preservação vem antes da obtenção completa. Em fontes abertas, o risco de perda é imediato: o anunciante apaga a publicação quando percebe a denúncia, a conta muda de nome, a página sai do ar. Uma captura inicial bem documentada pode ser o único registro disponível semanas depois.

Figura 1. Percurso da pesquisa em fontes abertas.



Fonte: elaboração própria, a partir do método em sete fases de Jorge (2027). As setas de retorno indicam que um achado pode exigir nova coleta ou revisão das hipóteses.

O percurso não é linear. Um achado na correlação pode revelar uma fonte ainda não preservada; uma contradição na interpretação pode exigir nova coleta. Cada retorno deve ser registrado, com a justificativa da ampliação da pesquisa, para que o caminho percorrido possa ser reconstruído por quem examinar o trabalho depois.

1.3 Observação, inferência e conclusão

O erro mais comum em fontes abertas não é técnico, é de raciocínio. Para evitá-lo, separe três níveis: a observação, aquilo que efetivamente apareceu na fonte em determinado momento; a inferência, uma explicação plausível para o que foi observado; e a conclusão, a afirmação que recebeu sustentação suficiente depois do confronto com fontes independentes. Um mesmo nome de usuário encontrado em duas plataformas é uma observação de coincidência de

identificador. Afirmar que as duas contas pertencem à mesma pessoa é uma inferência. Só se torna conclusão quando outros elementos, de natureza diferente, convergem nesse sentido e as explicações alternativas foram enfrentadas.

O Controle de Viés Investigativo, desenvolvido no livro de referência, oferece um roteiro simples para essa disciplina: para cada hipótese principal, formule uma hipótese alternativa plausível, indique o elemento que poderia sustentá-la e defina a diligência capaz de confirmá-la ou afastá-la (Jorge, 2027). Em fontes abertas, a hipótese alternativa costuma ser a coincidência, a cópia, a montagem, o perfil falso que usa a imagem de uma pessoa inocente ou o dado desatualizado.

Quadro 1. Três níveis do raciocínio em fontes abertas

Nível	O que é	Exemplo de redação
Observação	O que a fonte exibiu, com data e local de consulta	"Em 3 de setembro, o perfil @exemplo exibia a mesma fotografia do anúncio."
Inferência	Explicação plausível, ainda não testada	"A coincidência sugere possível reutilização da imagem pelo mesmo anunciante."
Conclusão	Afirmação sustentada por elementos convergentes e independentes	"Registros do provedor e o depoimento da vítima indicam que o perfil e o anúncio eram controlados pela mesma conta."

Fonte: elaboração própria.

> **Erro frequente.** Escrever no relatório que "o investigado utiliza as contas A, B e C" quando o que se observou foi apenas o mesmo apelido em três plataformas. A redação correta descreve o que foi visto e indica o grau de incerteza.

1.4 Fontes, confiabilidade e independência

Nem toda fonte tem o mesmo peso. Fonte primária é a que produz diretamente o dado, como o cadastro oficial de um domínio ou a publicação no endereço original. Fonte secundária interpreta, republica ou agrega registros de

terceiros, como um portal de notícias ou um site que compila dados empresariais. Fonte automatizada executa consultas e apresenta resultados compilados, sujeitos a falsos positivos. A classificação é funcional: uma fonte oficial pode estar desatualizada, e uma informação primária pode ser falsa por ter sido inserida pelo próprio usuário.

Ao avaliar uma informação, considere a origem identificável, a integridade do material, a data da observação, a atualidade do dado, a independência em relação a outras fontes e a pertinência para a pergunta. Duas páginas que reproduzem a mesma publicação não são duas confirmações, mas uma só, repetida. Por outro lado, um cadastro empresarial, um histórico de anúncios e o registro de um domínio oferecem perspectivas realmente distintas, ainda que nenhum deles, isoladamente, comprove autoria.

> **Síntese do capítulo.** Fonte aberta é critério de acesso, não de verdade. O método em sete fases organiza o trabalho, a separação entre observação, inferência e conclusão protege contra o viés de confirmação, e a independência das fontes é o que dá peso às convergências.

CAPÍTULO 2

Limites jurídicos e éticos da pesquisa aberta

2.1 Direitos fundamentais e proteção de dados

A Constituição Federal assegura a inviolabilidade da intimidade e da vida privada, o sigilo das comunicações e o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 1988, art. 5º, X, XII e LXXIX). Esses direitos não deixam de existir porque uma informação está acessível na internet. A disponibilidade pública reduz a expectativa de privacidade sobre aquele conteúdo específico, mas não autoriza a coleta indiscriminada, a exposição desnecessária nem o uso para finalidade diversa da investigação.

A Lei Geral de Proteção de Dados Pessoais não se aplica ao tratamento realizado para fins exclusivos de segurança pública e de investigação e repressão de infrações penais, que deve ser regido por legislação específica, com observância do devido processo legal, dos princípios gerais de proteção e dos direitos do titular (Brasil, 2018, art. 4º, III, "a" e "d", e § 1º). Na prática, isso significa que a pesquisa policial em fontes abertas não está livre de limites: deve observar finalidade, necessidade, adequação e segurança, coletando apenas o que interessa à apuração e protegendo o material obtido.

> **Orientação prática.** Antes de iniciar a pesquisa, registre a finalidade e o fato investigado. Esse registro simples demonstra a necessidade da coleta, delimita o escopo e justifica, depois, por que determinados dados foram preservados e outros descartados.

2.2 O que o Marco Civil da Internet reserva à via formal

O Marco Civil da Internet distingue o conteúdo publicamente acessível de outras categorias de dados (Brasil, 2014). Os registros de conexão e de acesso a aplicações, assim como o conteúdo de comunicações privadas, somente podem ser disponibilizados pelo provedor mediante ordem judicial (art. 10, §§ 1º e 2º, e art. 22). Os dados cadastrais que informem qualificação pessoal, filiação e endereço podem ser obtidos por autoridades administrativas que detenham competência legal para requisitá-los (art. 10, § 3º), o que, no inquérito policial,

se articula com o poder de requisição do Delegado de Polícia (Brasil, 2013a, art. 2º, § 2º).

Os provedores de conexão devem guardar os registros de conexão por um ano, e os provedores de aplicações, os registros de acesso por seis meses (Brasil, 2014, arts. 13 e 15). A autoridade policial pode requerer, cautelarmente, que esses registros sejam guardados por prazo superior, devendo apresentar o pedido de autorização judicial de acesso no prazo legal. Aqui está uma das contribuições mais valiosas da pesquisa aberta: ao identificar rapidamente qual plataforma, domínio ou serviço está envolvido, ela permite que o pedido de preservação seja feito antes que os registros sejam descartados.

Quadro 2. O que a pesquisa aberta alcança e o que exige outra via

Informação	Via adequada
Publicação, perfil ou página acessível sem burlar barreiras	Pesquisa em fonte aberta, com preservação e registro
Dados cadastrais de usuário (qualificação, filiação, endereço)	Requisição da autoridade com competência legal (Marco Civil, art. 10, § 3°)
Registros de conexão e de acesso a aplicações	Preservação cautelar e ordem judicial (Marco Civil, arts. 13, 15 e 22)
Conteúdo de comunicações privadas, mensagens e perfis fechados	Ordem judicial específica
Interação com o investigado sob identidade fictícia para obter informações	Infiltração virtual, com autorização judicial (ECA, art. 190-A; Lei n° 12.850/2013, art. 10-A)

Fonte: elaboração própria, com base em Brasil (1990, 2013b, 2014).

2.3 Observar não é infiltrar

Este é o ponto jurídico mais sensível da pesquisa em fontes abertas. Observar passivamente o que está publicamente acessível é atividade investigativa ordinária. Criar um perfil fictício para interagir com o investigado, conquistar sua confiança, ser aceito em grupo fechado ou solicitar que um perfil privado aceite o pedido de amizade é algo diferente: aproxima-se da infiltração de

agentes, que o ordenamento admite apenas nas hipóteses legais e mediante autorização judicial.

A infiltração de agentes de polícia na internet está prevista no Estatuto da Criança e do Adolescente, para a investigação de crimes contra a dignidade sexual de crianças e adolescentes e de outros delitos ali indicados, sempre precedida de autorização judicial fundamentada e com a exigência de que a prova não possa ser obtida por outros meios (Brasil, 1990, arts. 190-A a 190-E). A Lei nº 12.850/2013, com a redação dada pela Lei nº 13.964/2019, também disciplina a infiltração virtual na investigação de organizações criminosas e declara nula a prova obtida sem a observância de suas regras (Brasil, 2013b, art. 10-A, § 7º; Brasil, 2019).

Nesse ponto, a lei não traça uma linha precisa. Como orientação técnica, entende-se que o uso de conta funcional ou institucional apenas para visualizar conteúdo público, sem interação com o investigado, não caracteriza infiltração. Quando a pesquisa exige ocultar a identidade para obter acesso, diálogo ou confiança, a equipe deve avaliar com cuidado a necessidade de autorização judicial, sob pena de comprometer a prova e expor o policial. Em caso de dúvida, a via formal é a mais segura.

Também estão fora do escopo da pesquisa aberta, e deste guia, a invasão de contas, o uso de credenciais alheias, a superação de mecanismos de autenticação, a exploração de vulnerabilidades e a compra ou consulta de bases de dados vazadas. Além de comprometer a prova, essas condutas podem configurar crime, como a invasão de dispositivo informático (Brasil, 1940, art. 154-A).

> **Erro frequente.** Supor que tudo o que um mecanismo de busca indexou pode ser usado sem restrição, ou que um perfil privado se torna "aberto" quando o investigado aceita a solicitação de um perfil falso. O caminho até a informação é tão relevante quanto a informação.

2.4 Cadeia de custódia e capturas de tela

O Código de Processo Penal define cadeia de custódia como o conjunto de procedimentos que documentam a história cronológica do vestígio, desde seu

reconhecimento até o descarte (Brasil, 1941, arts. 158-A a 158-F, incluídos pela Lei nº 13.964/2019). No ambiente digital, isso significa registrar origem, data e hora, ambiente de coleta, responsável, método e integridade do material, de modo que outra pessoa possa verificar que aquilo que chega aos autos corresponde ao que foi observado.

O Superior Tribunal de Justiça tem sido rigoroso com provas digitais produzidas sem metodologia. No AgRg no HC 828.054/RN, a Quinta Turma declarou inadmissíveis capturas de tela de conversas obtidas por acesso direto a um celular apreendido, sem ferramenta forense e sem documentação das etapas, por reconhecer a quebra da cadeia de custódia (Brasil, 2024). O caso não trata de fontes abertas, mas sua lógica se aplica a elas: a captura isolada, sem registro de origem e integridade, é a forma mais frágil de levar um conteúdo digital ao processo. O capítulo 13 apresenta os cuidados de preservação que reduzem esse risco.

2.5 Cuidados com crianças, adolescentes e terceiros

A pesquisa aberta frequentemente alcança pessoas que nada têm a ver com o fato: familiares, amigos, seguidores, pessoas fotografadas ao fundo. O princípio da necessidade impõe que esses dados não sejam coletados nem reproduzidos além do indispensável. Quando houver crianças e adolescentes, a cautela é redobrada. O Estatuto Digital da Criança e do Adolescente, Lei nº 15.211/2025, em vigor desde 17 de março de 2026, reforça a proteção desse público no ambiente digital (Brasil, 2025). Imagens de abuso sexual infantil jamais devem ser baixadas, copiadas ou enviadas a ferramentas externas fora dos procedimentos legais e periciais próprios.

> **Síntese do capítulo.** A pesquisa aberta é legítima quando tem finalidade definida, coleta apenas o necessário e não ultrapassa barreiras de acesso. Registros, dados cadastrais e conteúdo privado seguem as vias do Marco Civil; a interação sob identidade fictícia aproxima-se da infiltração virtual, que exige autorização judicial; e a documentação da coleta é condição de validade da prova.

CAPÍTULO 3

Planejamento, segurança operacional e registro

3.1 Da pergunta ao plano de coleta

Uma boa pesquisa começa com uma pergunta delimitada. "Descobrir tudo sobre determinado perfil" é uma formulação excessivamente ampla, que conduz à dispersão e à coleta de dados irrelevantes. "Verificar se o endereço divulgado no anúncio corresponde ao domínio oficial da empresa mencionada" é um objetivo verificável, com fontes conhecidas e critério claro de encerramento.

O plano de coleta registra o objeto, a finalidade, a hipótese principal, a hipótese alternativa, o período de interesse, as fontes previstas, os parâmetros de busca, a forma de preservação, as restrições de acesso e o responsável. A pesquisa pode ser ampliada quando surgir dado novo, mas a ampliação deve ser justificada no registro. O Apêndice B traz uma ficha de planejamento pronta para uso.

> **Exemplo hipotético.** Pergunta: a fotografia usada pelo perfil de uma suposta loja já circulava antes do anúncio? Hipótese 1: a imagem foi produzida pelo anunciante. Hipótese 2: foi licenciada ou retirada do catálogo de um fabricante. Hipótese 3: foi copiada de terceiro. A busca reversa testa a anterioridade e a circulação da imagem, mas não define, sozinha, qual hipótese corresponde ao fato.

3.2 Segurança operacional do pesquisador

A navegação investigativa também deixa rastros. Visitas a perfis podem ser registradas pela plataforma, cookies e rastreadores associam o navegador a contas pessoais, links suspeitos podem conter código malicioso e extensões de navegador recebem permissões amplas. A segurança operacional, chamada em inglês de OPSEC, é o conjunto de cuidados que protege o investigador, a investigação e as vítimas.

Planeje o ambiente de trabalho conforme a política de segurança da instituição: navegador e sistema atualizados, perfis de navegação separados para a atividade funcional, contas institucionais autorizadas, nunca contas pessoais, e controle sobre o que é enviado a serviços de terceiros. Não instale extensões fora das lojas oficiais, não abra anexos suspeitos no equipamento de trabalho e não insira dados de vítimas, documentos sigilosos ou links privados em ferramentas públicas de análise.

> **Erro frequente.** Pesquisar o investigado a partir do perfil pessoal do policial em uma rede social. Além de expor o servidor, a plataforma pode sugerir o perfil do policial ao investigado como "pessoa que você talvez conheça".

3.3 Tempo, memória da internet e resultados negativos

Uma pesquisa registra o estado de uma fonte em determinado momento. Conteúdos são alterados, desindexados, apagados ou ocultados por regras de visibilidade. Por isso, registre separadamente quatro datas que podem ser diferentes: a data do fato alegado, a data da publicação, a data do conteúdo arquivado e a data da consulta. Registre sempre o fuso horário. Plataformas exibem horários conforme a configuração do usuário, e a conversão errada pode deslocar um evento para outro dia.

Resultado negativo é uma observação delimitada, e não prova de inexistência. A formulação correta é: "na consulta realizada em [data], com os parâmetros [descrição], no serviço [nome], não foi localizado o conteúdo referido". A ausência pode decorrer de limitação de indexação, exclusão, mudança de privacidade, bloqueio de acesso automatizado ou falha da ferramenta.

3.4 O registro mínimo de cada consulta

Cada consulta relevante deve deixar um registro com data, hora e fuso; operador e ambiente; serviço e URL completa; termo ou identificador pesquisado e parâmetros; resultado observado, inclusive ausência; forma de preservação, local de armazenamento e hash; avaliação de confiabilidade; e encaminhamento proposto. O Apêndice C traz o modelo de registro e um exemplo preenchido. Em investigações longas, mantenha uma planilha

cronológica com identificador para cada item preservado e referência cruzada aos arquivos.

Orientação prática. Copie sempre a URL completa da barra de endereços, e não apenas o nome do perfil. O identificador numérico de uma publicação ou de uma conta permanece mesmo quando o nome de usuário é alterado, e é ele que o provedor utilizará para localizar os registros.

Síntese do capítulo. Pergunta delimitada, hipótese alternativa, ambiente de trabalho seguro e registro de cada consulta são os quatro pilares do planejamento. A data da consulta e o fuso horário acompanham toda observação, e o resultado negativo é registrado com a mesma precisão que o positivo.

CAPÍTULO 4

Buscadores, pesquisa avançada e memória da web

4.1 A estratégia de busca

Mecanismos de busca indexam apenas parte da internet, e cada um o faz de modo diferente. A pesquisa textual eficiente combina especificidade e cobertura: comece pela expressão literal mais característica do caso, entre aspas, e depois amplie com sinônimos, grafias alternativas, erros de digitação comuns e variações de nome. Operadores restringem domínios, formatos de arquivo e períodos. Seu comportamento não é idêntico em todos os buscadores e pode mudar sem aviso, de modo que o resultado deve ser conferido sempre na página de origem, e não no resumo exibido pela busca (Google, [s. d.]).

Quadro 3. Operadores de pesquisa mais úteis

Operador	Função	Exemplo
"..."	Busca a expressão exata	"loja exemplo eletrônicos"
site:	Restringe a um domínio ou extensão	site:gov.br "fraude eletrônica"
filetype:	Restringe ao tipo de arquivo	filetype:pdf "cadeia de custódia"
- (sinal de menos)	Exclui um termo	golpe pix -notícia
OR	Aceita um termo ou outro	"loja exemplo" OR "lojaexemplo"
intitle: / inurl:	Busca no título ou no endereço da página	intitle:"política de troca" inurl:loja
before: / after:	Limita por data de indexação (Google)	"loja exemplo" after:2026-01-01

Fonte: elaboração própria. O funcionamento pode variar entre buscadores e ao longo do tempo.

Compare sempre ao menos dois buscadores e documente as divergências. A posição de um resultado na lista indica relevância para o algoritmo, e não

qualidade da evidência. Desde 2024, o Google deixou de oferecer o antigo recurso de cópia em cache das páginas, o que torna ainda mais importante a consulta a serviços de arquivamento e a preservação própria do conteúdo.

4.2 Páginas históricas e arquivos da web

Quando alguém alega que uma página foi alterada ou removida, os serviços de arquivamento permitem consultar versões antigas. A Wayback Machine, mantida pela organização sem fins lucrativos Internet Archive, guarda instantâneos de bilhões de páginas e permite também solicitar o arquivamento de uma URL pública no momento da consulta (Internet Archive, [s. d.]). Seus instantâneos são recortes: nem toda página foi arquivada, nem toda versão foi capturada, e conteúdos dinâmicos ou dependentes de login costumam aparecer incompletos.

> **Exemplo hipotético.** A vítima afirma que a página de uma loja anunciava "entrega garantida em 48 horas" quando fez a compra, mas o texto atual não traz essa promessa. A equipe localiza na Wayback Machine um instantâneo da semana da compra com a frase original, registra a URL do instantâneo, a data da captura e a diferença em relação à página atual, e preserva as duas versões. O instantâneo comprova o conteúdo arquivado naquela data, não quem o redigiu.

4.3 Ferramentas de pesquisa e memória da web

> **Google Pesquisa Avançada** ABERTO
>
> Combina termos exatos, idioma, região, domínio e formato de arquivo em um formulário.
>
> **Cautela:** Resultados dependem do índice e da personalização; abra sempre a origem.
>
> www.google.com/advanced_search

> **Bing** ABERTO
>
> Buscador complementar, com índice e resultados que frequentemente diferem do Google.
>
> **Cautela:** Ausência de resultado não demonstra inexistência da página.
>
> www.bing.com/

Wayback Machine ABERTO

Consulta versões arquivadas de páginas e permite salvar URLs públicas no momento da pesquisa.

Cautela: Cobertura incompleta; não substitui a preservação institucional.

web.archive.org/

Google Trends ABERTO

Mostra a tendência agregada de buscas por um termo, ao longo do tempo e por região.

Cautela: Dado agregado; não revela quem pesquisou.

trends.google.com/trends/

Google Fact Check Explorer ABERTO

Localiza checagens já publicadas sobre alegações e imagens em circulação.

Cautela: A existência de checagem não dispensa a verificação direta da fonte.

toolbox.google.com/factcheck/explorer

OSINT Framework ABERTO

Árvore temática que reúne ferramentas e recursos de fontes abertas por categoria.

Cautela: É um índice de referências, não uma chancela de cada destino.

osintframework.com/

Bellingcat Online Investigation Toolkit ABERTO

Catálogo comentado de ferramentas mantido pela comunidade de investigação da Bellingcat.

Cautela: Verifique individualmente cada ferramenta indicada.

bellingcat.gitbook.io/toolkit

Orientação prática. Para treinar, pesquise site:gov.br "segurança digital" filetype:pdf e depois a mesma expressão sem os filtros. Compare quais fontes desapareceram e anote, para cada resultado relevante, o título, a URL de destino e a data da consulta.

Síntese do capítulo. Buscadores mostram parte da internet e de modo diferente entre si; operadores tornam a pesquisa precisa, e arquivos da web permitem confrontar versões. Em todos os casos, a evidência é a página de origem preservada, e não a lista de resultados.

CAPÍTULO 5

Identidades digitais, nomes de usuário e redes sociais

5.1 Identificador não é identidade

Nomes de usuário, fotografias, apelidos, endereços de e-mail, números de telefone divulgados, endereços IP e domínios são identificadores de natureza distinta. Nenhum deles, por si só, equivale à identificação civil de uma pessoa. Uma conta pode ser compartilhada ou vendida, uma foto pode ser copiada, um telefone pode ter mudado de titular, e um apelido comum pode ser usado por centenas de pessoas sem relação entre si.

A vinculação entre identificadores e uma pessoa exige elementos convergentes, análise de temporalidade e enfrentamento das explicações alternativas. Na redação, prefira formulações descritivas, como "o perfil público apresentava o mesmo identificador", a conclusões antecipadas, como "a pessoa utilizava todas essas contas". A individualização da autoria depende de provas e diligências juridicamente adequadas.

5.2 Enumeração de nomes de usuário

Ferramentas de enumeração consultam centenas de sites para verificar se determinado nome de usuário existe em cada um deles. São detectores de presença provável, não de titularidade. O projeto WhatsMyName, por exemplo, mantém sua base colaborativa de detecções em repositório público e é utilizado por diversas interfaces de consulta (WebBreacher, [s. d.]). Qualquer que seja a ferramenta, o resultado precisa ser validado manualmente: abrir a página de destino, verificar se o perfil realmente existe com aquela grafia, observar o conteúdo público e classificar cada ocorrência como confirmação documental, possível coincidência ou descarte.

Sherlock INSTALAÇÃO

Verifica a ocorrência de um nome de usuário em centenas de plataformas, a partir da linha de comando.

Cautela: Gera falsos positivos e negativos; não comprova titularidade.

github.com/sherlock-project/sherlock

Maigret INSTALAÇÃO

Pesquisa nomes de usuário em ampla base de sites e exporta relatórios.

Cautela: Revise cada resultado automático individualmente.

github.com/soxoj/maigret

WhatsMyName ABERTO

Interface web que consulta a base colaborativa do projeto WhatsMyName, mantida em repositório público.

Cautela: Detecções dependem da base e mudam conforme os sites alteram suas páginas.

whatsmyname.app/

Erro frequente. Concluir que duas contas pertencem à mesma pessoa porque compartilham o nome de usuário, a foto de perfil ou o mesmo estilo de escrita. Apelidos reciclados, homônimos e cópias de imagem são explicações frequentes e precisam ser descartadas antes de qualquer afirmação.

5.3 Redes sociais na interface oficial

A pesquisa em redes sociais deve começar pela interface oficial e pela identificação do conteúdo efetivamente público. Em cada publicação relevante, registre a URL completa, o texto exibido, as imagens, as menções, os links externos, o identificador visível, a data de publicação indicada e o momento da observação. Visibilidade de comentários, histórico e perfis varia conforme o usuário esteja ou não autenticado e conforme as configurações da conta observada.

Listas de seguidores, curtidas e "amigos em comum" orientam hipóteses, mas não demonstram associação criminosa nem conhecimento entre as pessoas. Ferramentas externas de extração podem violar as condições de uso das

plataformas e deixam de funcionar com frequência após mudanças técnicas, devendo ser tratadas como apoio complementar, nunca como procedimento garantido.

Instagram ABERTO OU CADASTRO

Exame de biografia, nome público, publicações visíveis, links e elementos de contexto.

Cautela: Perfis privados não são fonte aberta.

www.instagram.com/

Facebook ABERTO OU CADASTRO

Consulta a páginas, publicações e informações explicitamente públicas, incluindo a transparência de páginas.

Cautela: A visibilidade depende do perfil e das políticas da plataforma.

www.facebook.com/

TikTok ABERTO OU CADASTRO

Pesquisa de perfis e vídeos disponíveis publicamente.

Cautela: Acesso automatizado e visibilidade podem ser limitados.

www.tiktok.com/

YouTube ABERTO

Consulta a vídeos, canais, descrições e datas de publicação exibidas.

Cautela: A data de publicação não autentica o contexto da filmagem.

www.youtube.com/

X (pesquisa avançada) CADASTRO

Filtra publicações por termos, contas, período e localização declarada.

Cautela: Exige login; resultados variam conforme a política da plataforma.

x.com/search-advanced

LinkedIn CADASTRO

Exame de informações profissionais publicadas por pessoas e organizações.

Cautela: Autodeclarações não comprovam vínculo profissional.

www.linkedin.com/

Telegram Web CADASTRO

Interface oficial para consultar canais e grupos públicos.

Cautela: Ingressar em grupos sob identidade fictícia exige a análise do capítulo 2.

web.telegram.org/

Instaloader INSTALAÇÃO

Projeto não oficial que baixa publicações e metadados de perfis públicos do Instagram.

Cautela: Sujeito a bloqueios e às regras da plataforma; uso apenas complementar.

github.com/instaloader/instaloader

5.4 Transparência de páginas e anúncios

A Biblioteca de Anúncios da Meta permite pesquisar anúncios veiculados no Facebook, no Instagram e em outros produtos da empresa, com data de início, páginas responsáveis e variações do mesmo anúncio. É especialmente útil em investigações de lojas falsas e golpes divulgados por publicidade paga. A Meta Content Library, por sua vez, é um ambiente de pesquisa de conteúdo público destinado a pesquisadores e instituições que cumpram requisitos de elegibilidade, e seu acesso depende de solicitação aprovada pela empresa (Meta, [s. d.]a, [s. d.]b). Não se trata de ferramenta aberta a qualquer usuário.

Biblioteca de Anúncios da Meta ABERTO

Pesquisa anúncios ativos e encerrados em produtos da Meta, por página ou palavra-chave.

Cautela: O histórico e os filtros variam conforme o tipo de anúncio e o país.

www.facebook.com/ads/library/

Meta Content Library e API RESTRITO

Ambiente oficial de pesquisa estruturada de conteúdo público do Facebook e do Instagram.

Cautela: Depende de elegibilidade e de aprovação da Meta.

developers.facebook.com/docs/content-library-and-api/

5.5 E-mails e exposição em vazamentos

Endereços de e-mail aparecem em páginas institucionais, cadastros de domínio, documentos publicados e incidentes de segurança. Serviços como o Have I Been Pwned informam se um endereço aparece em vazamentos conhecidos, sem exibir senhas, e são úteis para avaliar o risco de comprometimento de contas da vítima. Ferramentas de prospecção comercial, como o Hunter, apresentam e-mails profissionais associados a um domínio, muitas vezes inferidos a partir de padrões, o que exige separar o endereço efetivamente publicado do endereço apenas estimado.

Have I Been Pwned ABERTO

Informa se um endereço de e-mail consta de incidentes de vazamento conhecidos.

Cautela: Não fornece senhas; alguns vazamentos só são exibidos ao titular verificado.

haveibeenpwned.com/

Hunter FREEMIUM E CADASTRO

Lista e-mails profissionais associados publicamente a um domínio.

Cautela: Endereços podem ser inferidos; não confirmam autoria de mensagens.

hunter.io/domain-search

GitHub ABERTO OU CADASTRO

Localiza repositórios, perfis e conteúdo publicado por desenvolvedores.

Cautela: A pesquisa de código exige login.

github.com/search

Erro frequente. Buscar, baixar ou consultar bases de credenciais vazadas para "descobrir a senha" ou outros dados do investigado. Essas bases têm origem ilícita, e sua utilização compromete a prova e pode configurar crime.

Síntese do capítulo. Identificadores são pistas, e não pessoas. Ferramentas de enumeração apontam coincidências que exigem validação manual, redes sociais devem ser examinadas na interface oficial e com registro de URL e data, e a biblioteca de anúncios é aliada valiosa nas fraudes divulgadas por publicidade.

CAPÍTULO 6

Imagens, vídeos e geolocalização

6.1 Busca reversa de imagens

Uma fotografia pode ter passado por cortes, espelhamento, compressão, filtros e republicações. A busca reversa procura correspondências visuais em páginas indexadas, permitindo localizar versões anteriores, a fonte provável e outros contextos em que a imagem circulou. É a técnica mais simples para verificar se a foto de um produto, de um perfil ou de um suposto acontecimento é original ou foi copiada.

O resultado mais antigo encontrado não é, necessariamente, o original, pois depende do que os buscadores indexaram. Serviços diferentes encontram resultados diferentes, e por isso convém usar mais de um. Lembre-se de que a busca reversa exige enviar a imagem a um terceiro: imagens de vítimas, de crianças ou sob sigilo não devem ser submetidas sem avaliação institucional.

Google Lens ABERTO

Pesquisa ocorrências de imagens, objetos e textos visuais em páginas indexadas.

Cautela: Exige envio da imagem ao serviço.

lens.google/

TinEye ABERTO OU FREEMIUM

Localiza cópias e versões publicadas de uma imagem, com ordenação por data de indexação.

Cautela: Não certifica a primeira publicação absoluta.

tineye.com/

Bing Visual Search ABERTO

Busca visual complementar, com índice diferente do Google.

Cautela: Resultados variam conforme o recorte da imagem.

www.bing.com/visualsearch

6.2 Vídeos, quadros-chave e verificação

Para vídeos, a técnica consiste em extrair quadros-chave e pesquisar cada um deles separadamente. A extensão InVID Verification Plugin, desenvolvida no âmbito de projetos europeus de verificação jornalística, reúne essas funções: fragmenta vídeos em quadros, consulta vários buscadores, lê metadados e oferece lupa e filtros forenses de apoio. Preserve sempre o arquivo original e registre cada transformação realizada.

> **InVID Verification Plugin** INSTALAÇÃO
> Extensão para verificação de vídeos e imagens, com extração de quadros-chave e busca reversa.
> **Cautela:** Confira a origem da extensão e as permissões solicitadas.
> www.invid-project.eu/tools-and-services/invid-verification-plugin/

> **MediaInfo** INSTALAÇÃO
> Exibe contêiner, codec, duração, trilhas e propriedades técnicas de áudio e vídeo.
> **Cautela:** Propriedades técnicas não identificam o autor do vídeo.
> mediaarea.net/en/MediaInfo

> **Erro frequente.** Tratar a data exibida pela plataforma como a data da gravação. A data de publicação indica quando o arquivo foi enviado; o vídeo pode ter sido gravado anos antes, em outro lugar, e reaproveitado em novo contexto.

6.3 Geolocalização por marcadores independentes

Geolocalizar é testar a compatibilidade de um cenário com um local. Os sinais úteis incluem o traçado e a geometria das ruas, cruzamentos, relevo, fachadas, letreiros, placas de trânsito, postes, vegetação, a linha do horizonte e a posição de montanhas ou edifícios marcantes. Busque vários pontos independentes: um único elemento semelhante pode existir em muitos lugares, mas a combinação de cinco ou seis marcadores raramente se repete.

Ferramentas cartográficas oferecem imagens de épocas diferentes. Um estabelecimento pode ter mudado de nome, uma via pode ter sido duplicada e uma fachada reformada. Registre a data da imagem de satélite ou de rua

utilizada, quando disponível, e diferencie sempre "local compatível" de "local confirmado por marcadores independentes".

> **Exemplo hipotético.** Um vídeo de ameaça mostra, ao fundo, uma caixa d'água com formato incomum, um posto de combustível e uma rua em declive com canteiro central. A equipe identifica três bairros candidatos pelo padrão do posto, descarta dois pelo relevo no Google Earth e confirma, no terceiro, a caixa d'água e o canteiro em imagens de rua de períodos distintos. O relatório indica o local como compatível, registra as datas das imagens consultadas e recomenda diligência presencial para confirmação.

6.4 Sombras, sol e cronolocalização

A posição do Sol e a direção das sombras podem ajudar a estimar o horário de uma imagem ou a orientação de uma rua, desde que a data, a perspectiva e a topografia sejam suficientemente conhecidas. A Bellingcat publicou orientações e uma ferramenta de código aberto sobre o tema, que mostram o potencial e os limites da técnica (Bellingcat, 2021, 2024). Imagens de satélite do programa europeu Copernicus complementam a análise de áreas amplas e de mudanças no terreno, mas têm resolução insuficiente para identificar pessoas ou veículos (European Space Agency, 2026).

> **Google Maps** ABERTO
> Ruas, estabelecimentos e imagens ao nível da rua, com histórico de datas em muitas regiões.
> **Cautela:** Imagens e informações podem estar desatualizadas.
> www.google.com/maps/

> **Google Earth** ABERTO
> Relevo, ocupação do solo, visualização tridimensional e imagens históricas.
> **Cautela:** Disponibilidade e datas das imagens variam por região.
> earth.google.com/

OpenStreetMap ABERTO

Mapa colaborativo com vias, edificações e pontos de interesse.

Cautela: Depende da contribuição e atualização da comunidade.

www.openstreetmap.org/

Mapillary ABERTO

Fotografias de rua enviadas pela comunidade, úteis onde não há outras coberturas.

Cautela: Cobertura irregular; conteúdo enviado por usuários.

www.mapillary.com/app/

SunCalc ABERTO

Calcula a posição do Sol e a direção das sombras para data, hora e local informados.

Cautela: Só auxilia com data, perspectiva e topografia controladas.

www.suncalc.org/

Copernicus Browser ABERTO OU CADASTRO

Imagens de observação da Terra do programa Copernicus, com séries temporais.

Cautela: Resolução não permite identificar pessoas.

browser.dataspace.copernicus.eu/

Síntese do capítulo. A busca reversa revela a circulação de imagens, os quadros-chave estendem a técnica aos vídeos e a geolocalização exige marcadores independentes e datas das imagens consultadas. Data de publicação não é data de gravação, e local compatível não é local confirmado.

CAPÍTULO 7

Domínios, DNS, endereços IP e infraestrutura

7.1 Papéis distintos na cadeia técnica

Um site envolve vários agentes com papéis diferentes. O registrante contrata o nome de domínio por meio de um registrador. O serviço de DNS traduz o nome em endereços técnicos. A hospedagem guarda os arquivos do site, muitas vezes atrás de uma rede de distribuição de conteúdo, a CDN, que esconde o servidor de origem. Uma autoridade certificadora emite o certificado que habilita a conexão segura. E o operador do site pode ser pessoa diversa de todos esses. Confundir esses papéis é a origem de muitas conclusões erradas.

> **Erro frequente.** Atribuir a fraude ao registrador do domínio, ao provedor de nuvem ou à empresa titular de um bloco de endereços IP. Esses agentes prestam serviço a milhões de clientes legítimos; podem ser destinatários de requisições e ordens judiciais, mas não são, por isso, suspeitos.

7.2 Registro de domínios

O cadastro de domínios é consultado pelo protocolo RDAP, sucessor do antigo Whois. Para domínios genéricos, como .com e .net, a consulta oficial é o ICANN Lookup (ICANN, [s. d.]). Para domínios .br, o Registro.br oferece consulta pública, com regras próprias de uso e redistribuição dos dados (Registro.br, [s. d.]). Informações pessoais de registrantes estrangeiros costumam estar ocultas por serviços de privacidade, mas a data de criação do domínio é dado precioso: lojas falsas costumam usar domínios registrados poucos dias antes dos anúncios.

> **ICANN Lookup** ABERTO
>
> Consulta oficial de dados de registro de domínios genéricos por RDAP.
>
> **Cautela:** Dados pessoais podem estar protegidos por privacidade.
>
> lookup.icann.org/

Registro.br ABERTO

Consulta pública de domínios sob .br.

Cautela: Uso dos dados sujeito à política do Registro.br.

registro.br/tecnologia/ferramentas/whois/

7.3 DNS, certificados e tecnologias

Consultas DNS mostram para onde um nome aponta no momento da pesquisa: endereços IP, servidores de e-mail, registros de verificação. A resolução atual não prova a hospedagem passada. Os registros públicos de transparência de certificados, por sua vez, guardam todos os certificados emitidos para um domínio e revelam subdomínios e datas de emissão, inclusive de páginas que não aparecem nos buscadores. Ferramentas de identificação de tecnologias indicam a plataforma de comércio, o sistema de gestão de conteúdo e os serviços de terceiros usados no site, o que ajuda a comparar lojas falsas montadas com o mesmo modelo.

Google Public DNS ABERTO

Consulta registros DNS de um domínio pela interface web do serviço.

Cautela: Mostra a resolução atual, não a histórica.

dns.google/

crt.sh ABERTO

Pesquisa registros públicos de transparência de certificados por domínio.

Cautela: Certificado válido não atesta idoneidade do site.

crt.sh/

BuiltWith FREEMIUM

Identifica tecnologias e serviços usados por um site.

Cautela: Tecnologia não revela quem opera o site.

builtwith.com/

Wappalyzer FREEMIUM

Detecta plataformas e componentes de páginas, inclusive por extensão de navegador.

Cautela: Resultado pode ser incompleto.

www.wappalyzer.com/

Subfinder INSTALAÇÃO

Descobre subdomínios a partir de fontes públicas, de forma passiva.

Cautela: Algumas fontes exigem chaves; resultados podem ser antigos.

github.com/projectdiscovery/subfinder

7.4 Endereços IP, sistemas autônomos e geolocalização aproximada

Endereços IP identificam pontos de comunicação em redes, mas raramente apontam para uma pessoa. Redes móveis e residenciais compartilham um mesmo endereço público entre muitos usuários por meio de tradução de endereços, o NAT, e por isso o provedor precisa da porta lógica de origem, além do IP, da data e da hora com fuso, para individualizar a conexão. Serviços de VPN, proxies e hospedagem em nuvem acrescentam camadas intermediárias. A geolocalização de IP é uma estimativa ligada à infraestrutura do provedor, frequentemente situada em outra cidade, e jamais deve ser tratada como coordenada de residência.

Consultas a bases públicas de numeração e roteamento revelam o sistema autônomo, chamado ASN, e a organização responsável pelo bloco de endereços. É essa a informação que indica a quem dirigir a requisição ou o pedido judicial. Em exercícios, use endereços públicos de serviços conhecidos, como o DNS público 1.1.1.1, ou os blocos reservados para documentação, como 192.0.2.0/24 e 203.0.113.0/24, que não pertencem a usuários reais (Arkko; Cotton; Vegoda, 2010).

IPinfo FREEMIUM

Consulta ASN, organização e localização aproximada de um endereço IP.

Cautela: A localização normalmente não corresponde à de uma pessoa.

ipinfo.io/

RIPEstat ABERTO

Dados de roteamento, prefixos, sistemas autônomos e histórico.

Cautela: Roteamento não demonstra usuário individual.

stat.ripe.net/

ARIN RDAP ABERTO

Consulta a alocação de blocos de endereços e informações públicas da rede.

Cautela: O titular do bloco não é necessariamente o usuário.

search.arin.net/rdap/

BGP.Tools ABERTO

Informações de roteamento e de sistemas autônomos, com visualização simples.

Cautela: Anúncio de rota não atribui conduta a ninguém.

bgp.tools/

Shodan CADASTRO E PLANOS

Pesquisa serviços expostos à internet já indexados pelo próprio Shodan.

Cautela: Apenas observação passiva; nenhuma interação com os sistemas encontrados.

www.shodan.io/

Censys Platform CADASTRO E PLANOS

Pesquisa infraestrutura, serviços e certificados indexados.

Cautela: A antiga Legacy Search foi desativada para contas gratuitas; o plano gratuito usa créditos mensais.

platform.censys.io/

AbuseIPDB FREEMIUM

Reúne relatos de abuso associados a endereços IP.

Cautela: Relatos são indícios e podem conter erros.

www.abuseipdb.com/

A plataforma Censys ilustra como esses serviços mudam: a antiga interface de pesquisa deixou de atender usuários gratuitos e foi substituída por uma nova plataforma baseada em créditos (Censys, [s. d.]). Antes de recomendar uma ferramenta em relatório ou aula, confira se o acesso continua nas mesmas condições.

7.5 Do endereço IP à pessoa: o caminho jurídico

Em um caso real, o percurso típico combina pesquisa aberta e via formal. A pesquisa aberta identifica o domínio, a plataforma, o provedor de hospedagem e o sistema autônomo envolvidos. Com base nisso, a autoridade solicita a preservação dos registros e requer judicialmente o fornecimento dos registros de acesso à aplicação, que indicam IP, porta lógica, data e hora. Obtidos esses dados, nova ordem permite ao provedor de conexão informar qual assinante utilizava aquela conexão naquele instante (Brasil, 2014, arts. 13, 15 e 22). Mesmo então, o assinante não é necessariamente o autor: a conclusão depende de outros elementos.

Síntese do capítulo. Registrador, DNS, hospedagem, CDN, certificadora e operador desempenham papéis distintos. A data de criação do domínio e os registros de certificados são pistas valiosas, a geolocalização de IP é apenas aproximada, e a identificação do usuário exige porta lógica, horário preciso e a via formal do Marco Civil.

CAPÍTULO 8

Sites falsos, golpes e reputação

8.1 Triagem sem contaminar a investigação

A análise preliminar de uma página suspeita reúne domínio, anúncios, reputação, identidade visual, contatos, dados empresariais e histórico. Um preço muito abaixo do mercado ou um certificado de segurança não provam, isoladamente, fraude ou legitimidade: sites fraudulentos usam certificados válidos, imagens copiadas de marcas conhecidas e dados reais de empresas alheias. A comparação objetiva de vários sinais vale mais do que a impressão visual.

Serviços como urlscan.io e VirusTotal são úteis para consultar indicadores e capturas remotas de páginas. Entretanto, o envio de uma URL ou de um arquivo pode torná-lo visível a terceiros, conforme a modalidade de análise. Não submeta anexos de investigação, dados de vítimas, links de redefinição de senha ou endereços de acesso restrito. Consulte primeiro se já existem análises públicas do mesmo endereço e avalie, conforme a política institucional, se basta essa consulta ou se é necessária captura local em ambiente seguro.

> **urlscan.io** ABERTO OU CADASTRO
>
> Captura remota de páginas, com requisições, redirecionamentos e infraestrutura carregada.
>
> **Cautela:** Varreduras públicas ficam visíveis a outros usuários.
>
> urlscan.io/

> **VirusTotal** FREEMIUM E CADASTRO
>
> Agrega análises de URLs, domínios, IPs e arquivos por dezenas de mecanismos.
>
> **Cautela:** Arquivos enviados podem ser compartilhados com a comunidade de segurança.
>
> www.virustotal.com/

Google Transparency Report: status do site ABERTO

Informa se o Google classifica um endereço como inseguro.

Cautela: Ausência de alerta não significa que o site seja legítimo.

transparencyreport.google.com/safe-browsing/search

8.2 Sinais de alerta e contraprovas

Os sinais mais frequentes de loja falsa são o domínio recém-criado, o nome parecido com o de marca conhecida, preços incompatíveis com o mercado, pagamento apenas por Pix ou boleto a favor de pessoa física ou de empresa sem relação com a marca, ausência de canal de atendimento verificável, CNPJ de outra empresa no rodapé e anúncios pagos iniciados poucos dias antes. Cada sinal é indício a ser confrontado, e não conclusão. Para cada um, pergunte qual explicação legítima seria possível e qual consulta poderia afastá-la.

Exemplo hipotético. O rodapé da loja exibe um CNPJ ativo de uma empresa de tintas de outro estado. O domínio foi registrado nove dias antes, o certificado foi emitido no mesmo dia e a Biblioteca de Anúncios mostra campanhas iniciadas na véspera das primeiras reclamações. A empresa de tintas, contatada formalmente, declara desconhecer o site. A convergência de fontes independentes sustenta a hipótese de uso indevido do CNPJ por terceiros, e não de autoria pela empresa cadastrada.

Erro frequente. Concluir pela fraude a partir da nota de um único serviço de reputação, ou presumir legitimidade porque o navegador exibe o cadeado. O cadeado indica conexão criptografada, não honestidade de quem está do outro lado.

Síntese do capítulo. A triagem de sites suspeitos combina domínio, certificado, anúncios, dados empresariais e reputação, sem enviar material sensível a serviços públicos. Sinais de alerta são indícios a confrontar com explicações alternativas.

CAPÍTULO 9

Metadados e documentos digitais

9.1 O que os metadados revelam

Metadados são informações estruturadas associadas a um arquivo. Em fotografias, os campos EXIF e XMP podem indicar modelo de câmera ou celular, data e hora registradas pelo aparelho, configurações de captura e, às vezes, coordenadas geográficas. Em documentos PDF e de escritório, podem aparecer autor declarado, software produtor, datas de criação e modificação e histórico de edição. Em áudio e vídeo, aparecem contêiner, codec, duração e trilhas.

Esses campos são dados gravados no próprio arquivo, e não prova automática de autoria. O relógio do aparelho pode estar errado, o nome do autor pode ser o do proprietário do computador e não o de quem redigiu o texto, e qualquer campo pode ser alterado com programas de uso livre. Os metadados orientam hipóteses e diligências; sua força probatória depende do confronto com outros elementos e, quando necessário, do exame pericial.

9.2 Redes sociais removem e alteram metadados

A maioria das redes sociais e aplicativos de mensagens recomprime as imagens e remove boa parte dos metadados no envio. Por isso, a ausência de coordenadas em uma foto obtida de uma rede social não significa que o original não as tivesse, e a presença de coordenadas não comprova, isoladamente, o local da captura. Sempre que possível, obtenha o arquivo original diretamente da fonte, como a vítima ou o aparelho apreendido, com a documentação de cadeia de custódia correspondente.

9.3 Leitura local e segura

Metadados devem ser lidos em cópias de trabalho, com o hash do original calculado antes de qualquer operação. Prefira ferramentas locais, que não enviam o arquivo a terceiros. O ExifTool, mantido por Phil Harvey, é a referência para leitura de metadados em centenas de formatos (Harvey, [s. d.]);

o Poppler oferece utilitários para propriedades de PDF; e o Tesseract realiza reconhecimento óptico de caracteres, o OCR, em documentos digitalizados. O texto extraído por OCR contém erros, sobretudo em nomes, números e assinaturas, e deve ser sempre revisado contra a imagem de origem. O Apêndice E traz os comandos básicos.

ExifTool INSTALAÇÃO

Lê metadados de imagens, PDFs, áudio, vídeo e documentos, por linha de comando.

Cautela: Use apenas comandos de leitura e preserve o original.

exiftool.org/

Poppler INSTALAÇÃO

Utilitários locais para leitura de propriedades e texto de arquivos PDF.

Cautela: Obtenha os executáveis de fonte reconhecida.

poppler.freedesktop.org/

Tesseract OCR INSTALAÇÃO

Reconhecimento óptico de caracteres em imagens de documentos, com suporte ao português.

Cautela: Revise o texto reconhecido antes de usá-lo.

github.com/tesseract-ocr/tesseract

Erro frequente. Tratar o campo de data de criação como a data do fato, ou usar no relatório o texto extraído por OCR sem conferi-lo com a imagem. Ambos são dados técnicos sujeitos a erro e precisam ser contextualizados.

Síntese do capítulo. Metadados são indícios gravados no arquivo, sujeitos a relógio incorreto, alteração e supressão. A leitura deve ser local, em cópia de trabalho com hash do original, e o resultado precisa ser confrontado com outras fontes.

CAPÍTULO 10

Empresas, registros públicos e dados governamentais

10.1 Pessoas jurídicas e o CNPJ

Bases empresariais trazem dados de natureza cadastral e administrativa. Para verificar uma loja virtual ou um fornecedor, compare o CNPJ, a razão social, o nome fantasia, o endereço, a situação cadastral, a atividade econômica e o quadro de sócios com o que o site e os anúncios exibem. A consulta oficial ao cadastro de pessoas jurídicas é oferecida pelo governo federal por meio do Portal REDESIM (Brasil, [s. d.]). As juntas comerciais mantêm os atos constitutivos e alterações, e no estado de São Paulo a consulta é feita pela JUCESP.

A existência de empresa regularmente inscrita não comprova que o site pertença a ela. Golpistas utilizam dados de empresas reais, e a divergência entre o cadastro e o anúncio é, muitas vezes, o próprio indício da fraude. Registre a origem e a data de cada dado.

10.2 Transparência, diários oficiais e outras fontes públicas

O poder público disponibiliza bases que podem ser úteis à investigação, sempre dentro de sua finalidade. O Portal da Transparência reúne dados federais de despesas, servidores, convênios e cadastros de empresas sancionadas, como o CEIS e o CNEP. O Diário Oficial da União e os diários oficiais estaduais e municipais publicam nomeações, contratos, licitações e atos empresariais; o projeto Querido Diário organiza e permite pesquisar diários oficiais municipais de diversas cidades (Querido Diário, [s. d.]). O Tribunal Superior Eleitoral divulga candidaturas, bens declarados e prestação de contas eleitorais.

O Banco Nacional de Medidas Penais e Prisões, o BNMP, mantido pelo Conselho Nacional de Justiça, possui portal público de consulta a mandados de prisão e outras peças, com exigência de cadastro prévio do consulente (Conselho

Nacional de Justiça, [s. d.]). Profissionais de segurança pública dispõem de acesso próprio, mediante credenciamento, ao sistema completo.

Consultar CNPJ (gov.br e REDESIM) ABERTO

Serviço oficial de consulta a dados cadastrais de pessoas jurídicas.

Cautela: Empresa ativa não demonstra a regularidade de um anúncio específico.

www.gov.br/pt-br/servicos/consultar-cadastro-nacional-de-pessoas-juridicas

JUCESP Online ABERTO OU SERVIÇOS CONDICIONADOS

Pesquisa de registros empresariais na Junta Comercial do Estado de São Paulo.

Cautela: Informações variam conforme o tipo de consulta.

www.jucesponline.sp.gov.br/

Portal da Transparência ABERTO

Dados federais de gastos, servidores, convênios e sanções a empresas.

Cautela: Cobertura limitada às bases e períodos publicados.

portaldatransparencia.gov.br/

Diário Oficial da União ABERTO

Pesquisa de atos publicados no diário oficial federal.

Cautela: Atos estaduais e municipais estão em diários próprios.

www.in.gov.br/

Querido Diário ABERTO

Busca em diários oficiais de municípios brasileiros participantes do projeto.

Cautela: Nem todos os municípios estão cobertos.

queridodiario.org.br/

DivulgaCandContas (TSE) ABERTO

Candidaturas, bens declarados e contas eleitorais.

Cautela: Dados declarados pelos próprios candidatos.

divulgacandcontas.tse.jus.br/

Portal BNMP (CNJ) CADASTRO

Consulta pública a mandados de prisão e outras peças do BNMP.

Cautela: Confirme a situação da peça com o órgão expedidor.

portalbnmp.cnj.jus.br/

Erro frequente. Concluir que o anúncio foi publicado pela empresa cujo CNPJ aparece no rodapé, ou que toda divergência de endereço constitui fraude. O dado empresarial precisa ser confrontado com o domínio, os anúncios e os contatos efetivamente usados.

Síntese do capítulo. Cadastros oficiais, diários e portais de transparência oferecem dados de qualidade, mas com finalidade própria. Empresa ativa não é sinônimo de anúncio legítimo, e a divergência entre cadastro e anúncio é, muitas vezes, o indício mais relevante.

CAPÍTULO 11

Criptoativos e vestígios financeiros públicos

11.1 O que a blockchain mostra e o que esconde

Em redes públicas de criptoativos, como Bitcoin e Ethereum, as transações ficam registradas em um livro aberto, a blockchain, e podem ser consultadas por exploradores de blocos. É possível ver o identificador da transação, o bloco, o horário, os endereços envolvidos, os valores e, na Ethereum, contratos e tokens. O que a blockchain não mostra é quem controla cada endereço. A rastreabilidade é técnica; a identificação de pessoas depende, em regra, do ponto em que os valores passam por uma corretora ou outro prestador de serviços de ativos virtuais, que mantém cadastro dos clientes.

O marco legal dos ativos virtuais disciplinou a atividade desses prestadores e tipificou a fraude com utilização de ativos virtuais (Brasil, 2022). Na prática investigativa, a pesquisa aberta identifica a rede, as transações e os endereços de destino, e a via formal obtém, junto ao prestador, os dados do titular da conta que recebeu os valores.

11.2 Interpretar com cuidado

A interpretação exige identificar a rede correta, a unidade, as taxas e o modelo de transação. Na Bitcoin, uma transação pode ter várias entradas e saídas, incluindo o troco devolvido ao próprio remetente, e somar entradas e saídas sem entender esse modelo leva a valores errados. Rótulos atribuídos por plataformas e relatos comunitários de golpe são indícios que merecem verificação independente.

> **mempool.space** ABERTO
>
> Explorador de blocos, transações e endereços da rede Bitcoin.
>
> **Cautela:** Transferência registrada não identifica o beneficiário final.
>
> mempool.space/

Etherscan ABERTO

Consulta endereços, contratos, tokens e transações da rede Ethereum.

Cautela: Rótulos de entidades exigem validação adicional.

etherscan.io/

Chainabuse ABERTO OU CADASTRO

Relatos comunitários de golpes associados a endereços de criptoativos.

Cautela: Relatos são alegações, não prova de fraude.

www.chainabuse.com/

Erro frequente. Tratar o endereço de uma carteira como se fosse o nome de uma pessoa, confundir token com a moeda nativa da rede ou somar entradas e saídas sem compreender o modelo da transação.

Síntese do capítulo. A blockchain pública permite acompanhar o caminho dos valores, mas não revela quem controla cada endereço. O elo com pessoas surge, em regra, nos prestadores de serviços de ativos virtuais, alcançados pela via formal.

CAPÍTULO 12

Correlação, análise de vínculos e uso de inteligência artificial

12.1 Entidades, atributos e relações

A análise de vínculos organiza entidades (pessoas, perfis, domínios, e-mails, telefones, empresas, transações), seus atributos e as relações entre elas. A representação gráfica revela conexões, lacunas e pontos de convergência que a leitura linear esconde. Cada linha do gráfico, porém, precisa ter uma fonte. Diferencie a relação técnica ("o domínio resolveu para o IP"), a relação declarada ("o perfil aponta para o site"), a relação temporal ("publicações em horários próximos") e a inferência investigativa ("possível atuação coordenada").

Mais automação não significa mais confiabilidade. Ferramentas que cruzam dezenas de fontes podem retornar dados antigos, de fornecedores diferentes ou relacionados apenas por coincidência. Ao construir o gráfico, atribua um identificador a cada entidade, legende os tipos de relação e vincule cada conexão ao documento que a sustenta, inclusive aquelas descartadas ou contestadas.

Maltego FREEMIUM E CADASTRO

Visualiza entidades e conexões e integra fontes de dados por meio de transformações.

Cautela: Recursos e fontes dependem do plano contratado.

www.maltego.com/graph/

Gephi INSTALAÇÃO

Programa livre para visualizar e analisar redes de relações.

Cautela: O gráfico reproduz apenas a qualidade dos dados inseridos.

gephi.org/

SpiderFoot INSTALAÇÃO

Automatiza a coleta e o cruzamento de indicadores em fontes abertas.

Cautela: Configure apenas módulos passivos e fontes permitidas.

github.com/smicallef/spiderfoot

Recon-ng INSTALAÇÃO

Estrutura modular para organizar pesquisas em fontes abertas.

Cautela: Módulos podem exigir chaves e ter manutenção irregular.

github.com/lanmaster53/recon-ng

12.2 Inteligência artificial como apoio

Ferramentas de inteligência artificial ajudam a resumir grandes volumes de publicações, traduzir conteúdo estrangeiro, classificar documentos e sugerir hipóteses. Os riscos também são conhecidos: respostas plausíveis sem suporte, omissões, vieses e exposição de dados sigilosos ao fornecedor. O Volume 03 desta coleção trata o tema em profundidade. Em fontes abertas, a regra é simples: a IA pode organizar e sugerir, mas toda afirmação que ingressar no relatório deve ser conferida na fonte original preservada, e nenhum dado sigiloso deve ser inserido em serviço não autorizado pela instituição.

Erro frequente. Criar relações sem fonte, usar o tamanho de um nó no gráfico como prova de importância penal ou omitir os vínculos que enfraquecem a hipótese principal.

Síntese do capítulo. O gráfico de vínculos é instrumento de raciocínio, e cada aresta precisa de lastro documental. A automação e a inteligência artificial ampliam a capacidade de análise, mas não substituem a conferência na fonte nem a responsabilidade do analista.

CAPÍTULO 13

Preservação, cadeia de custódia e relatório

13.1 A captura de tela não é aquisição integral

Preservar conteúdo online significa documentar o que foi visto e, quando tecnicamente adequado, registrar os recursos necessários para reproduzi-lo. A captura de tela registra a aparência de uma interface naquele instante, mas omite o código, os endereços dos recursos carregados, os elementos dinâmicos e parte do contexto. É útil e muitas vezes indispensável, mas, isolada, é a forma mais frágil de preservação.

A escolha entre captura de tela, impressão em PDF, gravação em vídeo da navegação, arquivo web nos formatos WARC ou WACZ e download do arquivo original depende da pergunta e do tipo de conteúdo. O formato WARC é o padrão internacional de arquivamento da web, e o WACZ empacota as capturas com índices que permitem reproduzi-las depois. O Webrecorder, com a extensão ArchiveWeb.page, permite gravar sessões de navegação nesses formatos, inclusive em páginas dinâmicas (Webrecorder, [s. d.]). As orientações do Scientific Working Group on Digital Evidence e do National Institute of Standards and Technology dos Estados Unidos são referências metodológicas úteis, sem substituir a legislação brasileira e os procedimentos institucionais (Scientific Working Group on Digital Evidence, 2024; National Institute of Standards and Technology, 2022).

Quadro 4. Formas de preservação e o que cada uma documenta

Forma	O que documenta	Limitação principal
Captura de tela	Aparência da interface no momento	Não registra código, recursos nem URL de forma verificável
Impressão em PDF	Texto e layout da página	Pode alterar a diagramação e omitir conteúdo dinâmico
Gravação de vídeo da navegação	Sequência de acesso, rolagem e contexto	Arquivo grande; não captura o código
Arquivo WARC ou WACZ	Requisições, respostas e recursos da página	Exige ferramenta própria para reprodução
Download do arquivo original	O próprio arquivo publicado (imagem, vídeo, PDF)	Plataformas podem recomprimir o arquivo

Fonte: elaboração própria, com base em Scientific Working Group on Digital Evidence (2024) e National Institute of Standards and Technology (2022).

13.2 Hash e integridade

Hash é o resultado de uma função matemática aplicada a um arquivo, que produz uma sequência de tamanho fixo. Qualquer alteração de um único byte modifica completamente o resultado. O algoritmo SHA-256, padronizado pelo NIST, é o recomendado para registrar a integridade de arquivos preservados (National Institute of Standards and Technology, 2015). Calcule o hash logo após a preservação, registre-o na ficha da evidência e recalcule-o sempre que o arquivo for copiado ou apresentado. O Apêndice E mostra como fazê-lo no Windows e no Linux, com o comando oficial documentado pela Microsoft (Microsoft, [s. d.]).

O hash confirma que os bytes não mudaram desde o cálculo. Não demonstra que o conteúdo é verdadeiro, que a captura foi completa ou que a página não havia sido alterada antes da coleta. Por isso, ele complementa, e não substitui, o registro de origem, data, ambiente e método.

ArchiveWeb.page INSTALAÇÃO

Extensão do Webrecorder que grava sessões de navegação e exporta arquivos WARC e WACZ.

Cautela: Confira a captura e registre o que ficou de fora.

archiveweb.page/

Wayback Machine ABERTO

Arquivamento de páginas públicas em serviço de terceiros.

Cautela: Útil como registro complementar, não como preservação institucional.

web.archive.org/

QuickHash GUI INSTALAÇÃO

Programa local de cálculo e comparação de hashes de arquivos e pastas.

Cautela: Hash comprova igualdade de bytes, não veracidade.

github.com/tedsmith/quickhash

Hunchly COMERCIAL, COM PERÍODO DE AVALIAÇÃO

Registra automaticamente a navegação investigativa, com URLs, horários, hashes e capturas.

Cautela: Verifique licença, exportação e local de armazenamento.

www.hunch.ly/

13.3 O relatório auditável

O produto final deve permitir que outro profissional compreenda e refaça o caminho percorrido. Uma estrutura eficiente contém a identificação do procedimento e da pergunta que justificou a pesquisa; a delimitação jurídica, temporal e técnica; o método, os equipamentos e as ferramentas, com versões quando disponíveis; a relação cronológica das consultas, com URLs e anexos preservados; os achados objetivos, separados das inferências; as corroborações, divergências, limitações e hipóteses alternativas; as conclusões proporcionais ao material e as diligências complementares sugeridas; e o índice de anexos com hashes e registros de custódia.

Evite expressões de certeza quando os dados sustentam apenas possibilidade. Distinga o relato da vítima, a informação fornecida pela plataforma, a observação feita pelo policial e a interpretação do analista. A conclusão ideal informa não apenas o que foi encontrado, mas também o que permaneceu indeterminado e quais diligências legais poderiam reduzir a incerteza.

Síntese do capítulo. Preservar é documentar origem, momento, método e integridade. O formato deve ser escolhido conforme a pergunta, o hash SHA-256 garante a igualdade de bytes, e o relatório deve permitir que qualquer leitor técnico refaça o percurso e avalie suas limitações.

CAPÍTULO 14

Estudo de caso hipotético: a loja que não existia

14.1 O fato e a pergunta

Caso inteiramente fictício, criado para fins didáticos. Marta, moradora de uma cidade do interior paulista, comprou uma geladeira por menos da metade do preço de mercado em uma loja anunciada no Instagram, a "Casa Eletro Ofertas". Pagou por Pix a uma empresa cujo nome não coincidia com o da loja e, dez dias depois, sem receber o produto, procurou a delegacia com capturas do anúncio, o comprovante de pagamento e o endereço do site, aqui substituído pelo domínio de laboratório casaeletro-ofertas.invalid.

A pergunta investigativa foi delimitada assim: os elementos públicos ligados ao anúncio, ao site e ao recebedor do pagamento são compatíveis com uma loja regular ou indicam estrutura montada para fraude, e quais registros devem ser preservados e requisitados para identificar os responsáveis? A hipótese principal era a de loja fictícia. As alternativas eram loja real com falha de entrega e uso indevido de dados de empresa legítima por terceiros.

14.2 Preservação imediata

Antes de qualquer análise, a equipe preservou o perfil e o anúncio na interface oficial, com URL completa, identificador numérico e data e hora com fuso, gravou a sessão de navegação do site em arquivo WACZ e calculou o hash SHA-256 de cada arquivo. Solicitou também ao Instagram e ao provedor de hospedagem a preservação dos registros, com base no Marco Civil. Dois dias depois, o perfil foi desativado. Sem a preservação inicial, o anúncio estaria perdido.

14.3 Coleta e correlação

A Biblioteca de Anúncios mostrou cinco anúncios da mesma página, todos iniciados na mesma semana, com produtos de grandes marcas a preços

semelhantes. A consulta ao registro do domínio indicou criação doze dias antes dos anúncios, com dados do registrante protegidos por serviço de privacidade. Os registros de transparência de certificados mostraram um certificado emitido no mesmo dia do registro e um segundo subdomínio com o nome de outra loja, o que sugeria a reutilização da estrutura.

A busca reversa das fotografias dos produtos encontrou as mesmas imagens no site de um fabricante, publicadas meses antes. O CNPJ exibido no rodapé pertencia a uma empresa de reformas de outro estado, ativa e sem relação aparente com eletrodomésticos. O recebedor do Pix, conforme o comprovante, era uma terceira empresa, aberta quatro meses antes, com capital social mínimo.

Quadro 5. Atualização das hipóteses no estudo de caso

Hipótese	Elementos que a apoiam	Elementos que a enfraquecem
Loja fictícia montada para fraude	Domínio recente; imagens copiadas; CNPJ de terceiro; subdomínio de outra loja	Nenhum identificado até o momento
Loja real com falha de entrega	Pagamento recebido por empresa formalmente ativa	Ausência de estoque, endereço ou histórico comercial verificável
Uso indevido de dados de empresa legítima	CNPJ do rodapé de empresa de outro ramo e estado	Esclarecido como explicação parcial: a empresa do rodapé é vítima, não autora

Fonte: elaboração própria. Caso inteiramente hipotético.

14.4 Interpretação, limites e próximos passos

A convergência de fontes independentes sustentou a hipótese de estrutura montada para fraude e afastou a empresa de reformas como autora. Nada, porém, identificava ainda as pessoas responsáveis. O relatório registrou o que foi observado, as hipóteses avaliadas, as limitações e as diligências necessárias: requisição de dados cadastrais e pedido judicial de registros de acesso ao Instagram e ao provedor de hospedagem, informações sobre a conta recebedora

junto à instituição de pagamento, conforme as regras de sigilo bancário, e comunicação à empresa cujo CNPJ foi usado indevidamente.

Exemplo hipotético. Redação adequada para o relatório: "As consultas realizadas entre 3 e 5 de setembro de 2026 indicam que o domínio, o certificado e os anúncios foram criados em intervalo de doze dias e que as fotografias dos produtos reproduzem imagens publicadas anteriormente por fabricante. Esses elementos são compatíveis com estrutura destinada a fraude. A identificação dos responsáveis depende das diligências indicadas no item 6."

Síntese do capítulo. O caso mostra o método completo: pergunta delimitada, preservação antes da análise, fontes independentes, hipóteses alternativas enfrentadas e conclusão proporcional. A pesquisa aberta não identificou os autores, mas indicou com precisão onde estão os registros capazes de identificá-los.

CAPÍTULO 15

Oficinas práticas e casos simulados

15.1 Como realizar as oficinas

As oficinas a seguir foram escritas para formação policial e acadêmica. Todos os cenários são fictícios e devem ser realizados em ambiente de treinamento, com materiais próprios ou disponibilizados pelo instrutor, sem pesquisar pessoas reais. Para domínios, use a extensão reservada .invalid, que não corresponde a sites operacionais (Cheshire; Krochmal, 2013); para endereços IP, use os blocos de documentação ou o DNS público 1.1.1.1.

15.2 Oficina A. Loja anunciada em rede social

Situação: um consumidor viu anúncio patrocinado de loja de eletrônicos com preços muito baixos e possui apenas a captura do anúncio, o nome da página e o endereço do site. Roteiro: registre a URL do anúncio com data e fuso; consulte a Biblioteca de Anúncios; verifique o domínio no ICANN Lookup ou no Registro.br; confira o CNPJ informado; faça busca reversa das fotos; monte quadro com fatos confirmados, inconsistências, hipóteses alternativas e diligências formais necessárias.

> **Aprendizado.** Nenhum indício isolado comprova a fraude. Um CNPJ válido não autentica a loja, e uma imagem reproduzida em outros sites não demonstra, sozinha, a intenção de enganar.

15.3 Oficina B. Perfil com fotografia de terceiro

Situação: um perfil público usa fotografia de banco de imagens e se apresenta como profissional de uma área incompatível com a origem da foto. Roteiro: registre o identificador e a URL do perfil; submeta apenas a imagem de treinamento ao Google Lens e ao TinEye; anote ocorrências anteriores e contextos; pesquise o nome de usuário com Sherlock ou Maigret e valide manualmente; redija conclusão restrita.

Aprendizado. A reutilização da foto pode ser demonstrada, mas não define quem controla a conta. A pessoa fotografada pode ser vítima de uso indevido de imagem.

15.4 Oficina C. Metadados de documento

Situação: um PDF fornecido para a aula contém dados de software e datas de modificação. Roteiro: preserve o original em pasta separada e calcule seu SHA-256; execute o ExifTool e o pdfinfo na cópia; anote datas, aplicação produtora e campos ausentes; reexporte o documento em outro editor e compare.

Aprendizado. Metadados estão sujeitos a relógio incorreto, conversão e alteração. Hashes diferentes indicam bytes diferentes, e não, por si, manipulação dolosa.

15.5 Oficina D. Endereço IP em registro de acesso

Situação: os alunos recebem o endereço 1.1.1.1 como dado de exercício, sem atribuição a pessoa ou crime. Roteiro: consulte IPinfo e RIPEstat; anote organização, ASN e localização estimada; explique a diferença entre serviço, sistema autônomo e usuário; descreva o caminho jurídico necessário em caso real.

Aprendizado. Sem porta lógica, horário preciso com fuso e registros do provedor obtidos pela via formal, um endereço IP não individualiza ninguém.

15.6 Oficina E. Imagem com local controverso

Situação: uma fotografia publicada afirma retratar determinado município, sem geolocalização confiável. Roteiro: use imagem de treinamento com licença aberta; liste elementos arquitetônicos, relevo, vegetação, placas e direção da luz; compare Google Maps, Google Earth, OpenStreetMap e Mapillary; use o SunCalc apenas se houver dados suficientes; relate compatibilidades e incompatibilidades.

Aprendizado. Marcadores independentes e coerência temporal fortalecem a hipótese; imagens cartográficas antigas podem criar falsa correspondência.

15.7 Oficina F. Página alterada ou removida

Situação: uma página de treinamento muda de conteúdo entre duas datas. Roteiro: registre a versão atual; procure instantâneos na Wayback Machine; grave a sessão com ArchiveWeb.page; calcule o SHA-256 do arquivo; monte a linha do tempo com URLs, datas e diferenças.

> **Aprendizado.** Um instantâneo registra uma versão arquivada, não todo o histórico. A preservação deve indicar o que foi capturado e o que ficou de fora.

15.8 Oficina G. Apelidos iguais, pessoas diferentes

Situação: duas contas usam o mesmo nome de usuário; uma publica sobre esportes, a outra vende eletrônicos, e a ferramenta de enumeração apresenta ambas como resultado. Roteiro: registre a grafia exata e as URLs; compare biografia, idioma, período de atividade e links declarados; classifique cada vínculo como coincidência, possível vínculo ou vínculo corroborado.

> **Aprendizado.** A ferramenta comprovou apenas a ocorrência provável do identificador nas plataformas consultadas, segundo seus critérios de detecção.

15.9 Oficina H. Infraestrutura de página suspeita

Situação: o domínio de laboratório loja-exemplo.invalid aparece em simulação de anúncio. Roteiro: desenhe a cadeia URL, domínio, subdomínio, DNS, IP, certificado e hospedagem; consulte de forma passiva um domínio real autorizado pelo instrutor; registre as respostas de RDAP, DNS e crt.sh com data; identifique registrador, hospedagem e operador.

> **Aprendizado.** Registrador, hospedagem, DNS e operador exercem funções distintas. O uso de nuvem ou CDN é comum em serviços legítimos e não indica participação em ilícito.

15.10 Oficina I. Transação pública de criptoativo

Situação: o instrutor fornece o identificador de uma transação pública sem relação com procedimento policial. Roteiro: identifique a rede; abra o explorador correspondente; registre identificador, bloco, horário, valores e

endereços; separe dados da blockchain, rótulos de fornecedores e inferências; descreva a diligência formal necessária para identificar o titular.

> **Aprendizado.** A rastreabilidade das operações não equivale à identificação de pessoas, que depende, em regra, de dados mantidos por prestadores de serviços.

15.11 Oficina J. Resultado negativo bem documentado

Situação: a pesquisa por conteúdo supostamente publicado em 2024 não retorna resultados em 2026. Roteiro: descreva termos, datas, filtros e ferramentas; consulte arquivos da web; registre o resultado negativo com a fórmula do capítulo 3; indique documentos, testemunhos e registros que poderiam esclarecer a lacuna.

> **Aprendizado.** A ausência de resultado não permite concluir pela inexistência histórica da publicação, nem por sua remoção deliberada.

15.12 Critérios de avaliação

Para atividades em grupo, sugere-se avaliar cinco critérios, cada um com até dois pontos: delimitação da pergunta e formulação de hipótese alternativa; escolha proporcional das fontes e ferramentas; registro reprodutível de URLs, parâmetros, datas e resultados; preservação correta e respeito aos limites legais; e conclusão fundamentada, com distinção entre observação, hipótese e comprovação. A avaliação deve privilegiar o método. Um resultado negativo bem documentado vale mais do que uma conclusão afirmativa sem lastro.

Considerações finais

A investigação em fontes abertas é tanto mais valiosa quanto mais combina inteligência humana, método, preservação e controle jurídico. Nenhuma plataforma, isoladamente, substitui a verificação independente dos dados ou o dever de fundamentar conclusões. Uma ferramenta pode deixar de funcionar, uma publicação pode ser apagada e uma base pode conter erros. O procedimento bem documentado continua sendo a principal garantia de que a pesquisa possa ser explicada, revisada e contestada.

Ao longo deste volume, as técnicas foram apresentadas junto com seus limites: o identificador que não é pessoa, a geolocalização de IP que não é endereço, a captura de tela que não é aquisição integral, o hash que não prova veracidade, a empresa ativa que não autentica o anúncio. Essa honestidade metodológica não enfraquece a investigação. Ao contrário, é o que permite que seus resultados resistam ao contraditório e sirvam de base segura para as medidas que dependem de decisão judicial.

O profissional que domina as ferramentas de fontes abertas precisa conhecer também a fronteira entre observar e infiltrar, entre o dado público e o dado protegido, entre a pista e a prova. Respeitada essa fronteira, a pesquisa aberta é das mais eficientes aliadas da investigação criminal contemporânea: rápida, de baixo custo e capaz de indicar, com precisão, onde estão os registros que esclarecerão o fato.

APÊNDICE A

Consulta rápida: qual ferramenta escolher

Use o quadro como ponto de partida. Consulte o capítulo indicado para conhecer limitações, alternativas e o procedimento de registro.

Necessidade investigativa	Primeira consulta sugerida	Cap.
Pesquisar expressão exata, arquivo ou documento	Google Pesquisa Avançada; Bing	4
Consultar página antiga ou removida	Wayback Machine	4
Localizar nome de usuário em várias plataformas	Sherlock; Maigret; WhatsMyName	5
Examinar publicações de perfil público	Instagram; Facebook; TikTok; YouTube	5
Investigar anúncios de loja suspeita	Biblioteca de Anúncios da Meta	5 e 8
Verificar se uma imagem já circulava	Google Lens; TinEye	6
Verificar vídeo em circulação	InVID Verification Plugin	6
Testar o local de uma foto ou vídeo	Google Earth; Google Maps; Mapillary	6
Consultar registro de domínio	ICANN Lookup; Registro.br	7
Descobrir subdomínios e certificados	crt.sh	7
Consultar IP, ASN e provedor	IPinfo; RIPEstat; ARIN RDAP	7
Avaliar página suspeita	urlscan.io; VirusTotal	8
Ler metadados de foto ou PDF	ExifTool; Poppler	9
Conferir CNPJ ou empresa	Consultar CNPJ (gov.br); JUCESP	10
Pesquisar atos públicos e diários	Diário Oficial da União; Querido Diário	10
Verificar transação de criptoativo	mempool.space; Etherscan	11
Construir mapa de vínculos	Maltego; Gephi	12
Preservar página e conferir integridade	ArchiveWeb.page; QuickHash GUI	13

Fonte: elaboração própria.

APÊNDICE B

Ficha de planejamento da pesquisa

Procedimento e referência: _____

Responsável e data: _____

Fato investigado e finalidade da pesquisa

_____

_____

Pergunta investigativa

_____

_____

Hipótese principal: _____

Hipótese alternativa: _____

Identificadores já conhecidos: _____

Fontes e ferramentas previstas: _____

Período de interesse: _____

Base jurídica, limites e dados que não serão coletados

_____

_____

Forma de preservação e local de armazenamento: _____

Critério de encerramento da pesquisa: _____

Fonte: instrumento próprio. Adapte aos sistemas e normas da instituição.

APÊNDICE C

Registro de consulta em fonte aberta

Preencha uma linha por consulta relevante. Em investigações longas, mantenha o registro em planilha, com identificador único para cada item preservado.

Campo	O que registrar
Data, hora e fuso	Momento da consulta, com horário local e, se possível, UTC
Operador e ambiente	Servidor responsável, equipamento e navegador utilizados
Fonte	Serviço, URL completa e versão da ferramenta, quando houver
Consulta	Termo, identificador e parâmetros exatos
Resultado	Conteúdo observado, inclusive a ausência de resultado
Preservação	Arquivo, formato, local seguro e hash SHA-256
Confiabilidade	Confirmação externa, riscos e explicações alternativas
Encaminhamento	Diligência proposta, fundamento e responsável

Fonte: instrumento próprio.

Exemplo preenchido (simulação didática)

Procedimento: treinamento OSINT-001/2026. Data, hora e fuso: 3 set. 2026, 14h12 (UTC-3). Operador: agente de treinamento, perfil de navegação institucional. Fonte: Biblioteca de Anúncios da Meta, URL completa da pesquisa. Consulta: nome da página "Casa Eletro Ofertas", país Brasil, todos os anúncios. Resultado: cinco anúncios ativos, iniciados entre 21 e 23 ago. 2026. Preservação: captura de tela e arquivo WACZ da sessão, com SHA-256 registrado na ficha do item E-03. Confiabilidade: fonte primária da plataforma; datas de início confirmadas nos cinco anúncios. Encaminhamento: pedido de preservação de registros à Meta e confronto com a data de registro do domínio. Os dados são fictícios e não representam consulta real.

APÊNDICE D

Checklist antes de encaminhar os resultados

- ☐ A pesquisa tem finalidade legítima, delimitada e registrada.
- ☐ Nenhuma barreira de acesso foi superada e não houve interação sob identidade fictícia sem autorização.
- ☐ Todas as URLs relevantes estão registradas por completo.
- ☐ Datas e horários estão acompanhados de fuso horário.
- ☐ Termos exatos, filtros e versões das ferramentas foram anotados.
- ☐ Fontes primárias, secundárias e automatizadas estão diferenciadas.
- ☐ Resultados negativos e limitações foram registrados.
- ☐ Nenhuma identidade ou autoria foi concluída apenas por nome de usuário, foto ou IP.
- ☐ Nenhum material sigiloso ou dado de vítima foi enviado a serviço público.
- ☐ O material foi preservado e os hashes SHA-256 estão documentados.
- ☐ Hipóteses alternativas e elementos favoráveis ao investigado foram considerados.
- ☐ O relatório permite que outro profissional refaça o procedimento.

Fonte: instrumento próprio.

APÊNDICE E

Comandos locais de integridade e metadados

Os comandos abaixo são de leitura e devem ser executados em cópias de trabalho de arquivos próprios ou formalmente disponibilizados. Os nomes de arquivo são ilustrativos. Preserve o original, registre a ferramenta e a versão utilizadas e não execute programas baixados de anúncios ou fontes desconhecidas.

Calcular SHA-256 no Windows (PowerShell)

```
Get-FileHash -Algorithm SHA256 -Path "C:\dados\arquivo.pdf"
```

O resultado mostra o algoritmo, o valor hexadecimal e o caminho do arquivo. Anote o valor no registro da evidência (Microsoft, [s. d.]).

Calcular SHA-256 no Windows (Prompt de Comando)

```
certutil -hashfile C:\dados\arquivo.pdf SHA256
```

Calcular SHA-256 no Linux

```
sha256sum arquivo.pdf
```

Compare cópias usando sempre o mesmo algoritmo. Se o arquivo for convertido, redimensionado ou recompactado, o hash mudará, ainda que o conteúdo visível pareça idêntico.

Ler metadados com o ExifTool

```
exiftool -G1 -a -s arquivo.jpg

exiftool -time:all -a -G1 -s arquivo.pdf
```

A opção -G1 mostra o grupo de cada campo, -a inclui campos duplicados e -s exibe os nomes técnicos. Esses comandos não gravam alterações no arquivo.

Ler propriedades de PDF com o Poppler

```
pdfinfo arquivo.pdf
```

A saída indica título, autor declarado, software produtor, número de páginas e datas registradas. Diferenças entre ferramentas não significam, necessariamente, adulteração.

Extrair texto de imagem com o Tesseract

```
tesseract imagem_treino.png saida -l por
```

O pacote de idioma português precisa estar instalado. Revise o texto reconhecido contra a imagem original, sobretudo nomes, números e datas.

APÊNDICE F

Glossário

ASN. Número que identifica um sistema autônomo, isto é, uma rede ou conjunto de redes sob a mesma administração na internet.

Cadeia de custódia. Conjunto de procedimentos que documentam a história cronológica do vestígio, desde o reconhecimento até o descarte (CPP, art. 158-A).

CDN. Rede de distribuição de conteúdo que intermedeia o acesso aos sites e pode ocultar o servidor de origem.

Certificado digital TLS. Arquivo que permite a conexão criptografada com o site; não atesta a idoneidade de quem o opera.

DNS. Sistema que traduz nomes de domínio em endereços e outros registros técnicos.

EXIF e XMP. Padrões de metadados gravados em imagens e outros arquivos.

Falso positivo. Resultado que parece atender ao critério pesquisado, mas não corresponde ao fato.

Hash. Resultado de função matemática aplicada a um arquivo, usado para verificar se seus bytes permanecem iguais.

Identificador. Valor como nome de usuário, e-mail, domínio ou número de conta, que não equivale à identidade civil.

Infiltração virtual. Atuação de agente de polícia na internet com identidade oculta, admitida nas hipóteses legais e mediante autorização judicial.

Metadado. Informação que descreve características técnicas ou administrativas de um arquivo.

NAT. Tradução de endereços que permite a vários usuários compartilharem o mesmo IP público.

OCR. Reconhecimento óptico de caracteres em imagens de texto.

OPSEC. Segurança operacional; cuidados que protegem o investigador e a investigação.

OSINT. Inteligência de fontes abertas; pesquisa metódica em fontes legalmente acessíveis.

Porta lógica. Número que, junto com o IP, individualiza uma conexão em redes com endereços compartilhados.

RDAP. Protocolo atual de consulta a dados de registro de domínios e endereços IP, sucessor do Whois.

WARC e WACZ. Formatos de arquivamento de páginas da web que guardam requisições, respostas e recursos.

APÊNDICE G

Índice de ferramentas e endereços

Os nomes são clicáveis no arquivo digital. Finalidades, condições de acesso e cautelas estão descritas nos capítulos indicados no Apêndice A.

Ferramenta	Endereço oficial
AbuseIPDB	www.abuseipdb.com/
ArchiveWeb.page	archiveweb.page/
ARIN RDAP	search.arin.net/rdap/
Bellingcat Online Investigation Toolkit	bellingcat.gitbook.io/toolkit
BGP.Tools	bgp.tools/
Biblioteca de Anúncios da Meta	www.facebook.com/ads/library/
Bing	www.bing.com/
Bing Visual Search	www.bing.com/visualsearch
BuiltWith	builtwith.com/
Censys Platform	platform.censys.io/
Chainabuse	www.chainabuse.com/
Consultar CNPJ (gov.br e REDESIM)	www.gov.br/pt-br/servicos/consultar-cadastro-nacional-de-pessoas-juridicas
Copernicus Browser	browser.dataspace.copernicus.eu/
crt.sh	crt.sh/
DivulgaCandContas (TSE)	divulgacandcontas.tse.jus.br/
Diário Oficial da União	www.in.gov.br/
Etherscan	etherscan.io/
ExifTool	exiftool.org/
Facebook	www.facebook.com/
Gephi	gephi.org/
GitHub	github.com/search
Google Earth	earth.google.com/
Google Fact Check Explorer	toolbox.google.com/factcheck/explorer

Ferramenta	Endereço oficial
Google Lens	lens.google/
Google Maps	www.google.com/maps/
Google Pesquisa Avançada	www.google.com/advanced_search
Google Public DNS	dns.google/
Google Transparency Report: status do site	transparencyreport.google.com/safe-browsing/search
Google Trends	trends.google.com/trends/
Have I Been Pwned	haveibeenpwned.com/
Hunchly	www.hunch.ly/
Hunter	hunter.io/domain-search
ICANN Lookup	lookup.icann.org/
Instagram	www.instagram.com/
Instaloader	github.com/instaloader/instaloader
InVID Verification Plugin	www.invid-project.eu/tools-and-services/invid-verification-plugin/
IPinfo	ipinfo.io/
JUCESP Online	www.jucesponline.sp.gov.br/
LinkedIn	www.linkedin.com/
Maigret	github.com/soxoj/maigret
Maltego	www.maltego.com/graph/
Mapillary	www.mapillary.com/app/
MediaInfo	mediaarea.net/en/MediaInfo
mempool.space	mempool.space/
Meta Content Library e API	developers.facebook.com/docs/content-library-and-api/
OpenStreetMap	www.openstreetmap.org/

Ferramenta	Endereço oficial
OSINT Framework	osintframework.com/
Poppler	poppler.freedesktop.org/
Portal BNMP (CNJ)	portalbnmp.cnj.jus.br/
Portal da Transparência	portaldatransparencia.gov.br/
Querido Diário	queridodiario.org.br/
QuickHash GUI	github.com/tedsmith/quickhash
Recon-ng	github.com/lanmaster53/recon-ng
Registro.br	registro.br/tecnologia/ferramentas/whois/
RIPEstat	stat.ripe.net/
Sherlock	github.com/sherlock-project/sherlock
Shodan	www.shodan.io/
SpiderFoot	github.com/smicallef/spiderfoot
Subfinder	github.com/projectdiscovery/subfinder
SunCalc	www.suncalc.org/
Telegram Web	web.telegram.org/
Tesseract OCR	github.com/tesseract-ocr/tesseract
TikTok	www.tiktok.com/
TinEye	tineye.com/
urlscan.io	urlscan.io/
VirusTotal	www.virustotal.com/
Wappalyzer	www.wappalyzer.com/
Wayback Machine	web.archive.org/
WhatsMyName	whatsmyname.app/
X (pesquisa avançada)	x.com/search-advanced
YouTube	www.youtube.com/

Referências

ARKKO, J.; COTTON, M.; VEGODA, L. **IPv4 address blocks reserved for documentation**. [S. l.]: Internet Engineering Task Force, 2010. (RFC 5737). Disponível em: https://www.rfc-editor.org/rfc/rfc5737.html. Acesso em: 2 set. 2026.

BELLINGCAT. **A beginner's guide to social media verification**. [S. l.]: Bellingcat, 2021. Disponível em: https://www.bellingcat.com/resources/how-tos/2021/11/01/a-beginners-guide-to-social-media-verification/. Acesso em: 27 set. 2026.

BELLINGCAT. **Chasing shadows: geolocate images with Bellingcat's Shadow Finder Tool**. [S. l.]: Bellingcat, 2024. Disponível em: https://www.bellingcat.com/resources/2024/08/22/shadow-geolocate-geolocation-locate-image-tool-open-source-bellingcat-measure/. Acesso em: 9 out. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 ago. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 ago. 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 7 set. 2026.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 3 set. 2026.

BRASIL. Lei nº 12.830, de 20 de junho de 2013. **Dispõe sobre a investigação criminal conduzida pelo delegado de polícia**. Brasília, DF: Presidência da República, 2013a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 1 out. 2026.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal**. Brasília, DF: Presidência da República, 2013b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 22 out. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 out. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 ago. 2026.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. **Aperfeiçoa a legislação penal e processual penal**. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 23 set. 2026.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. **Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais**. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Acesso em: 26 set. 2026.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. **Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente)**. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 10 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Agravo Regimental no Habeas Corpus 828.054/RN**. Relator: Min. Joel Ilan Paciornik. Julgado em 23 abr. 2024. Diário da Justiça Eletrônico, Brasília, DF, 29 abr. 2024.

BRASIL. **Consultar Cadastro Nacional de Pessoas Jurídicas**. Brasília, DF: gov.br, [s. d.]. Disponível em: https://www.gov.br/pt-br/servicos/consultar-cadastro-nacional-de-pessoas-juridicas. Acesso em: 16 set. 2026.

CENSYS. **Censys Legacy Search**. [S. l.]: Censys, [s. d.]. Disponível em: https://search.censys.io/. Acesso em: 11 nov. 2026.

CHESHIRE, S.; KROCHMAL, M. **Special-use domain names**. [S. l.]: Internet Engineering Task Force, 2013. (RFC 6761). Disponível em: https://www.rfc-editor.org/rfc/rfc6761.html. Acesso em: 13 out. 2026.

CONSELHO NACIONAL DE JUSTIÇA. **BNMP 3.0: Banco Nacional de Medidas Penais e Prisões**. Brasília, DF: CNJ, [s. d.]. Disponível em: https://www.cnj.jus.br/sistema-carcerario/bnmp-3-0/. Acesso em: 5 out. 2026.

EUROPEAN SPACE AGENCY. **How to use Copernicus Browser in your classroom**. [S. l.]: ESA Education, 2026. Disponível em: https://education.esa.int/copernicus_browser_guide/. Acesso em: 14 nov. 2026.

GOOGLE. **Refine Google searches**. Mountain View: Google, [s. d.]. Disponível em: https://support.google.com/websearch/answer/2466433. Acesso em: 31 ago. 2026.

HARVEY, Phil. **ExifTool**. [S. l.]: Phil Harvey, [s. d.]. Disponível em: https://exiftool.org/. Acesso em: 13 set. 2026.

ICANN. **ICANN Lookup**. [S. l.]: ICANN, [s. d.]. Disponível em: https://lookup.icann.org/. Acesso em: 30 set. 2026.

INTERNET ARCHIVE. **Using the Wayback Machine**. San Francisco: Internet Archive, [s. d.]. Disponível em: https://archivesupport.zendesk.com/hc/en-us/articles/360004651732-Using-The-Wayback-Machine. Acesso em: 21 ago. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais**. 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

META. **Meta Content Library and API**. Menlo Park: Meta, [s. d.]a. Disponível em: https://developers.facebook.com/docs/content-library-and-api/. Acesso em: 6 nov. 2026.

META. **Get access to Meta Content Library and API**. Menlo Park: Meta, [s. d.]b. Disponível em: https://developers.facebook.com/docs/content-library-and-api/get-access. Acesso em: 18 nov. 2026.

MICROSOFT. **Get-FileHash (Microsoft.PowerShell.Utility)**. Redmond: Microsoft Learn, [s. d.]. Disponível em: https://learn.microsoft.com/pt-br/powershell/module/microsoft.powershell.utility/get-filehash. Acesso em: 6 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Secure Hash Standard (SHS)**. Gaithersburg: NIST, 2015. (FIPS PUB 180-4). DOI: 10.6028/NIST.FIPS.180-4. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Acesso em: 8 nov. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Digital evidence preservation: considerations for evidence handlers**. Gaithersburg: NIST, 2022. (NIST IR 8387). DOI: 10.6028/NIST.IR.8387. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf. Acesso em: 4 ago. 2026.

QUERIDO DIÁRIO. **Querido Diário: diários oficiais municipais**. [S. l.]: Open Knowledge Brasil, [s. d.]. Disponível em: https://queridodiario.org.br/. Acesso em: 28 out. 2026.

REGISTRO.BR. **Serviço de diretório Whois**. São Paulo: NIC.br, [s. d.]. Disponível em: https://registro.br/tecnologia/ferramentas/whois/. Acesso em: 25 ago. 2026.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **Best practices for acquiring online content**. [S. l.]: SWGDE, 2024. Disponível em: https://www.swgde.org/wp-content/uploads/2024/04/2024-03-15-SWGDE-Best-Practices-for-Acquiring-Online-Content-21-F-001-1.1.pdf. Acesso em: 17 out. 2026.

WEBBREACHER. **WhatsMyName**. [S. l.]: GitHub, [s. d.]. Disponível em: https://github.com/WebBreacher/WhatsMyName. Acesso em: 19 nov. 2026.

WEBRECORDER. **ArchiveWeb.page**. [S. l.]: Webrecorder, [s. d.]. Disponível em: https://webrecorder.net/archivewebpage/. Acesso em: 2 nov. 2026.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne nove cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

Vol. 01 **Investigação Criminal Tecnológica**. Fundamentos, métodos e aplicações práticas

Vol. 02 **Provas digitais e cadeia de custódia**. Da coleta à valoração jurídica

Vol. 03 **Inteligência artificial na investigação criminal**. Aplicações, limites e boas práticas

Vol. 04 **Golpes digitais e fraudes eletrônicas**. Prevenção, identificação e investigação

Vol. 05 **Investigação de crimes na internet**. Dados, registros, sigilos e medidas judiciais

Vol. 06 **Raciocínio investigativo e decisão fundamentada**. Do indício ao relatório final

Vol. 07 **Internet segura**. Guia prático para proteger você e sua família

Vol. 08 **Crianças e adolescentes na internet**. Guia de proteção para pais e responsáveis

Vol. 09 **Investigação em fontes abertas**. Guia prático de OSINT para a investigação criminal (este volume)

Canais oficiais do autor

Site	www.higorjorge.com.br
YouTube	youtube.com/@direitoetecnologia
Instagram	@higorjorge
Facebook	facebook.com/professorhigorjorge