

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 02

Provas digitais e cadeia de custódia

Da coleta à valoração jurídica



02

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Provas digitais e cadeia de custódia

Da coleta à valoração jurídica

Como reconhecer, preservar, obter, examinar e apresentar vestígios digitais com rastreabilidade, controle de legalidade e respeito ao contraditório.

Coleção Investigação e Proteção na Era Digital
Volume 02

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 02.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Provas digitais e cadeia de custódia : da coleta à valoração jurídica [recurso eletrônico] / Higor Vinicius Nogueira Jorge.

-- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (53 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 2)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências e apêndices.

Publicação de distribuição gratuita.

1. Prova digital. 2. Cadeia de custódia. 3. Investigação criminal. 4. Perícia computacional. 5. Processo penal. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 Conceito e particularidades da prova digital.....	7
2 Fundamentos legais e admissibilidade.....	10
3 Origem, integridade, autenticidade, atribuição e contexto.....	13
4 Cadeia de custódia e etapas do CPP.....	17
5 Dispositivos eletrônicos.....	21
6 Mensagens, capturas, áudios e arquivos.....	25
7 Nuvem, registros, metadados e fontes distribuídas.....	28
8 Falhas de preservação e impactos probatórios.....	31
9 Estudo de caso hipotético de extorsão digital.....	34
10 Boas práticas e documentação da prova.....	38
Considerações finais.....	41
Apêndice A. Formulário de identificação de evidências.....	42
Apêndice B. Modelo de movimentação e acesso.....	44
Apêndice C. Checklist de cadeia de custódia.....	46
Referências.....	48
Minicurrículo do autor.....	50
Para aprofundar o estudo.....	52
A coleção.....	53

Apresentação

Uma conversa recebida no celular, uma gravação de câmera e um registro de acesso podem esclarecer o mesmo fato. Também podem induzir a conclusões erradas quando sua origem, seu percurso ou seu significado são tratados como evidentes. Investigar exige demonstrar como o dado foi obtido, o que efetivamente contém e até onde permite concluir.

Este volume desenvolve essa responsabilidade. A cadeia de custódia conecta o vestígio apresentado ao histórico de sua obtenção e de seu tratamento. Sua documentação torna examináveis as escolhas técnicas e permite localizar falhas, transformações e limites. O cuidado começa no reconhecimento do elemento relevante e continua durante a guarda, a análise e a apresentação.

No livro *Investigação criminal tecnológica: fundamentos, método e limites* na era dos vestígios informacionais, sustento que o modo de obtenção participa da avaliação do resultado. A presente cartilha aprofunda essa orientação, especialmente em relação às particularidades dos dispositivos, das mensagens e dos registros distribuídos (Jorge, 2027).

O leitor encontrará explicações, situações hipotéticas e instrumentos para uso profissional. A finalidade é melhorar decisões reais: o que preservar, qual acesso precisa ser fundamentado, que exame requisitar e como apresentar conclusões compatíveis com os elementos disponíveis. A qualidade da prova depende de escolhas que possam ser explicadas e submetidas à crítica.

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

Esta cartilha destina-se a Delegados de Polícia, policiais civis, peritos, profissionais da investigação, operadores do Direito, estudantes e pesquisadores. Pressupõe interesse na apuração de fatos e explica os termos técnicos necessários, sem exigir domínio prévio de ferramentas periciais.

Ao final da leitura, espera-se que o profissional consiga delimitar o objeto digital relevante, distinguir preservação e acesso, reconhecer o alcance de uma aquisição e organizar a documentação necessária à revisão do trabalho. Outro objetivo é avaliar criticamente a relação entre arquivo, pessoa e fato investigado.

O volume trata a prova digital como assunto transversal. Um homicídio, uma extorsão ou um desvio patrimonial podem envolver vestígios informacionais. O ambiente digital pode ser cenário, instrumento, fonte de informação ou local de armazenamento, sem que o delito seja necessariamente um crime cibernético (Jorge, 2027).

Como utilizar

Os capítulos 1 a 4 apresentam conceitos, direitos e responsabilidades. Os capítulos 5 a 8 examinam fontes, procedimentos e falhas. O caso do capítulo 9 integra essas escolhas; o capítulo 10 orienta a documentação e a apresentação. Os apêndices oferecem três modelos de registro.

Os modelos não substituem autos, laudos ou sistemas oficiais. Campos sem informação devem ser identificados como desconhecidos ou não aplicáveis. Um formulário completo de aparência, preenchido com suposições, prejudica a rastreabilidade.

CAPÍTULO 1

Conceito e particularidades da prova digital

1.1 O vestígio e a afirmação que se pretende demonstrar

Prova digital envolve informações representadas em meio digital e utilizadas para esclarecer fatos juridicamente relevantes. Para trabalhar com precisão, convém separar o vestígio encontrado, a fonte que o contém, o meio de obtenção e a conclusão pretendida. Um arquivo de vídeo é um objeto; o equipamento que o armazenava é uma fonte; a exportação é um procedimento. A afirmação de que alguém esteve no local é uma interpretação que ainda exige exame.

O emprego da expressão prova digital nesta cartilha abrange o percurso probatório, sem atribuir automaticamente a todo dado recolhido o valor de prova judicial. Elementos obtidos na investigação precisam ser tratados segundo sua natureza e submetidos às regras do Código de Processo Penal (CPP), conforme sua natureza (Brasil, 1941, art. 155).

A abordagem acompanha o objeto material da Investigação Criminal Tecnológica: o vestígio informacional juridicamente relevante. Seu interesse depende da pergunta investigativa. Milhares de arquivos podem ser irrelevantes; uma configuração de relógio pode explicar uma aparente contradição decisiva (Jorge, 2027).

Exemplo hipotético. Uma câmera registra uma pessoa retirando uma caixa. A imagem pode demonstrar um deslocamento, mas não esclarece, sozinha, o conteúdo da caixa, a autorização para retirá-la ou a identidade da pessoa. Cada afirmação demanda suporte próprio. Preservar o vídeo é necessário para examinar essas questões, sem antecipar suas respostas.

1.2 Alterabilidade e dependência do ambiente

Vestígios digitais dependem de sistemas para sua criação, armazenamento e interpretação. Um mesmo conjunto de bytes pode ser exibido de maneiras diferentes conforme o programa, a configuração ou o formato empregado.

Abrir uma base de mensagens em um visualizador não equivale a reproduzir integralmente o funcionamento do aplicativo que a produziu.

A volatilidade varia entre fontes. A memória de um equipamento em funcionamento pode mudar continuamente; um arquivo estável em mídia preservada permite comparações sucessivas. A estratégia deve responder à condição real do vestígio. A palavra digital não justifica um único procedimento para todos os objetos.

Jorge (2027) destaca a alterabilidade, a volatilidade e a dependência do contexto como dificuldades centrais. Uma consequência prática é registrar o estado encontrado e as intervenções realizadas. Se o equipamento precisou permanecer ligado, o motivo e seus efeitos previsíveis integram a documentação. O objetivo é controlar e explicar a intervenção tecnicamente necessária.

Também existe dependência de credenciais, chaves criptográficas e infraestrutura. A posse física de um suporte pode não permitir leitura; uma sessão acessível pode perder-se por alteração do estado do sistema. Esses riscos devem ser avaliados por equipe capacitada, dentro da autorização jurídica aplicável.

Erro frequente. Tratar a facilidade de visualização como demonstração de confiabilidade. Uma tela clara pode omitir dados essenciais; um arquivo ilegível ao usuário pode conter informações relevantes. A aparência da interface não define o alcance probatório.

1.3 Fonte, objeto e representações derivadas

A noção de original precisa ser descrita com cuidado. No meio digital, podem existir cópias com o mesmo conteúdo binário em suportes distintos. A descrição deve apontar qual objeto foi recebido, sua relação com a fonte e o procedimento que produziu a cópia. Chamar tudo de original encobre diferenças relevantes.

Considere uma filmagem exportada de um gravador e depois convertida para reprodução em audiência. O arquivo exportado e a conversão são objetos relacionados, mas possuem históricos próprios. A conversão pode facilitar a

compreensão e alterar compressão, metadados ou qualidade. Deve ser identificada como derivada e vinculada ao arquivo preservado.

Objeto	Pergunta de controle
Suporte apreendido	Qual equipamento, em que estado e sob qual identificação?
Arquivo recebido	Quem o entregou e como foi produzido ou exportado?
Cópia de trabalho	De qual objeto deriva e como foi conferida?
Recorte ou conversão	O que foi selecionado ou transformado e com qual finalidade?

Síntese do capítulo. Definir a prova começa por individualizar objetos e perguntas. O controle continua na relação entre cada representação e a fonte correspondente. A confiabilidade deve ser examinada por aspectos verificáveis, sem depender da designação atribuída ao arquivo. Nas páginas seguintes, a legalidade da obtenção será articulada com esse controle técnico.

CAPÍTULO 2

Fundamentos legais e admissibilidade

2.1 Direitos fundamentais orientam a obtenção

O uso de tecnologia deve respeitar intimidade, privacidade, proteção de dados, devido processo e defesa. A Constituição também veda provas ilícitas. Esses parâmetros orientam a escolha da fonte, a extensão da medida e a destinação do material, inclusive quando a ferramenta permite acesso muito mais amplo (Brasil, 1988, art. 5º).

A análise jurídica começa pela descrição da intervenção. Apreender um equipamento, consultar seu conteúdo, obter registros de um provedor e acompanhar comunicações em curso são ações distintas. O profissional deve identificar a base legal e o âmbito da autorização para cada uma. A regularidade de uma ação não autoriza presumir a regularidade das demais.

Essa separação evita diligências genéricas. Em uma investigação sobre mensagens de determinado período, deve-se explicar a pertinência das contas, dos intervalos e das categorias de dados pretendidas. A extensão tecnicamente necessária à aquisição pode diferir da extensão do exame autorizado; essa diferença exige controle explícito.

Exemplo hipotético. Um mandado permite apreender computador ligado a uma fraude. A equipe não deve concluir que qualquer serviço externo acessível por uma sessão salva integra automaticamente o objeto da autorização. Deve registrar a situação, preservar o que legitimamente lhe compete e submeter a necessidade de acesso adicional à avaliação jurídica da autoridade responsável.

2.2 Categorias de dados e meios de obtenção

O Marco Civil distingue registros de conexão, registros de acesso a aplicações, dados pessoais e conteúdo de comunicações. A disponibilização de registros protegidos e de comunicações privadas observa os requisitos legais e a reserva judicial. O art. 10, § 3º, contempla dados cadastrais delimitados, para

autoridades com competência legal, sem converter qualquer informação sobre uma conta em cadastro livremente requisitável (Brasil, 2014).

O acompanhamento de comunicações em curso exige análise própria. A Lei nº 9.296/1996 disciplina a interceptação e estabelece pressupostos de necessidade e autorização judicial. Não se deve usar a expressão quebra de sigilo como se descrevesse, com precisão, todas as intervenções possíveis (Brasil, 1996, arts. 1º a 5º).

O acesso legítimo de um participante à própria conversa também precisa ser diferenciado de uma intervenção estatal na comunicação alheia. Na entrega voluntária, documentam-se identidade, capacidade de disposição, conteúdo entregue e circunstâncias. Essa entrega não concede acesso irrestrito a contas, dispositivos ou conversas de terceiros.

Orientação prática. Descrever o dado pretendido, quem o mantém, o período, a relação com o fato, a forma de obtenção e os limites de uso. Se a obtenção depender de decisão judicial, esses elementos subsidiam a representação fundamentada. Requisição, cooperação técnica e preservação não substituem a autorização que a lei exigir.

2.3 Responsabilidades jurídicas e técnicas

Na investigação conduzida por Delegado de Polícia, cabe à autoridade exercer as competências legais de direção, requisitar os exames pertinentes e fundamentar suas decisões. O indiciamento exige análise técnico-jurídica própria e motivada; a ferramenta de extração não produz esse ato (Brasil, 2013, art. 2º).

À perícia compete o exame especializado segundo a disciplina processual. Um relatório de investigação pode organizar informações e apontar diligências, mas não deve ser apresentado como laudo pericial por simples mudança de título. Quando o fato deixa vestígios, é necessário observar as exigências de exame de corpo de delito e as regras relativas aos peritos (Brasil, 1941, arts. 158 e 159).

A divisão de responsabilidades funciona melhor quando existe comunicação. A requisição deve formular perguntas técnicas, informar o objeto autorizado e

indicar circunstâncias relevantes. O perito precisa conhecer, por exemplo, que houve manipulação anterior ou que o horário do aparelho parece divergente. O silêncio sobre essas condições pode comprometer a interpretação.

Exemplo hipotético. Em vez de requisitar que se prove quem cometeu o crime, a autoridade pergunta se há mensagens do período delimitado, quais identificadores as vinculam à base examinada e quais limitações afetam a leitura. A investigação correlaciona esse resultado com outros elementos. A individualização jurídica permanece sujeita à análise do conjunto, com consideração das hipóteses alternativas.

2.4 Admissibilidade, confiabilidade e força explicativa

A admissibilidade examina se o elemento pode ingressar e permanecer validamente no processo. A confiabilidade técnica investiga sua obtenção e seu tratamento. A força explicativa diz respeito ao que ele sustenta no caso concreto. Essas perguntas se relacionam, mas pedem respostas próprias.

Um arquivo tecnicamente íntegro pode ter sido obtido ilicitamente. Um material obtido por via regular pode ser insuficiente para identificar o autor. A preservação de bytes não supre a legalidade do acesso nem demonstra a veracidade de toda declaração registrada. A Constituição e o art. 157 do CPP disciplinam a exclusão da prova ilícita; a avaliação não se encerra em uma conferência de hash (Brasil, 1988; Brasil, 1941).

A proteção dos dados continua após o recebimento. A Lei Geral de Proteção de Dados Pessoais (LGPD) delimita a exclusão dos tratamentos realizados para fins exclusivos de investigação e repressão de infrações penais, remetendo a disciplina específica, com exigências de necessidade, proporcionalidade e direitos. Essa previsão não cria espaço de atuação sem garantias (Brasil, 2018, art. 4º, III e § 1º).

Síntese do capítulo. A obtenção deve ter fundamento identificável, objeto delimitado e execução compatível com a autorização. A guarda precisa proteger pessoas e permitir controle do trabalho. A apresentação deve separar resultado técnico e conclusão jurídica. Cabe ao julgador valorar a prova conforme o processo, com possibilidade de contestação efetiva pelas partes.

CAPÍTULO 3

Origem, integridade, autenticidade, atribuição e contexto

3.1 Cinco perguntas complementares

A origem trata da proveniência do objeto e do caminho pelo qual foi obtido. A integridade examina a manutenção de suas características dentro de um escopo e de um intervalo definidos. A autenticidade pergunta se o material corresponde ao que afirma ser. A atribuição relaciona ações e pessoas. O contexto permite interpretar o significado do vestígio.

Essa distinção desenvolve o cuidado com proveniência, integridade e interpretação presente no livro de referência. Um dado pode permanecer inalterado depois de recebido e ter sido produzido antes por uma fonte enganosa. Também pode ser autêntico e insuficiente para demonstrar a autoria da conduta investigada (Jorge, 2027).

Dimensão	Questão orientadora
Origem	De onde veio este objeto e por qual percurso?
Integridade	Que conteúdo foi conferido e desde quando?
Autenticidade	Corresponde ao documento ou evento alegado?
Atribuição	Que elementos vinculam a ação a uma pessoa?
Contexto	Que circunstâncias modificam sua interpretação?

Exemplo hipotético. Uma imagem recebida como captura de conversa é preservada sem alteração. Essa integridade posterior não demonstra que a conversa ocorreu no aplicativo indicado. É preciso investigar a proveniência, a existência de registros compatíveis e os elementos de contexto. A análise melhora quando cada dúvida recebe um teste próprio, em vez de ser respondida por uma única etiqueta de confiabilidade.

3.2 Hash e o limite da comparação

Uma função hash transforma uma sequência de bytes em um resumo de tamanho definido. Algoritmos como o SHA-256 são empregados para conferir objetos digitais. A comparação tem sentido quando se documentam algoritmo, objeto exato e momento do cálculo. O padrão FIPS 180-4 do National Institute of Standards and Technology (NIST) descreve essa família de funções (National Institute of Standards and Technology, 2015).

Valores coincidentes, obtidos adequadamente para objetos delimitados, oferecem forte suporte à manutenção do conteúdo binário comparado. Não constituem identificação matemática exclusiva de toda informação possível: colisões são teoricamente possíveis, e a segurança depende do algoritmo e do uso correto. Adote algoritmo robusto compatível com o protocolo institucional e registre sua identificação.

O resumo não informa quem criou o arquivo, se a cena filmada foi encenada ou se houve alteração antes do primeiro cálculo. Preservar o valor em registro protegido é essencial: quem pudesse substituir arquivo e resumo sem controle comprometeria a própria referência de comparação. O NIST IR 8387 recomenda cálculo próximo à coleta e proteção dos registros correspondentes (Guttman; White; Walraven, 2022).

Exemplo hipotético. O vídeo é convertido para outro formato. O hash muda porque o objeto binário mudou. Isso não prova fraude; exige descrever a conversão, conservar o objeto de origem e identificar a versão derivada. Já a mudança inexplicada no arquivo que deveria permanecer preservado demanda apuração e limitação do uso até esclarecimento.

3.3 Da conta à pessoa que praticou a ação

O identificador de uma conta descreve um vínculo técnico ou cadastral. A autoria da conduta depende de outras relações: controle no período, uso do dispositivo, acesso por terceiros, compartilhamento e compatibilidade com os fatos. A investigação deve testar essas relações sem transformar titularidade em presunção de autoria.

Exemplo hipotético. Uma mensagem de extorsão parte de conta registrada em nome de Marcos. O cadastro orienta diligências, mas a hipótese de uso por outra pessoa permanece examinável. Registros de sessões, dispositivos vinculados, comunicações próximas ao fato e outros elementos regularmente obtidos podem esclarecer quem controlava a conta naquele momento.

A corroboração deve ser independente quanto à origem. Três relatórios que repetem a mesma captura de tela não representam três confirmações autônomas. Antes de somar elementos, identifique se derivam de uma única fonte. A repetição pode aumentar a aparência de certeza sem acrescentar suporte.

O Controle de Viés Investigativo proposto em Jorge (2027) ajuda a organizar esse exame: formular alternativa plausível, localizar o elemento que a sustenta e escolher diligência capaz de diferenciá-la da hipótese inicial. A alternativa precisa ter relação com o caso, não ser possibilidade abstrata impossível de testar.

Orientação prática. Escrever primeiro o fato técnico demonstrado, depois a inferência e suas premissas. Se o exame vincula mensagem a uma conta, não redigir como se vinculasse diretamente a pessoa à execução material do delito.

3.4 Contexto, tempo e significado

Uma sequência de mensagens pode revelar negociação, ameaça, ironia ou resposta a evento anterior. Recortar apenas a frase impactante pode eliminar o contexto necessário à interpretação. O relatório deve indicar os critérios de seleção e permitir localizar os trechos adjacentes relevantes no material preservado.

O tempo exige tratamento semelhante. Horário de criação, modificação, recebimento, sincronização e exportação podem representar eventos diferentes. O campo apresentado pela ferramenta precisa ser explicado. Um relógio configurado incorretamente não pode ser silenciosamente ajustado como se a correção estivesse na fonte.

Exemplo hipotético. A câmera mostra 10h12, enquanto o controle de acesso registra 10h07. Uma verificação documentada encontra diferença de cinco minutos entre o relógio da câmera e a referência consultada naquele momento. A linha do tempo deve preservar os valores originais e mostrar separadamente a normalização proposta. Não se presume, sem investigação, que a diferença tenha permanecido constante durante todo o período.

O mesmo cuidado vale para fuso, horário de verão histórico, precisão de segundos e registros incompletos. Quando a incerteza temporal impede distinguir duas versões, ela integra a conclusão.

Síntese do capítulo. A qualidade do material resulta da resposta articulada às cinco perguntas. Hash, cadastro e aparência de autenticidade possuem funções específicas. A conclusão deve conservar as diferenças entre o que foi encontrado, o que foi tecnicamente verificado e o que permanece inferido.

CAPÍTULO 4

Cadeia de custódia e etapas do CPP

4.1 História verificável do vestígio

A cadeia de custódia documenta a história do vestígio e permite acompanhar posse e manuseio. No CPP, sua disciplina está nos arts. 158-A a 158-F. O reconhecimento de interesse pericial já exige preservação; não se deve esperar a chegada ao laboratório para iniciar o registro (Brasil, 1941).

Essa orientação, também desenvolvida em Jorge (2027), exige continuidade entre cena, transporte, exame e apresentação. Em ambiente digital, o histórico abrange ainda a produção de cópias e derivados. O dispositivo pode manter o mesmo lacre enquanto um arquivo exportado circula por diversos destinatários. Cada percurso precisa ser documentado.

As sete fases do método da Investigação Criminal Tecnológica organizam a investigação. As dez etapas da cadeia de custódia possuem definição legal e finalidade própria. São planos relacionados de organização do trabalho, com correspondências possíveis, sem substituição de um pelo outro. A fase metodológica de apresentação, por exemplo, não encerra a guarda legal do vestígio.

Exemplo hipotético. Um agente recebe de uma testemunha uma mídia com vídeo. Registra a pessoa que entregou, a hora, o suporte e a alegada origem. O reconhecimento de relevância não transforma essa origem declarada em fato verificado. O formulário deve manter as duas informações separadas: recebimento documentado e versão sobre a produção do arquivo.

4.2 As dez etapas e sua documentação

O quadro sintetiza as etapas do art. 158-B. As aplicações indicadas são exemplos de organização documental e precisam observar os procedimentos definidos pelo órgão competente (Brasil, 1941).

Etapa legal	Exemplo de registro aplicável
Reconhecimento	Vínculo potencial do item com o fato.
Isolamento	Medidas de proteção do ambiente e do acesso.
Fixação	Estado encontrado e descrição contextual.
Coleta	Responsável e procedimento empregado.
Acondicionamento	Identificação individual e proteção.
Transporte	Percurso, responsáveis e condições.
Recebimento	Conferência formal da transferência.
Processamento	Exame, método, resultados e laudo.
Armazenamento	Local, vínculo e controle de acesso.
Descarte	Destinação conforme requisitos legais.

As etapas não devem virar dez marcações idênticas para qualquer caso. Um arquivo fornecido por provedor e um celular apreendido exigem descrições diferentes. A equipe deve explicar como preservou identificação, continuidade e controle em cada situação, inclusive quando determinado campo não se aplica ao objeto.

Erro frequente. Usar coleta e processamento como sinônimos. Receber ou adquirir o material não esgota o exame especializado. A documentação precisa permitir reconhecer quem realizou cada ação, a finalidade e a relação entre o material recebido e o resultado apresentado.

4.3 Individualização, lacres e transferências

O CPP disciplina acondicionamento, abertura, relacração e identificação de acessos, além das centrais de custódia. A coleta é preferencialmente realizada por perito oficial, com detalhamento operacional pelo órgão central de perícia (Brasil, 1941, arts. 158-C a 158-F).

O registro físico identifica equipamento, recipiente e lacre. O registro digital identifica arquivos, conjuntos, cópias e transformações. Lacre físico e hash

respondem a problemas distintos: o primeiro permite controlar acesso ao recipiente; o segundo auxilia a comparação de conteúdo delimitado. Um não substitui o outro.

Cada transferência deve informar remetente, destinatário, data, hora, finalidade, objeto e conferência realizada, além dos campos legais pertinentes. A pessoa que recebe deve descrever divergências observáveis, como numeração incompatível ou embalagem danificada, sem tentar corrigi-las silenciosamente.

Exemplo hipotético. O laudo menciona o item E-03, mas a remessa identifica E-30. Antes de utilizar o resultado, é preciso esclarecer se houve erro de transcrição ou troca de objeto. A correção deve conservar os documentos anteriores, indicar sua causa e permitir seguir a correspondência. A simples substituição do número elimina justamente a evidência do que ocorreu.

A memória individual não deve ser o único registro do percurso. Formulários e sistemas precisam ter responsáveis definidos, campos compreensíveis e meios de registrar ocorrências excepcionais. A cadeia se fortalece quando o procedimento cotidiano facilita a documentação contemporânea dos atos.

4.4 Guarda, acesso e destinação

A custódia continua depois do exame. O material precisa permanecer localizável, protegido e apto à verificação possível. O CPP trata do retorno à central e prevê solução específica quando ela não possui condições de armazenamento, mediante o procedimento do art. 158-F (Brasil, 1941).

Para objetos digitais, a instituição deve planejar controles de acesso, cópias de segurança, conferências periódicas e recuperação. Também é preciso conservar os meios necessários à leitura. Um arquivo intacto pode se tornar praticamente inacessível se forem perdidos o formato, as chaves legitimamente custodiadas ou a documentação do sistema.

As cópias devem ter finalidade identificada: preservação, trabalho ou apresentação. O acesso pode ser concedido conforme função, com registro individual e restrição ao necessário. Um repositório compartilhado por senha

única dificuldade identificar quem alterou ou exportou determinado objeto. A proteção alcança o material e os registros de sua própria custódia.

A destinação final não deve decorrer da simples conveniência de liberar espaço. É necessário verificar a competência, os requisitos legais e a necessidade de conservação para revisão, defesa e outros usos processualmente cabíveis. A decisão e sua execução precisam ser documentadas.

Síntese do capítulo. A cadeia de custódia combina continuidade de registros, controle sobre objetos e possibilidade de revisão. Seu alcance vai além da embalagem inicial. A organização deve acompanhar a vida do vestígio e das representações que dele foram produzidas.

CAPÍTULO 5

Dispositivos eletrônicos

5.1 O primeiro atendimento

O primeiro contato com um dispositivo pode modificar o cenário antes da intervenção especializada. Por isso, a equipe deve registrar o estado observável, proteger o local, identificar quem já teve contato e acionar suporte capacitado. A cautela desenvolvida no livro de referência concentra-se em evitar navegação exploratória e intervenções sem finalidade definida (Jorge, 2027).

Entre as condições relevantes estão funcionamento, bloqueio, conexões aparentes, cabos, periféricos, alimentação e posição no ambiente. A fixação não deve exigir manipulação invasiva para produzir uma descrição mais completa. Se um dado não pôde ser observado legitimamente, essa limitação deve constar do registro.

Não existe orientação universal para desligar ou manter ligado todo equipamento. As escolhas envolvem risco de perda de dados voláteis, criptografia, alterações automáticas e comunicação remota. As diretrizes de perícia móvel do NIST discutem essa dependência do estado e do ambiente, exigindo decisão tecnicamente informada (Ayers; Brothers; Jansen, 2014).

Exemplo hipotético. Um celular é encontrado ligado e desbloqueado. O agente fotografa, dentro da atuação autorizada, sua condição externa e registra a tela já visível, sem iniciar buscas por mensagens. Comunica o estado à equipe técnica. Qualquer intervenção adicional precisa considerar competência, autorização e risco de alteração. O registro permite distinguir o que foi observado do que foi posteriormente adquirido.

5.2 Preservação e acondicionamento adequados

Isolar comunicações pode reduzir determinados riscos, mas a medida precisa ser tecnicamente avaliada. Alterar configurações pode modificar o dispositivo; proteção de radiofrequência depende de equipamento adequado e de suas

condições de uso. Nenhum recurso deve ser tratado como garantia absoluta de isolamento.

A preservação considera também integridade física, riscos elétricos e condições do transporte. Acondicionar dispositivos de maneira inadequada pode danificar componentes ou comprometer sua leitura. A equipe deve observar o protocolo institucional e registrar a condição encontrada, a medida adotada e as razões da escolha, sem improvisar procedimentos de laboratório.

O atendimento deve evitar conexão a computadores pessoais, instalação de aplicativos ou uso de serviços externos para explorar o conteúdo. Essas ações introduzem novos ambientes e dificultam explicar o que pertence à fonte e o que resulta da intervenção. A urgência deve ser descrita concretamente e encaminhada à autoridade e ao apoio técnico responsáveis.

Erro frequente. Usar a falta de ferramenta especializada como justificativa para navegar livremente no equipamento. A limitação de recursos exige priorização, preservação possível e comunicação transparente. Ela não amplia a competência jurídica nem torna invisíveis os efeitos do manuseio.

A documentação deve acompanhar o dispositivo durante a remessa. Se houve acesso anterior por proprietário, agente ou terceiro, registrar quem informou isso, quando teria ocorrido e o que é conhecido sobre a ação. Informação incompleta, identificada como tal, é mais útil que uma declaração genérica de que ninguém tocou no objeto.

5.3 O alcance da aquisição

Aquisição é a obtenção técnica dos dados dentro de um escopo definido. Uma imagem de mídia estática pode reproduzir setores acessíveis, inclusive áreas não alocadas, quando o método permite. Em celulares, nuvem e sistemas em funcionamento, as modalidades e os limites variam. A expressão cópia forense não deve ocultar o que efetivamente foi adquirido.

Aquisição lógica utiliza interfaces e estruturas disponibilizadas pelo sistema. Uma aquisição de sistema de arquivos busca estruturas e arquivos conforme a capacidade do método. A aquisição física refere-se ao acesso a camadas de armazenamento, com alcance dependente do ambiente e da tecnologia. As

denominações devem ser acompanhadas de descrição do resultado, inclusive quanto à criptografia e às áreas inacessíveis.

Em fontes dinâmicas, pode ser inviável calcular previamente um hash de todo o dispositivo em estado imutável. O registro deve individualizar os objetos adquiridos, suas verificações e as mudanças inerentes ao procedimento. A ausência dessa possibilidade não deve ser ocultada sob a afirmação genérica de espelhamento integral. As diretrizes de perícia móvel ajudam a compreender essas diferenças (Ayers; Brothers; Jansen, 2014).

Exemplo hipotético. A ferramenta exporta mensagens de determinada conta, mas não anexos antigos mantidos somente no servidor. O relatório deve dizer exatamente isso. A ausência do anexo na exportação não demonstra que ele nunca existiu, e o título extração completa seria inadequado para descrever esse resultado.

5.4 Exame reproduzível dentro de limites conhecidos

O exame deve registrar método, ferramenta, versão, configurações relevantes, objetos de entrada e resultados. Quando se trabalha sobre cópia, sua vinculação ao material preservado precisa ser demonstrável. Se foi necessária intervenção na fonte, documentam-se os motivos, as ações e as limitações decorrentes.

A validação precisa considerar a finalidade e o ambiente. Uma ferramenta capaz de ler determinado formato pode interpretar incorretamente um campo criado por versão diferente do aplicativo. O NIST IR 8354 distingue a adequação do método ao uso pretendido da verificação de sua implementação, destacando a necessidade de testes e o alcance limitado de suas conclusões (Lyle et al., 2022).

A requisição deve formular quesitos verificáveis. Pode perguntar quais objetos foram examinados, que período abrangem, como o horário é representado, se há sinais tecnicamente identificáveis de alteração e quais aspectos não puderam ser determinados. Perguntas jurídicas sobre autoria ou culpabilidade não devem ser transferidas à ferramenta.

Síntese do capítulo. Preservar o estado, escolher aquisição adequada e declarar o alcance do exame são decisões interdependentes. Nome comercial, volume extraído ou expressão técnica não substituem uma descrição verificável. Quando houver incerteza relevante sobre o resultado, cabe solicitar esclarecimento ou exame complementar, em vez de preencher a lacuna com suposição.

CAPÍTULO 6

Mensagens, capturas, áudios e arquivos

6.1 Capturas de tela e exportações

Uma captura de tela registra uma apresentação visual. Pode orientar a investigação e documentar conteúdo relevante, mas normalmente não conserva todos os dados de origem. Nome exibido, imagem de perfil e horário na tela exigem contextualização. A captura deve ser recebida com indicação de quem a produziu, de qual ambiente provém e do que é conhecido sobre sua elaboração.

A exportação também possui limites. Pode alterar a organização, omitir campos ou separar anexos. É necessário conhecer a função utilizada e conferir se o resultado contém o período pretendido. Quando houver fonte acessível por via legítima, sua preservação e exame podem permitir testar questões que a imagem isolada não responde.

Exemplo hipotético. A vítima entrega quatro capturas de uma ameaça. A equipe registra o recebimento e as trata como material inicial. Pergunta sobre mensagens anteriores e posteriores, preserva os arquivos entregues e avalia, com autorização adequada, a obtenção de dados que confirmem sequência e origem. O fato de a vítima colaborar não dispensa o controle do procedimento.

A ata notarial pode documentar fatos percebidos pelo tabelião, nos termos do art. 384 do Código de Processo Civil (Brasil, 2015). Isso não converte automaticamente toda origem remota ou atribuição pessoal em conclusão pericial. O mesmo cuidado vale para fotografias, declarações e relatórios: cada documento deve ser interpretado pelo que efetivamente atesta, conservando as questões que permanecem abertas.

6.2 Áudio e vídeo exigem mais que reprodução

Ouvir uma gravação permite perceber seu conteúdo aparente. Identificar locutor, continuidade, edição ou compatibilidade com determinado evento pode exigir exame especializado. O profissional deve separar transcrição,

descrição do que percebeu e conclusão pericial. A semelhança de uma voz com a de pessoa conhecida é uma informação a avaliar, sem equivaler automaticamente à identificação técnica.

O arquivo recebido deve ser preservado antes de melhorar volume, reduzir ruído ou converter formato. As versões de trabalho precisam ser identificadas e relacionadas ao objeto de origem. Uma transcrição deve indicar trechos inaudíveis e dúvidas, sem completar palavras pela narrativa da investigação.

Exemplo hipotético. Um áudio contém frase ambígua e ruído. Dois ouvintes apresentam leituras diferentes. A equipe registra a divergência, conserva o arquivo e formula quesito sobre a inteligibilidade do trecho. Não deve redigir a versão mais incriminadora como se fosse conteúdo inequívoco.

Conteúdo sintético ou manipulado exige cautela semelhante. Um programa que classifica um vídeo como provável manipulação produz resultado auxiliar, dependente de método e condições conhecidas. A investigação deve examinar proveniência, arquivos disponíveis, circunstâncias e corroboração. O rótulo de uma ferramenta não encerra a análise de autenticidade nem autoriza afirmar que tudo é falso por existir tecnologia de geração de imagens.

6.3 Arquivos, anexos e seleção

O vínculo entre mensagem e anexo deve ser preservado sempre que tecnicamente possível. Um arquivo encontrado no mesmo diretório não deve ser automaticamente atribuído à conversa selecionada. É necessário identificar o mecanismo que sustenta a relação: referência na base, identificador de mensagem, estrutura de exportação ou outro elemento verificável.

A extensão do arquivo também não define seu conteúdo. A interpretação deve considerar formato real, estrutura e ambiente de origem. Arquivos compactados, bancos de dados e documentos com objetos incorporados podem exigir tratamento específico, com descrição do que foi aberto, extraído ou excluído da análise.

O recorte apresentado ao destinatário deve conservar rastreabilidade até o objeto preservado. No relatório, use identificadores estáveis e indique o local de

cada trecho. Evite depender somente da ordem de páginas gerada por um visualizador, que pode mudar entre versões.

Erro frequente. Renomear o único arquivo recebido e perder a designação original sem registrar a correspondência. A organização interna pode exigir nomes padronizados, mas o inventário deve manter a relação entre identificação de origem e identificação institucional.

Síntese do capítulo. Capturas, exportações, áudios e anexos possuem funções úteis quando suas limitações são conhecidas. O tratamento deve conservar a fonte disponível, distinguir derivados e permitir testar a interpretação. Clareza de apresentação não deve apagar dúvidas sobre proveniência, completude e significado.

CAPÍTULO 7

Nuvem, registros, metadados e fontes distribuídas

7.1 A fonte pode estar em vários lugares

Uma conta pode manter dados no aparelho, em servidor, em cópia de segurança e em dispositivos sincronizados. Essas fontes não são necessariamente idênticas. O que está no telefone pode corresponder apenas ao período recentemente acessado; o servidor pode não conservar conteúdo eliminado ou protegido por arquitetura criptográfica.

A investigação deve construir um mapa das fontes: quem detém cada categoria, qual período pode existir, que risco de perda há e por qual via jurídica seria obtida. A identificação do provedor não permite presumir que ele tenha todos os dados imaginados pela equipe. É necessário formular pedido tecnicamente inteligível e compatível com sua função.

O Marco Civil prevê regimes específicos de guarda de registros de conexão e de acesso a aplicações, com pressupostos próprios. Esses regimes não equivalem a uma obrigação geral de conservar todo conteúdo de toda conta. A análise deve distinguir preservação cautelar e disponibilização (Brasil, 2014, arts. 13 e 15).

Exemplo hipotético. A vítima informa ameaça em uma aplicação. A equipe identifica conta, intervalo e dados relevantes. A autoridade avalia a preservação cabível e as medidas necessárias à obtenção. O procedimento deve registrar protocolo, destinatário, objeto, resposta e providências subsequentes. O simples envio de pedido não comprova que todos os dados foram preservados.

7.2 Preservar, obter e conferir

Preservar busca evitar a perda de dados delimitados. Obter envolve acesso e entrega por via juridicamente adequada. Nos pedidos cautelares previstos no Marco Civil, devem ser observados os requisitos e prazos legais, inclusive a vinculação ao pedido judicial de acesso. A preservação não dispensa essa etapa quando exigida (Brasil, 2014, arts. 13, §§ 2º a 5º, e 15, §§ 2º e 3º).

No recebimento, registre o canal, a identificação da resposta, os arquivos e eventuais documentos explicativos. Preserve a estrutura fornecida antes de reorganizar ou converter. Se o provedor informar fuso, critérios de consulta, campos ou limitações, esses elementos acompanham a análise.

Exemplo hipotético. A resposta contém linhas com identificadores e horários, mas não explica se o horário é de início de sessão ou de geração do registro. A equipe solicita esclarecimento antes de construir a linha do tempo. Interpretar o nome de uma coluna por intuição pode deslocar a sequência dos fatos.

Uma resposta incompleta precisa ser avaliada com base no pedido e no que o detentor efetivamente mantém. Ausência de retorno, inexistência de dado e dado não abrangido pela consulta são situações diferentes. O relatório deve descrevê-las sem transformar silêncio em confirmação de que um evento não ocorreu.

7.3 Metadados e limites de identificação

Metadados descrevem atributos ou eventos associados aos dados. Podem ajudar a localizar origem, horários, formato e relações, mas também podem ter sido alterados, omitidos ou recriados. Seu significado depende do sistema e do processo que os produziu. A interpretação deve indicar essa dependência.

Na correlação de acesso à internet, endereço IP, porta de origem e informação temporal podem ser necessários para distinguir usuários em ambientes de compartilhamento. A RFC 6302 apresenta recomendações de registro para esse cenário. É referência técnica, sem estabelecer competência requisitória ou obrigação legal brasileira de guarda (Durand et al., 2011).

Exemplo hipotético. Um IP aparece associado a uma conexão compartilhada. Mesmo que o assinante seja identificado por dados tecnicamente suficientes, permanece a pergunta sobre quem realizou a ação. Outros usuários, dispositivos e acessos precisam ser considerados conforme os elementos do caso. A conexão é um elo da investigação.

Fontes distribuídas também exigem atenção à duplicidade. O mesmo evento pode aparecer no aparelho, no relatório do provedor e no arquivo de

sincronização. Reconhecer essa relação evita contabilizar reproduções como ocorrências independentes.

Síntese do capítulo. A investigação em nuvem exige mapa de detentores, separação das categorias de dados, preservação oportuna e obtenção regular. A correlação deve conservar o significado dos campos e a incerteza da atribuição. Quantidade de registros não resolve, por si, a qualidade da interpretação.

CAPÍTULO 8

Falhas de preservação e impactos probatórios

8.1 Identificar exatamente o problema

Uma falha pode atingir a legalidade da obtenção, a identificação do objeto, a integridade, a completude ou a possibilidade de revisão. A análise precisa localizar qual aspecto foi afetado e em que momento. A expressão quebra da cadeia de custódia, isoladamente, não descreve a ocorrência nem demonstra seu alcance.

Exemplo hipotético. Um formulário omite a hora de recebimento, mas há protocolo contemporâneo que permite verificá-la. Em outra situação, não se conhece o equipamento de origem de um arquivo nem o procedimento de extração. Ambos os casos exigem esclarecimento, mas apresentam problemas diferentes. A investigação deve preservar os registros existentes e explicitar o que permanece sem resposta.

No livro de referência, a qualidade da documentação é vinculada à possibilidade de controle do resultado. A presente orientação desenvolve essa preocupação: descreva a lacuna, busque elementos verificáveis sobre o percurso e avalie se ainda é possível testar a afirmação proposta (Jorge, 2027).

A constatação de falha não autoriza encobri-la por documentação posterior com aparência de contemporaneidade. Um relato elaborado depois deve trazer sua data verdadeira, sua fonte e suas limitações. Ele pode contribuir para esclarecimento, mas não transforma memória tardia em registro produzido no momento do ato.

8.2 Consequências exigem fundamentação

A avaliação deve considerar a regra violada, a confiabilidade afetada e o exercício da defesa. A prova ilícita recebe o tratamento constitucional e processual próprio. Em problemas de custódia, é necessário examinar concretamente o que a falha impede verificar, sem prometer admissibilidade

ou exclusão automática para toda situação (Brasil, 1988; Brasil, 1941, arts. 157 e 158-A a 158-F).

Uma lacuna pode permitir esclarecimento documental; outra pode impedir relacionar o resultado ao objeto supostamente apreendido. A conclusão deve explicar essa diferença. A equipe investigativa e o perito devem apontar os limites de suas análises, preservando a apreciação jurídica pela autoridade competente e, no processo, pelo julgador.

Ocorrência	Pergunta que orienta a avaliação
Objeto sem identificação segura	É possível vinculá-lo à fonte declarada?
Transformação não registrada	Qual conteúdo ou atributo pode ter mudado?
Acesso sem responsável conhecido	Que intervenções ficaram sem controle?
Fonte indisponível para revisão	Que conclusões deixaram de ser testáveis?

Cautela. A ausência de demonstração de adulteração não prova, por si, que todo o percurso foi confiável. Da mesma forma, uma irregularidade formal não demonstra sozinha que houve falsificação. O exame precisa articular registros, riscos concretos e efeitos sobre a afirmação sustentada.

8.3 Conter, esclarecer e comunicar

Ao perceber uma inconsistência, interrompa as operações que possam agravá-la, preserve as versões existentes e comunique os responsáveis. A forma de contenção depende do ambiente e do protocolo: não se deve desligar indiscriminadamente um sistema ou destruir arquivos para interromper a dúvida.

O esclarecimento deve buscar registros de acesso, relatórios de ferramentas, cópias preservadas e documentos contemporâneos. Se for necessário novo exame, seu objeto e sua relação com o trabalho anterior precisam estar identificados. As versões não devem ser misturadas em um pacote apresentado como se sempre houvesse sido único.

Exemplo hipotético. O hash da cópia de trabalho diverge do registro de recebimento. A equipe conserva ambas as referências, verifica se houve comparação entre objetos diferentes e examina se ocorreu conversão. Se o arquivo preservado também divergir sem explicação, o relatório não pode afirmar integridade contínua. Deve indicar a ocorrência e as medidas adotadas.

A correção pode reduzir o impacto de um erro e melhorar o sistema, mas não recupera necessariamente informação perdida. Não se deve compensar uma falha com linguagem mais categórica sobre autoria ou materialidade.

Síntese do capítulo. Tratar falhas exige transparência e diagnóstico específico. O caminho útil é preservar o que existe, esclarecer o que pode ser esclarecido e limitar a conclusão ao que permanece verificável. A qualidade institucional também se mede pela capacidade de registrar e corrigir seus próprios erros.

CAPÍTULO 9

Estudo de caso hipotético de extorsão digital

9.1 Relato inicial e prioridades

Caso inteiramente fictício, criado para fins didáticos. Renata procura a polícia e relata que uma conta de mensagens exige dinheiro sob ameaça de divulgar documentos pessoais. Entrega capturas de tela e um arquivo de áudio. Reconhece na voz semelhança com a de um antigo prestador de serviços, Daniel. O perfil exibe uma fotografia de Daniel disponível em página pública. A semelhança é uma alegação inicial, não identificação comprovada.

O Delegado de Polícia organiza o atendimento, avalia as providências de proteção e define as diligências. A equipe registra os materiais efetivamente entregues e a versão sobre sua produção. O relato deve esclarecer como começaram os contatos, que documentos teriam sido usados, quem possuía acesso e quais comunicações continuam disponíveis.

A primeira pergunta probatória é se existem elementos que confirmem a exigência e a ameaça nas circunstâncias narradas. A segunda é como identificar quem controlava a conta. A terceira é se há risco concreto que demande providência urgente de proteção ou preservação. As perguntas se relacionam, mas não recebem a mesma resposta técnica.

A equipe não orienta a vítima a provocar o interlocutor ou investigar por conta própria. Registra a continuidade dos contatos informada por ela e encaminha a situação à autoridade. As decisões operacionais devem considerar a segurança da vítima e o fundamento jurídico das medidas pretendidas.

9.2 Planejamento das fontes e alternativas

As capturas recebem identificadores E-01 a E-04; o áudio, E-05. Os identificadores apenas organizam o material, sem certificar autenticidade. O dispositivo de Renata é indicado como fonte potencial a ser examinada por via adequada. A conta do remetente, os registros do serviço e eventual informação financeira constituem outras linhas, sujeitas a regimes jurídicos próprios.

Hipótese	Elemento inicial	Teste que pode discriminá-la
Daniel controla a conta	Semelhança de voz relatada	Corroborar controle no período e examinar o áudio.
Terceiro usa identidade de Daniel	Uso de foto disponível publicamente	Examinar proveniência e vínculos técnicos pertinentes.
Material entregue tem contexto incompleto	Existem somente recortes	Obter sequência relevante por via legítima.

A matriz emprega o Controle de Viés Investigativo de Jorge (2027). A segunda hipótese não afirma que houve imitação; identifica uma alternativa a testar. A terceira não acusa a vítima de falsidade; reconhece que recortes podem ser incompletos mesmo quando produzidos de boa-fé.

A autoridade avalia a preservação cabível junto ao detentor de registros e fundamenta o pedido judicial necessário à disponibilização dos dados protegidos. O planejamento define período e identificadores disponíveis. Evita pedir todas as informações de todos os contatos apenas porque o serviço dispõe de grande volume de dados.

9.3 Obtenção, custódia e exame

No cenário fictício, o acesso ao dispositivo e aos dados protegidos é realizado sob autorização adequada, com alcance documentado. A equipe técnica registra estado, método, versão da ferramenta, objeto adquirido e limitações. Os arquivos obtidos recebem identificação e verificação de integridade, com guarda institucional e cópia de trabalho vinculada.

O exame encontra sequência compatível com a exigência relatada, incluindo mensagens anteriores que explicam a referência a documentos. O áudio analisado é relacionado à mensagem por registros identificados na base. O perito descreve o vínculo técnico, sem concluir que a conta necessariamente era usada por Daniel.

A resposta do provedor, obtida regularmente, contém registros de acesso. A equipe confere campos e informações temporais antes de correlacionar os eventos. Descobre que uma referência de horário do relatório de mensagens foi normalizada pelo visualizador. Conserva o valor de origem e registra separadamente a normalização, evitando alterar a cronologia silenciosamente.

A semelhança de voz relatada pela vítima continua insuficiente para identificação conclusiva. O exame especializado informa o que pôde avaliar e quais limitações decorrem da duração e da qualidade do áudio. A investigação busca elementos independentes sobre controle da conta e acesso aos documentos.

Ponto de aprendizagem. A confirmação de mensagens ameaçadoras fortalece a análise do fato narrado. A autoria exige caminho adicional, com corroboração e individualização. A documentação permite seguir os dois raciocínios sem confundi-los.

9.4 Falha localizada e conclusão proporcional

Na revisão, a equipe percebe que o áudio inicialmente entregue foi encaminhado por aplicativo que pode modificar arquivos. Essa condição não havia sido descrita no primeiro registro. A ocorrência é anotada com data verdadeira, preservando o arquivo recebido e a declaração sobre seu percurso.

O objeto obtido posteriormente da fonte examinada apresenta características diferentes. A equipe não trata a divergência de hash entre esses objetos como prova automática de adulteração. Solicita análise da relação entre as versões e de possíveis transformações, conservando ambos os percursos. O resultado precisa informar o que foi comparado.

Ao final desta etapa hipotética, há suporte para a existência da comunicação descrita, mas o controle pessoal da conta ainda não foi suficientemente individualizado. O relatório recomenda diligências específicas sobre essa lacuna e registra as alternativas pendentes. Não se redige indiciamento apenas para conferir aparência de conclusão à investigação.

Se novos elementos forem obtidos, sua análise deverá ser incorporada com identificação de origem, relação com as hipóteses e limites. O caso pode

fortalecer uma hipótese, afastá-la ou permanecer inconclusivo. Nenhum desfecho foi predeterminado para satisfazer a narrativa didática.

Síntese do capítulo. Proteção da vítima, legalidade, custódia e raciocínio probatório funcionam conjuntamente. A qualidade está em conectar resultados a perguntas concretas e conservar as incertezas relevantes, inclusive quando o material confirma parte do relato e não resolve a autoria.

CAPÍTULO 10

Boas práticas e documentação da prova

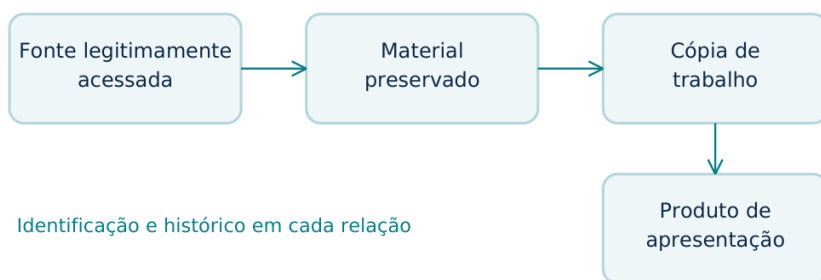
10.1 Um conjunto documental organizado

A documentação deve permitir que outro profissional compreenda o que foi recebido, o que foi feito e por que se chegou à conclusão. Convém organizar o conjunto em torno de identificadores estáveis: fonte, objeto, autorização, aquisição, cópia, exame e apresentação. A relação entre esses componentes precisa permanecer explícita.

O inventário descreve os objetos. O registro de custódia acompanha movimentos e acessos. O registro técnico explica método e transformações. O relatório analítico apresenta os resultados relevantes e a interpretação. A segregação funcional desses registros melhora a consulta, desde que exista vinculação entre eles.

Um esquema simples mostra as relações a conservar. As derivações não substituem o material preservado, e cada transformação deve ser explicada.

Figura 1. Relações entre fonte, material preservado e derivados.



Fonte: elaboração própria.

Orientação prática. Ao citar um resultado, indique objeto e localização verificável. Evite referências como conforme encontrado no celular, que não permitem saber qual material sustenta a afirmação. O leitor deve poder percorrer o caminho inverso, da conclusão até o dado e o procedimento correspondente.

10.2 Revisão técnica e apresentação compreensível

Antes da apresentação, confira correspondência entre identificadores, valores de hash, nomes de arquivos, períodos e objetos mencionados. Revise também as palavras que ampliam indevidamente uma conclusão: integral, exclusivo, impossível e comprovado exigem suporte específico. A presença de uma expressão no relatório automático não dispensa exame crítico.

A revisão por outro profissional ajuda a localizar saltos inferenciais e erros de referência. Quem não participou da diligência pode verificar se o percurso está compreensível e se os resultados sustentam a conclusão. Quando a revisão exigir conhecimento especializado, deve envolver profissional habilitado para o ponto técnico.

A seleção de imagens e trechos precisa favorecer compreensão sem ocultar contexto relevante. Preserve o material de base e indique o caminho de acesso processualmente adequado. Dados de terceiros sem pertinência não devem ser expostos por mera conveniência de apresentação; a proteção deve ser compatível com o exercício efetivo da defesa.

Exemplo hipotético. O relatório apresenta uma linha do tempo com horários normalizados. A legenda informa o fuso, os campos de origem e as incertezas. Cada evento aponta o objeto correspondente. O leitor consegue distinguir a evidência da organização feita pelo analista e examinar a pertinência da normalização.

Uma apresentação clara conserva as limitações em lugar visível. Não é adequado relegar a dúvida decisiva a nota de difícil localização enquanto o título anuncia autoria certa.

10.3 Possibilidade de contestação e aprendizagem

O trabalho deve conservar condições para que o material seja questionado. No âmbito pericial, o CPP disciplina quesitos, assistência técnica e exame do material nas condições legais. A organização da custódia deve servir a esse controle, com segurança e identificação dos acessos (Brasil, 1941, art. 159).

A possibilidade de repetição depende da fonte. Dados voláteis podem não existir mais; versões de serviços podem ter mudado. Nesses casos, registros contemporâneos, materiais preservados e descrição do método tornam-se ainda mais relevantes. Reprodutibilidade não deve ser prometida em grau que o ambiente não permite.

O uso de automação pode ajudar na triagem e na organização, mas requer verificação dos resultados. Transcrições automáticas e classificações devem ser tratadas como produtos derivados, com indicação da ferramenta e revisão humana. Conteúdo sigiloso não deve ser enviado a serviço externo sem avaliação institucional, autorização pertinente e controles de proteção.

Falhas identificadas devem alimentar melhoria de protocolos, capacitação e gestão. Uma instituição aprende quando transforma ocorrência concreta em ajuste verificável: campo mais claro, conferência de recebimento ou teste adicional da ferramenta. O objetivo é reduzir a repetição do problema.

Síntese do capítulo. A documentação precisa sustentar a explicação e permitir sua crítica. O checklist do Apêndice C ajuda a revisar o percurso, sem certificar automaticamente a validade de qualquer prova. Cada item deve remeter a um registro real e à pessoa responsável pela conferência.

Considerações finais

O cuidado com a prova digital começa na pergunta investigativa e continua enquanto o vestígio puder ser utilizado. Identificar uma fonte, preservar um objeto e produzir um relatório são momentos conectados por escolhas jurídicas e técnicas que precisam permanecer compreensíveis.

Esta cartilha desenvolveu a distinção entre origem, integridade, autenticidade, atribuição e contexto. A distinção impede que um único recurso, como o hash ou um cadastro, receba funções que não possui. Também permite formular diligências mais úteis: cada dúvida precisa de elemento capaz de testá-la.

O método da Investigação Criminal Tecnológica apresentado em Jorge (2027) ajuda a organizar esse percurso. Suas fases e o Controle de Viés Investigativo articulam tratamento de vestígios, correlação e revisão de hipóteses. A cadeia de custódia, com seu fundamento legal próprio, fornece o registro contínuo necessário ao controle do material.

A conclusão responsável conserva o alcance efetivo do exame. Pode sustentar uma afirmação, afastar uma hipótese ou reconhecer que faltam elementos. Em qualquer dessas situações, a qualidade depende da possibilidade de mostrar as fontes, explicar os procedimentos e permitir contestação.

Os três instrumentos seguintes traduzem essa responsabilidade em registros de trabalho. Seu uso deve ser acompanhado de treinamento e integração aos sistemas oficiais. Formulários ajudam quando refletem o que aconteceu e permitem localizar o que ainda precisa ser esclarecido.

APÊNDICE A**Formulário de identificação de evidências**

Modelo de apoio. Adaptar ao sistema oficial e anexar inventário quando houver vários objetos. Registrar o desconhecido sem completar por suposição.

Procedimento e unidade: _____

Identificador do item: _____ Data/hora e fuso: _____

Responsável, matrícula e função: _____

Fonte e circunstâncias

Local ou detentor de origem: _____

Pessoa que entregou e condição declarada: _____

Descrição e estado observado: _____

Relação potencial com o fato: _____

Origem declarada ou verificada? Como? _____

Fundamento e obtenção

Base legal e documento autorizativo: _____

Objeto, período e limites autorizados: _____

Forma de coleta ou recebimento: _____

Ferramenta, versão e configurações relevantes: _____

Intervenções e limitações conhecidas: _____

Individualização e destino

Suporte, arquivo ou conjunto identificado: _____

Algoritmo, hash e objeto exato ou razão de inaplicabilidade: ____

Lacre, recipiente ou repositório e controle de acesso: _____

Destino e vínculo com registro de movimentação: _____

Responsável pela conferência e assinatura: _____

Não registrar senhas ou chaves em campo de circulação ampla. Identificar o procedimento seguro de custódia aplicável.

APÊNDICE B

Modelo de movimentação e acesso

Procedimento/unidade: _____

Item e objeto digital correspondente: _____

Identificação da folha e vínculo com inventário: _____

Protocolo, tipo de vestígio e exame solicitado: _____

Código de rastreamento e transportador: _____

Registro 01

Data/hora e fuso: _____

Remetente e destinatário, matrícula e função: _____

Origem, destino e finalidade: _____

Descrição da ação ou do acesso: _____

Condições recebidas e conferências: _____

Lacre anterior/novo ou vínculo da cópia: _____

Ocorrências e documentos associados: _____

Assinaturas ou autenticação do registro: _____

Registro 02

Data/hora e fuso: _____

Remetente e destinatário, matrícula e função: _____

Origem, destino e finalidade: _____

Descrição da ação ou do acesso: _____

Condições recebidas e conferências: _____

Lacre anterior/novo ou vínculo da cópia: _____

Ocorrências e documentos associados: _____

Assinaturas ou autenticação do registro: _____

Utilizar folhas de continuação vinculadas ao item. Registrar também cópias, transformações e acessos relevantes. A versão ampliada para impressão contém espaço adicional. O modelo deve ser complementado pelos campos exigidos no CPP e no protocolo institucional.

APÊNDICE C

Checklist de cadeia de custódia

Procedimento/item: _____ Conferente/data: _____

Marcar apenas o que foi conferido. Identificar pendências e documento comprobatório; usar N/A com justificativa quando cabível.

Antes e durante a obtenção

- ☐ Pergunta investigativa e pertinência do vestígio definidas.
- ☐ Categoria de dado, base legal e autorização conferidas.
- ☐ Fonte, estado e manipulações anteriores registrados.
- ☐ Risco de perda e providência de preservação avaliados.
- ☐ Método, responsável e alcance da aquisição descritos.
- ☐ Objetos individualizados e recebimento documentado.

Guarda e tratamento

- ☐ Lacres, transferências e acessos vinculados ao item.
- ☐ Hashes ou verificações pertinentes registrados e protegidos.
- ☐ Material preservado e cópias de trabalho identificados.
- ☐ Ferramentas, versões e transformações documentadas.
- ☐ Limitações, falhas e ocorrências preservadas no histórico.
- ☐ Repositório, permissões e recuperação definidos.

Apresentação e revisão

- ☐ Trechos apresentados localizáveis na fonte preservada.
- ☐ Horários e normalizações explicados.
- ☐ Autoria pessoal diferenciada de vínculo técnico ou cadastral.
- ☐ Hipóteses alternativas e elementos contrários considerados.
- ☐ Resultado, inferência e conclusão claramente separados.
- ☐ Condições legais de revisão e destinação observadas.

Pendências, providência e responsável: _____

Conferir itens não equivale a certificar admissibilidade ou autoria.

Referências

AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. **Guidelines on mobile device forensics**. Gaithersburg: National Institute of Standards and Technology, 2014. (NIST SP 800-101, rev. 1). DOI: 10.6028/NIST.SP.800-101r1. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>. Acesso em: 25 jun. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Brasília, DF, 5 out. 1988. Texto consolidado. Disponível em: <https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-normaatualizada-pl.html>. Acesso em: 1 jun. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 13 out. 1941. Texto consolidado. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-normaatualizada-pe.html>. Acesso em: 2 jun. 2026.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, 25 jul. 1996. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1996/lei-9296-24-julho-1996-349049-normaatualizada-pl.pdf>. Acesso em: 22 jul. 2026. Texto consolidado.

BRASIL. **Lei nº 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Diário Oficial da União: seção 1, Brasília, DF, 21 jun. 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2013/lei-12830-20-junho-2013-776286-publicacaooriginal-140173-pl.html>. Acesso em: 3 jul. 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. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Texto consolidado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-normaatualizada-pl.html>. Acesso em: 15 jun. 2026.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Diário Oficial da União: seção 1, Brasília, DF, 17 mar. 2015. Texto consolidado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2015/lei-13105-16-marco-2015-780273-normaatualizada-pl.html>. Acesso em: 19 ago. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Texto

consolidado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html>. Acesso em: 19 jul. 2026.

DURAND, Alain et al. **Logging recommendations for Internet-facing servers**. [S. l.]: Internet Engineering Task Force, 2011. (RFC 6302; BCP 162). Disponível em: <https://www.rfc-editor.org/rfc/rfc6302.html>. Acesso em: 4 out. 2026.

GUTTMAN, Barbara; WHITE, Douglas R.; WALRAVEN, Tracy. **Digital evidence preservation: considerations for evidence handlers**. Gaithersburg: National Institute of Standards and Technology, 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: 9 set. 2026.

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

LYLE, James R. et al. **Digital investigation techniques: a NIST scientific foundation review**. Gaithersburg: National Institute of Standards and Technology, 2022. (NIST IR 8354). DOI: 10.6028/NIST.IR.8354. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf>. Acesso em: 13 out. 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: 15 set. 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 oito 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 (este volume)
- 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

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge