**MINISTÉRIO PÚBLICO FEDERAL**
**SECRETARIA DE PESQUISA, PERÍCIA E ANÁLISE**

# INSTRUÇÃO DE SERVIÇO Nº 7, DE 12 DE MARÇO DE 2021.

Aprova o Manual Prático de Cadeia de Custódia, elaborado pelo Grupo de Trabalho instituído no âmbito da Secretaria de Perícia, Pesquisa e Análise.

O SECRETÁRIO DE PERÍCIA, PESQUISA E ANÁLISE, no uso das atribuições que lhe foram conferidas pelo art. 61, inciso III, do Regimento Interno do Gabinete do Procurador-Geral da República , aprovado pela Portaria PGR/MPF n° 40, de 24 de abril de 2020, e pelo art. 41, inciso I, do Regimento Interno da Secretaria de Perícia, Pesquisa e Análise, aprovado pela Portaria PGR/MPF n° 532, de 12 de junho de 2020, RESOLVE:

Art. 1º Aprovar e homologar as normas técnicas e os procedimentos do Manual Prático de Cadeia de Custódia, elaborado pelo Grupo de Trabalho instituído no âmbito da Secretaria de Perícia, Pesquisa e Análise pela Instrução de Serviço n° 17, de 7 de abril de 2020, constante como anexo desta Instrução de Serviço.

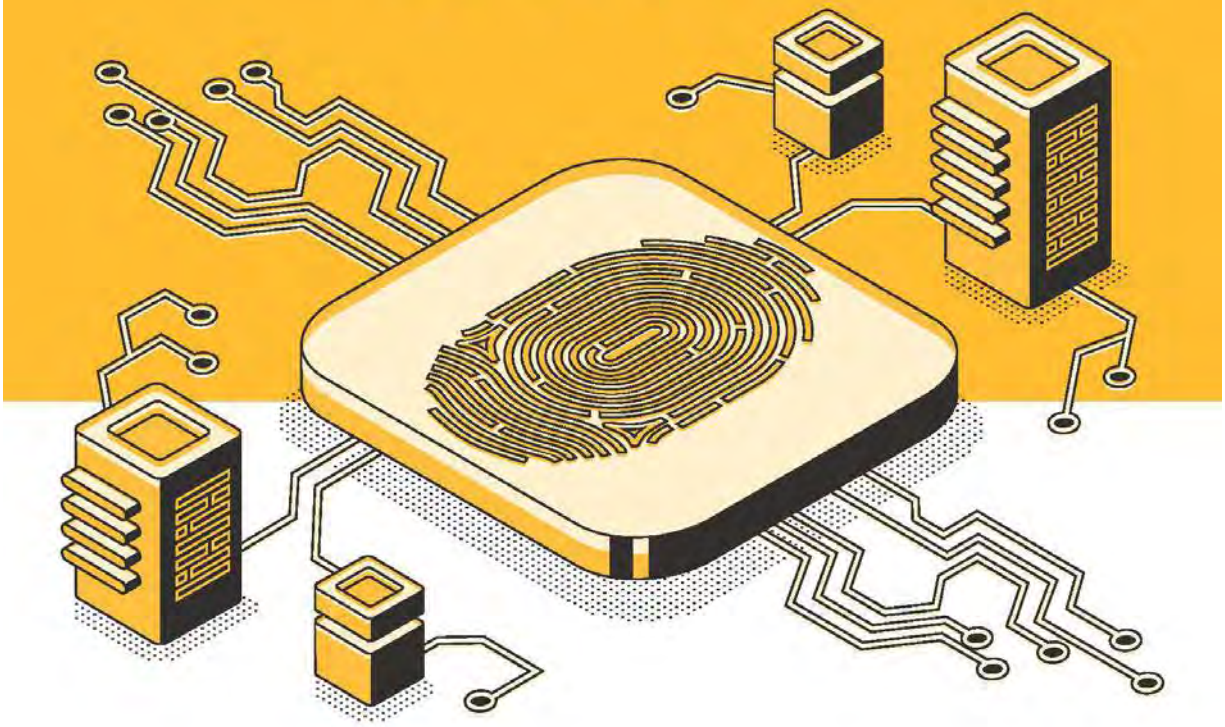
Art. 2º Esta Instrução de Serviço entra em vigor na data de sua publicação.

PAULO RUBENS CARVALHO MARQUES
Procurador da República
Secretário de Perícia, Pesquisa e Análise/SPPEA

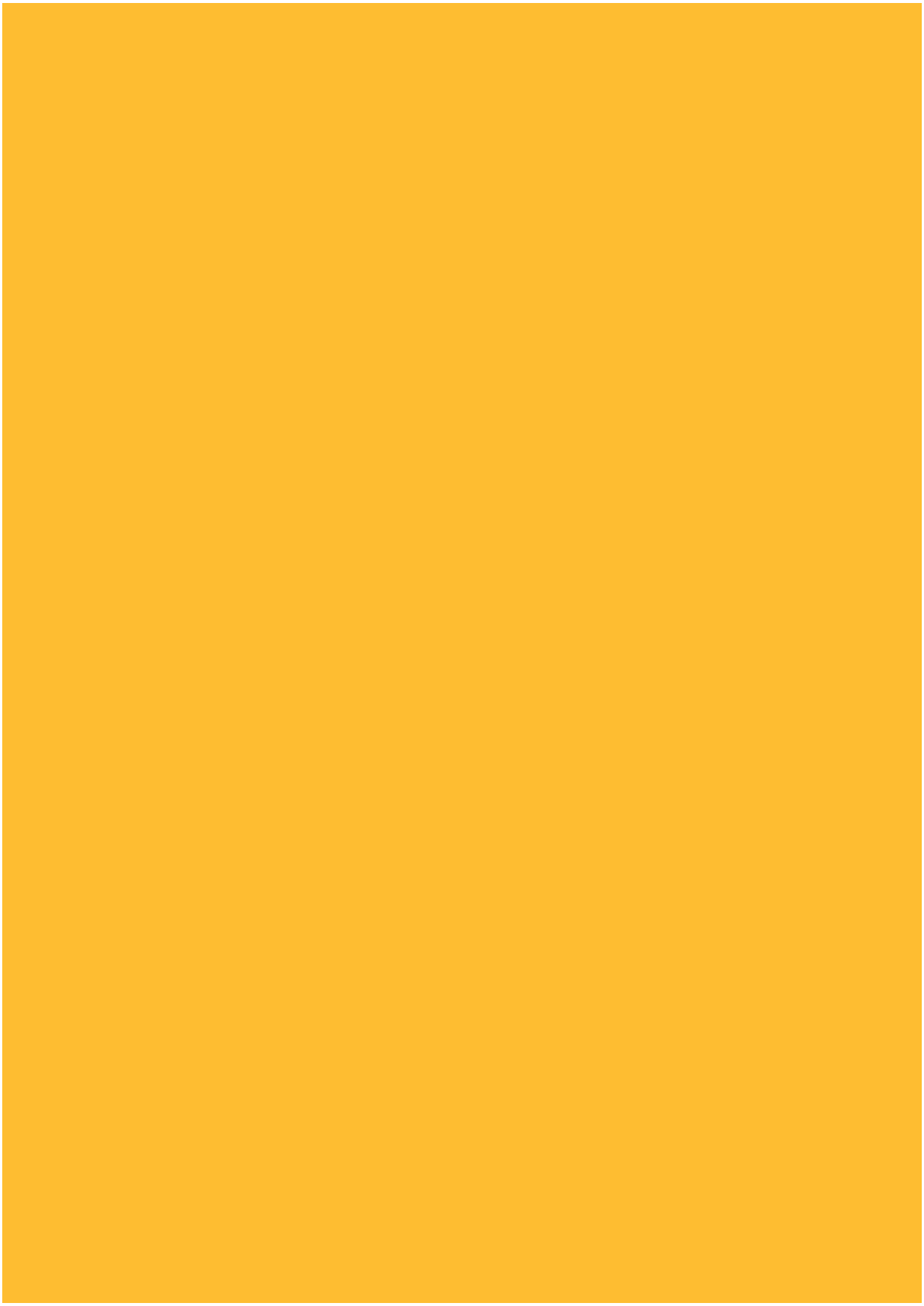
Este texto não substitui o publicado no DMPF-e, Brasília, DF, 16 mar. 2021. Caderno Administrativo, p. 3.

PERÍCIA, PESQUISA E ANÁLISE

# MANUAL PRÁTICO DE CADEIA DE CUSTÓDIA



MPF
Ministério Público Federal



# MANUAL PRÁTICO DE CADEIA DE CUSTÓDIA

**MINISTÉRIO PÚBLICO FEDERAL**

**Procurador-Geral da República**
Antônio Augusto Brandão de Aras

**Vice-Procurador-Geral da República**
Humberto Jacques de Medeiros

**Vice-Procurador-Geral Eleitoral**
Renato Brill de Goés

**Ouvidor-Geral**
Brasilino Pereira dos Santos

**Corregedora-Geral do Ministério Público Federal**
Elizeta Maria de Paiva Ramos

**Secretária-Geral**
Eliana Peres Torelly de Carvalho

Ministério Público Federal
Secretaria de Perícia, Pesquisa e Análise

# MANUAL PRÁTICO DE CADEIA DE CUSTÓDIA

MPF
Brasília/DF
2021

Disponível em: https://portal.mpf.mp.br/intranet/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios-1 (Material reservado)

**Dados Internacionais de Catalogação na Publicação (CIP)**

B823m

Brasil. Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise.

Manual prático de cadeia de custódia / Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. – Brasília : MPF, 2021.

116 p.

Disponível em: https://portal.mpf.mp.br/intranet/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios-1 (Material reservado).

1. Cadeia de custódia. 2. Evidência digital – preservação. 3. Evidência digital – controle. 4. Integridade (segurança da informação). 5. Prova criminal. 6. Procedimento investigatório. 7. Ministério Público Federal – manual. I. Autor. II. Título.

CDDir 341.413

**Elaborado por Juliana de Araújo Freitas Leão – CRB 1/2596**

**AUTORES**

**Pablo Coutinho Barreto**
*Secretário de Perícia, Pesquisa e Análise*
*Procurador da República*

**Paulo Rubens Carvalho Marques**
*Secretário Adjunto da Secretaria de Perícia, Pesquisa e Análise*
*Procurador da República*

**PROCURADORES DA REPÚBLICA**
Yuri Corrêa da Luz
Lúcio Mauro Carloni Fleury Curado
Eduardo Ribeiro Gomes El-Hage
Marcelo Ribeiro de Oliveira
Rafael Ribeiro Rayol
Leandro Musa de Almeida
Fernanda Teixeira Souza Domingos

**SERVIDORES**
Fábio Cardoso Pinto Coelho
Presley McQuade Nogueira Costa
Willian de Araújo Sales
Rodrigo Cauê Araldi
Adriana Shimabukuro
Marcelo Beltrão Caiado
Dalton Nunes Tavares
Winícius Ferraz Neres
Leonardo Peres Fagundes
Vinicius Maia Pacheco

**ORGANIZAÇÃO E COORDENAÇÃO**
Secretaria de Perícia, Pesquisa e Análise

**COLABORADORES**
Marcelo Pires da Silva, Emerson de Paula Rodrigues e Adelino Soares de Brito Filho

**SUPERVISÃO**
Pablo Coutinho Barreto e Paulo Rubens Carvalho Marques

**REVISÃO DO TEXTO**
Roberto D'Oliveira Vieira e Flávio Pereira da Costa Matias

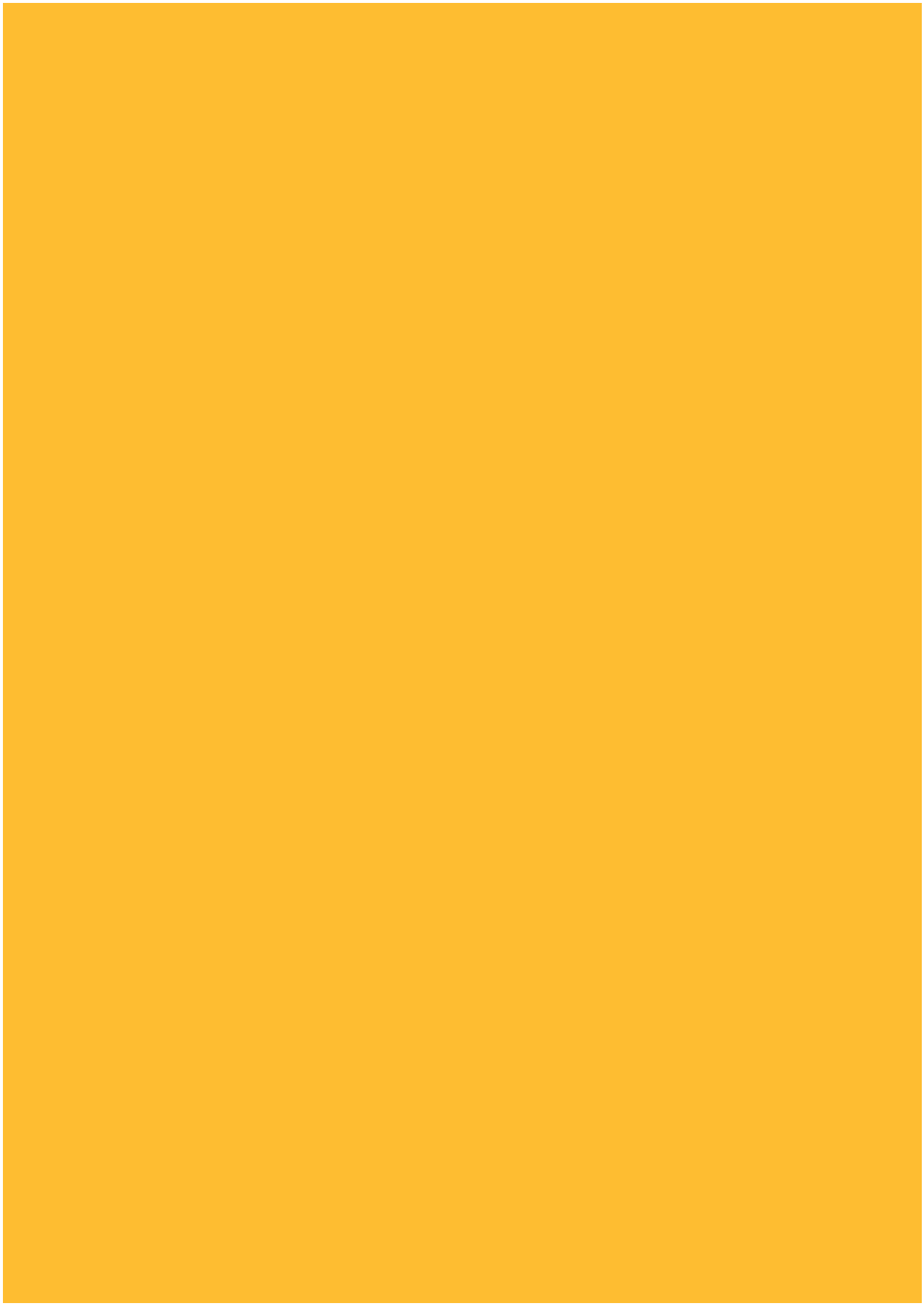
**NORMALIZAÇÃO BIBLIOGRÁFICA**
Coordenadoria de Biblioteca e Pesquisa (Cobip)

**PLANEJAMENTO VISUAL E DIAGRAMAÇÃO**
Bianca Prado / Secom

**REVISÃO**
Ana Paula Rodrigues de Azevedo / Secom
Fernanda Souza / Secom

**PROCURADORIA-GERAL DA REPÚBLICA**
SAF Sul, Quadra 4, Conjunto C
CEP 70050-900 – Brasília, DF
Tel.: (61) 3105-5100
www.mpf.mp.br

# SUMÁRIO



# APRESENTAÇÃO

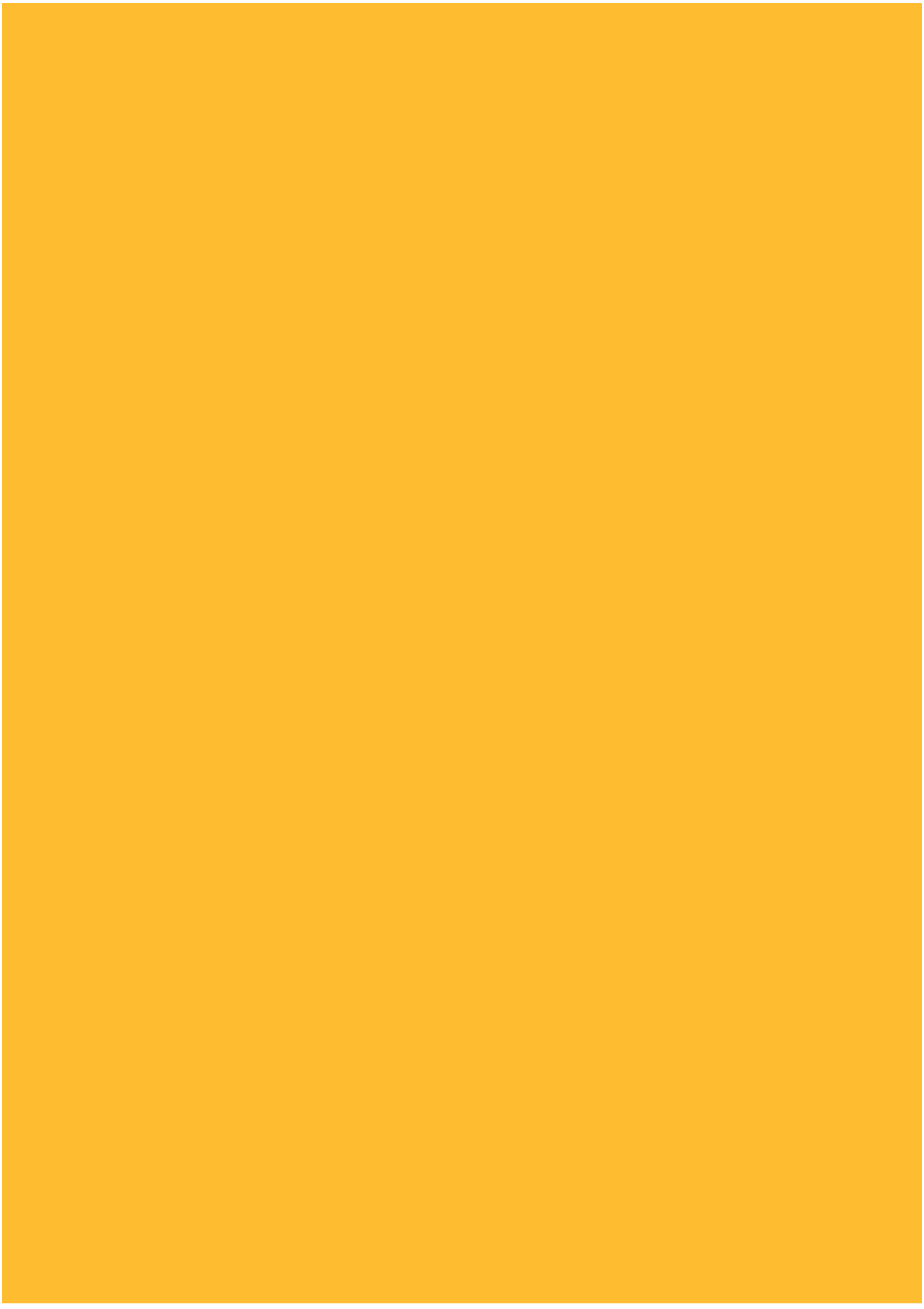
A Lei nº 13.964/2019, vigente desde 23 de janeiro de 2020, alterou a legislação penal e processual penal, disciplinando, entre outros temas, a Cadeia de Custódia e perícias em geral.

A Cadeia de Custódia é fundamental para garantir a higidez e a rastreabilidade dos vestígios, físicos ou digitais. Diante da relevância e da transversalidade do tema, a Secretaria de Perícia, Pesquisa e Análise (Sppea/PGR), por meio da Assessoria Nacional de Perícia em Tecnologia da Informação e Comunicação (Anptic), tem orientado os integrantes do Ministério Público Federal (MPF) a observarem determinadas cautelas básicas para preservação da integridade dos vestígios, sobretudo os digitais.

Esses cuidados se aplicam não apenas a equipamentos eletrônicos apreendidos ou mídias disponibilizadas por colaboradores ou provedores de internet, mas também a dados disponibilizados em nuvem para *download*.

Com a finalidade de orientar os membros do Ministério Público Federal no que diz respeito às questões referentes à Perícia, Pesquisa e Análise, a Sppea/PGR instituiu Grupo de Trabalho visando à elaboração de estudos técnicos e jurídicos relacionados à Cadeia de Custódia de vestígios (Instrução de Serviço nº 17, de 7 de abril de 2020), o que resultou na elaboração do presente manual.

A presente publicação é, portanto, fruto do esforço coletivo de membros e servidores da SPPEA, de Forças-Tarefas do Ministério Público Federal, do Grupo de Trabalho Ferramentas de Tecnologia da Informação (5ª Câmara de Coordenação e Revisão), do Grupo de Apoio sobre Criminalidade Cibernética (2ª Câmara de Coordenação e Revisão), da Secretaria de Tecnologia da Informação e Comunicação e da Secretaria de Comunicação Social.



# CAPÍTULO 1

# CONCEITOS BÁSICOS DE INTEGRIDADE DE EVIDÊNCIAS DIGITAIS

## 1.1 Introdução

A Cadeia de Custódia pode ser considerada uma garantia que busca formalizar, de maneira detalhada, os procedimentos executados sobre determinado elemento relevante para a constituição de uma prova (CAMARGO, 2019, p. 42). Desse modo, ela é essencial para fundamentar as investigações e subsidiar respostas ou questionamentos durante o processo probatório.

Imaginemos as seguintes situações:

a) Um colaborador dirige-se ao Serviço de Atendimento ao Cidadão (SAC) do Ministério Público Federal e disponibiliza um HD externo (*hard disk*) contendo sua caixa de e-mail dos últimos dez anos, fundamental para determinar os vínculos subjetivos entre os investigados e suficiente complemento para subsidiar uma ação penal.

b) Um provedor de aplicação atende à ordem estatal para a implementação de quebras telemáticas, essenciais para a investigação do caso. No seu ofício de resposta, o provedor disponibiliza um *link* para *download* com as credenciais de acesso, diante do caráter sigiloso.

I. As duas situações apresentam contextos bastante comuns nas investigações criminais, os quais tendem a ser ainda mais frequentes. Diante desse cenário, surgem os seguintes questionamentos: Como formalizar o recebimento da mídia de armazenamento? Foi gerada alguma certidão simples cadastrada no sistema de gestão documental do MPF (sistema Único)?

II. Como certificar recebimento dos dados? O provedor só forneceu o *link* para *download*, mas não enviou os dados propriamente ditos. Devo realizar o *download* e gravar em um HD? Como certificar que os dados baixados correspondem àqueles descritos no ofício de resposta?

Esses questionamentos ficam ainda mais complicados quando se tem em mente que vestígios digitais são extremamente sensíveis, podendo inclusive, em alguns casos, ser facilmente modificáveis e bastante voláteis. Em qualquer uma das situações apresentadas, o usuário despreparado que venha a acessar o HD ou a realizar o *download* do *link* cor-

rerá sérios riscos de alterar os dados, perdendo a originalidade destes. Isso pode ocorrer, seja por conta do antivírus instalado, que pode apagar arquivos considerados maliciosos, ou até mesmo se o HD estiver em um formato de partição que não é reconhecido pelo sistema operacional do usuário. Neste último caso, normalmente, o sistema operacional (Windows) fornece a opção de formatar o HD, o que poderia ser drástico.

## 1.2 Como garantir a integridade e a Cadeia de Custódia?

O que fazer diante de cenários como os apresentados? Qualquer ação sem conhecimento mínimo de preservação de evidências digitais pode ser danosa e muitas vezes irreversível. Isso pode gerar margem para questionamentos e até a invalidação da prova no curso da persecução penal.

Portanto, é necessário seguir padrões e procedimentos que busquem garantir a integridade das provas e estabelecer uma sólida Cadeia de Custódia. Se o usuário não possui o mínimo de conhecimento sobre como receber vestígios digitais, deve procurar orientação para que não os comprometa por falhas básicas.

Assim, a Cadeia de Custódia está relacionada ao tratamento das fontes de provas, sendo de fundamental importância na garantia da integridade das evidências digitais. Com isso, evita-se que vícios ocorridos no manuseio das evidências digitais possam dar margem a questionamentos.

Não por acaso, a Lei nº 13.964, de 24 de dezembro de 2019, que alterou o Código de Processo Penal (CPP), expandiu os conceitos e os procedimentos necessários para se determinar a Cadeia de Custódia, no contexto da produção da prova pericial. Nesse sentido, a lei inseriu no CPP o art. 158-A, que conceituou Cadeia de Custódia como "o conjunto de todos os **procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado** em locais ou em vítimas de crimes, para rastrear sua posse e manuseio, a partir de seu reconhecimento até o descarte.

Percebe-se que a lei deu especial atenção à necessidade do detalhamento dos procedimentos realizados, mas também destacou a documentação da história cronológica do vestígio coletado. Nesse sentido, o § 1º do art. 158-A do CPP definiu o marco inicial da Cadeia de Custódia como sendo o momento da preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio.

Nos exemplos apresentados, esse marco inicial corresponderia ao momento da disponibilização dos dados. No momento em que se firma o reconhecimento do vestígio digital, deve ser diligenciado seu isolamento, a fim de garantir sua integridade vestígio este que, em um momento posterior, tornar-se-á uma evidência digital.

Além do marco histórico, a lei relacionou fases que possibilitam o rastreamento dos vestígios, decompondo a Cadeia de Custódia em: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

Todavia, para que se possa compreender essas fases, em especial as de isolamento, fixação e coleta – que compõem a Cadeia de Custódia no contexto dos vestígios digitais – é necessário entender alguns conceitos básicos de prova eletrônica, vestígio digital, dados, sistemas e evidência digital. Esses são princípios básicos para a gestão segura desses elementos.

## 1.3 Conceitos básicos que norteiam o controle e a preservação de vestígios digitais

Quando se estuda a preservação de vestígios digitais, é impossível se afastar dos conceitos da disciplina de Computação Forense, pois esta se relaciona diretamente aos vestígios digitais como objeto de estudo. Essa disciplina é uma ramificação da Criminalística, e objetiva estudar os vestígios cibernéticos que podem se conectar com diferentes áreas, como contabilidade e audiovisual.

É importante observar o perceptível movimento do mundo analógico para o digital, quando, há pouco tempo, os peritos passaram de analisar fitas VHS para dispositivos de armazenamento eletrônico, como memória flash, e que podem ser utilizados como prova para instruir o processo judicial (VELHO *et al.*, 2016, p. 3).

Todavia, na atualidade, ainda é possível identificar que algumas informações não estão disponibilizadas especificamente em dispositivos físicos, como o *pen drive*, mas podem estar hospedadas na nuvem, como websites, instâncias de computação na nuvem, ou simples *links* para *download* de arquivos, muito comum em sites de compartilhamento de arquivos como o mega.nz. Essa forma de disponibilização caracteriza o chamado **vestígio digital**, e requer que sejam adotados mecanismos específicos para analisar cada caso, conforme sua natureza.

Deve-se considerar que a análise de qualquer vestígio digital deve obedecer aos padrões científicos e legais, de forma a garantir que não haja qualquer perturbação que cause prejuízo na validade dos procedimentos e, consequentemente, o descarte da prova. Esses padrões determinam o meio adequado para garantir o que se chama de Cadeia de Custódia das provas.

Antes de continuarmos o estudo sobre a Cadeia de Custódia precisamos definir alguns conceitos que podem parecer confusos:

- **Vestígio:** dado bruto marca, objeto ou sinal sensível que possa ter relação com o fato investigado (VELHO; GEISER; ESPÍNDULA, 2013, p. 10);
- **Indício:** "é expressão utilizada no meio jurídico que significa cada uma das informações (periciais ou não) relacionadas com o conjunto probante" (VELHO; GEISER; ESPÍNDULA, 2013, p. 11);
- **Evidência:** incontestável, que todos podem ver e verificar, certeza manifesta (VELHO; GEISER; ESPÍNDULA, 2013, p. 10);
- **Evidência digital:** Patrícia Peck Pinheiro (2013, p. 216) conceitua que "[...] a evidência digital é toda informação ou assunto de criação, intervenção humana ou não, que pode ser extraído de um compilado ou depositário eletrônico.";
- **Prova:** evidência formalizada no processo (RAFFUL; RAFFUL 2017, p. 52-54);
- **Provas digitais:** a prova digital abrange impulsos eletromagnéticos momentâneos relevantes para a rede ou sistema informático de comunicações eletrônicas. Por tal, a prova digital caracteriza-se como dinâmica e mutável. As competências do investigador exigem que este realize uma investigação estruturada temporalmente, comparando vários períodos temporais, permitindo aceder à prova digital de maior utilidade para a investigação (CANCELA, 2016, p. 20).

Importante ressaltar que as provas eletrônicas, por exemplo *pen drive* USB, podem conter dados digitais armazenados, que por sua vez podem se tratar de provas digitais gravadas (como dados cadastrais, dados do Google Drive, iCloud, OneDrive) em dispositivos eletrônicos encaminhados por provedores de aplicação.

Para facilitar o entendimento, vejam-se alguns exemplos de provas digitais:

- endereço de IP;
- mensagens de e-mail, disponíveis em diversos formatos como: EML, PST, EMLX, MSG, MBOX;
- fotos (PNG, JPEG etc.);
- metadados de arquivos digitais;
- registros de acessos a aplicações;
- registros de ações de usuário nos Sistemas Operacionais;

- dados de GPS;
- diversos outros tipos que podem estar dispostos das mais variadas formas como: *backup* de dados no Google Drive, iCloud etc.

Todos esses exemplos apresentados são provenientes, de algum modo, do meio digital que normalmente é gerado por algum tipo de sistema informático. Nesse contexto, para o melhor entendimento dos sistemas informáticos e dos meios de obtenção de provas digitais, vejamos alguns conceitos apresentados pela *Convenção de Budapeste de Cibercrime*, ocorrida em 23 de novembro de 2001, e que servirá para elucidar o contexto dos meios de obtenção de provas no meio digital:

> a) **Sistema informático** significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de um entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
>
> b) **Dados informáticos** significa qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;
>
> c) **Fornecedor de serviço** significa:
>
> (I) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático; e
>
> (II) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores deste serviço.
>
> d) **Dados de tráfego** significa todos os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente. (MPF, 2001, p. 3)

Diante do exposto, reitera-se ser de extrema necessidade ter muita atenção ao analisar vestígios digitais, pois estes poderão ser de suma importância na instrução das provas durante a persecução penal. Com isso em mente, torna-se claro que, ao receber no SAC um ofício encaminhando um *pen drive* ou HD contendo dados armazenados, é necessário que sejam adotadas medidas para o isolamento e a preservação do dispositivo e dos dados. Deve-se, portanto, evitar conectar o dispositivo no computador, ainda que para breve análise do conteúdo.

Mas podem ser levantadas algumas dúvidas quanto ao motivo dos vestígios e das provas digitais serem tão específicos e sensíveis, demandando tarefas especializadas. Essa condição se deve às suas características peculiares, conforme afirma Vaz (2012):

> 1. Imaterialidade e invisibilidade: representada por uma sequência de bits, necessita de um suporte para transporte
>
> 2. Volatilidade e fragilidade: pode ser manipulada, intencionalmente ou não, exemplo: falta de bateria, gravação acidental. Frágil, pois pode ser manipulada e alterada
>
> 3. Dispersão: pode estar em vários locais diferentes (HD, cache, contas, provedores, nuvem etc.)
>
> 4. Copiada sem degradação: indefinidamente e as cópias são exatamente como os originais. (VAZ, 2012, p. 68-69)

O isolamento de vestígio digital é uma fase extremamente importante para preservar a integridade da evidência, especialmente para evitar a hipótese de deleção (*wipe*) remota. Ocorre que, apesar de essa fase ser prevista após a fase do reconhecimento de vestígio, na maioria das vezes, elas podem ocorrer ao mesmo tempo. O isolamento deve ser feito tão logo o vestígio seja identificado.

Entre as modificações que se busca evitar, destacam-se a alteração, a supressão, a inserção ou a própria destruição. Todavia, como na Cadeia de Custódia, temos que registrar a evidência e sua cronologia. Nesse contexto, mostra-se necessário definir algumas informações do vestígio identificado, isolado e coletado. Assim, a que permite verificar se o vestígio permanece íntegro é o *hash*, que é gerado por uma função *hash* (algoritmo matemático que mapeia dados de comprimento variável para dados de comprimento fixo) importante para manutenção de integridade de dados, garantindo que a informação não foi alterada.

Em regra, uma vez calculado e registrado o *hash*, este pode ser reproduzido quantas vezes se faça necessário para verificar a integridade da informação. Assim, se um vestígio foi coletado na fase investigativa, com o registro do *hash*, ele poderá ser verificado com o cálculo *hash* na fase de instrução, quando as provas serão produzidas na fase processual. Assim, se um bit de dado for alterado, o valor do *hash* será diferente e não poderá ser verificado.

Existem duas categorias de isolamento: o físico e o lógico. Para o contexto dos vestígios digitais, o isolamento lógico é o que se destaca. O isolamento lógico, diferentemente do isolamento físico – que foca na delimitação do perímetro físico da área investigada – possui relação com a natureza lógica dos dispositivos alvos de investiga-

ção. A natureza do dispositivo, que será isolado para posterior apreensão (se for o caso), determinará o procedimento mais adequado (VELHO *et al.*, 2016, p. 28).

## 1.4 Uma visão prática

Nessa linha de raciocínio, podem-se citar os cenários mais comuns na área de investigação do Ministério Público Federal:

**IMPLEMENTAÇÃO DE QUEBRAS TELEMÁTICAS**

1. O provedor de aplicação fornece credenciais de login para acesso a uma conta disponibilizada via protocolo IMAP. Em outras palavras, uma conta espelho da caixa de e-mail do investigado pode ser acessada pelo investigador por meio de um navegador, normalmente dentro de uma janela de tempo;

2. O provedor de aplicação fornece um *link de download* do conteúdo da implementação da quebra, como Gmail, Google Drive, iCloud, OneDrive, entre outros. Normalmente eles disponibilizam uma chave de acesso ao link e outra chave de acesso para descriptografar o dado baixado. Tal modalidade não diz respeito à comunicação de dados, mas aos dados armazenados em si mesmos, tratando-se de medida investigativa a ser adotada inclusive em apurações cíveis;

3. Provedor de aplicação encaminha um HD – *hard disk* – contendo o conteúdo da implementação da quebra telemática, conforme o item anterior.

**COLABORAÇÃO E FORNECIMENTO VOLUNTÁRIO DE DADOS**

4. Um colaborador apresenta-se ao Serviço de Atendimento ao Cidadão (SAC). Nesse momento ele apresenta um HD/*Pen drive* (mídia física) contendo, por exemplo, sua caixa de e-mail, documento fundamental para determinar os vínculos subjetivos dos investigados, complemento suficiente para subsidiar uma ação de responsabilidade.

**DADOS COLETADOS DA INTERNET, PORTANTO NÃO FORNECIDOS DIRETAMENTE PELO COLABORADOR**

5. Quando o investigador coleta dados hospedados e abertos na nuvem como sites, fotos, dados de rede sociais, links de compartilhamento, entre outros.

Pergunta-se: quais são as melhores práticas para se garantir o isolamento e a integridade dos vestígios digitais? E o que devo evitar para não colocar em risco a integridade das evidências? Como eu devo certificar o procedimento adequado para o caso concreto?

Sempre que tiver dúvidas, consulte o setor responsável pelo manuseio desses vestígios ou entre em contato com Assessoria Nacional de Perícia em Tecnologia da Informação (ANPTIC/Sppea).

Este manual contempla um capítulo específico para as fases mais importantes da Cadeia de Custódia. Alguns dos cenários aqui relatados já foram apresentados no início deste capítulo, demonstrando alguns problemas que poderão surgir ao longo da instrução. Não obstante, a seguir serão demonstrados alguns cuidados que se deve ter ao realizar a coleta de dados na internet, além de ações a serem evitadas para assegurar a integridade das evidências e garantir uma sólida Cadeia de Custódia em sua fase inicial.

### 1.4.1 O que não se deve fazer: erros mais comuns:

#### CENÁRIO 1

- Ao utilizar uma ferramenta de sincronização de caixas de e-mail por meio do protocolo IMAP (como o Thunderbird) não realize o procedimento em um computador comum. Isso porque, caso esse computador possua um antivírus ou esteja sob uma rede protegida por firewall, esses elementos externos poderão modificar ou excluir informações contidas nos e-mails, como excluir *spams* ou arquivos supostamente maliciosos dos anexos.

- É um erro comum fazer *download* utilizando um ambiente não controlado, sem que o responsável pela coleta tome conhecimento de que sua conexão está sob proteção de *firewall*. Tal procedimento pode modificar os dados do *download*.

- Os peritos da ANPTIC podem atuar na preservação da Cadeia de Custódia, realizando o *download* e a geração dos *hashes*, assim como a indexação de todo o conteúdo, sendo que na solicitação de quebra alguns provedores permitem o compartilhamento da solicitação com e-mails adicionais. Nesses casos, a ANPTIC deverá ser contatada para informar o e-mail do perito para o qual os dados serão enviados, possibilitando o tratamento inicial.

#### CENÁRIO 2

- As mesmas considerações do cenário 1. Todavia, é muito importante que não se certifique um vestígio antes de recalcular os *hashes* dos arquivos baixados e compará-los com os fornecidos, buscando verificar a integridade dos dados.

**CENÁRIO 3 E 4**

- Nunca conecte o dispositivo de armazenamento diretamente em uma máquina que possua um antivírus sem o devido preparo ou outro software de segurança com a mesma finalidade. O antivírus poderá analisar o conteúdo dos dispositivos para excluir os arquivos maliciosos. Mesmo que exista conteúdo desse tipo, se removido, o vestígio perderá sua originalidade, por decorrência da falta de um correto isolamento.

**CENÁRIO 5**

- Esse cenário é muito peculiar e, normalmente, o responsável pela coleta não terá nenhuma informação para fazer a comparação de hashes. Assim, utilize ferramentas consolidadas para coleta da informação e na certificação da coleta não deixe de calcular os *hash* dos dados para garantir o marco temporal da integridade destes.

### 1.4.2 O que pode ser feito como boa prática

Para os cinco cenários supratranscritos, é muito importante que se documente todo o procedimento realizado, bem como as ferramentas utilizadas. Tal procedimento deverá ser realizado desde a fase de isolamento até o procedimento de coleta, documentando, inclusive, as ferramentas utilizadas na fase do processamento.

Assim, é fundamental, em todos os cenários, ter um ambiente preparado e controlado para receber e tratar os vestígios, garantindo-se um correto isolamento e a coleta de dados. Certifique as informações que identifiquem o vestígio, a data do reconhecimento, o local e o cálculo *hash* de todos os dados apresentados e coletados, descrevendo-se a natureza, a peculiaridade e a forma de armazenamento.

Quanto à forma de armazenamento, é altamente recomendada a garantia do armazenamento para dois dos cenários apresentados. O primeiro diz respeito ao cenário 5 e decorre do armazenamento da forma original do vestígio, e ocorrerá quando realizado o *download*, o espelhamento de determinado HD (que precisar ser restituído), ou quando realizada a coleta externa de dados abertos na nuvem.

O segundo cenário é o que se chama de cópia de trabalho. Ocorre quando é realizado todo o processamento dos dados, de forma a disponibilizá-los para análise. Em regra, nunca se processa nada sobre a cópia originária, mas sim na cópia de trabalho, para que se garanta sempre a integridade da evidência original.

Tenha em mente que o primeiro *download*, realizado no cenário 2, será o primeiro procedimento de "geração" dos dados locais, portanto é a cópia originária do vestígio

digital. Uma outra cópia, chamada de melhor evidência, será utilizada sempre que ocorrer algum problema na cópia de trabalho, evitando manuseios e possíveis problemas na manipulação da evidência original.

**CENÁRIO 1**

- Prepare um ambiente controlado e isolado para realizar a cópia da caixa de e-mail, de modo a evitar qualquer interferência externa sobre os dados que estão sendo baixados.
- Não desabilite o antivírus pensando que todos os problemas estão resolvidos; você pode estar colocando sua máquina e a rede em risco; converse com a equipe técnica de tecnologia da informação para que ela possa disponibilizar esse ambiente para você.
- Lembre-se de que seu computador ainda pode estar sob a proteção de *firewall*, o que é recomendado como requisito de segurança da informação. Porém, ao baixar os dados, o *firewall* pode impedir que alguns pacotes de dados entrem na rede do seu computador, o que ocasionará a perda da originalidade do vestígio.
- Certifique todo o procedimento realizado.
- Crie uma cópia original e uma cópia de trabalho que será disponibilizada para processamento, e, se for o caso, uma cópia de melhor evidência.
- Documente toda a identificação do vestígio, detalhando sua natureza e peculiaridades importantes, assim como a geração de *hash* de todos os arquivos e o marco cronológico do procedimento.
- Assine a certidão eletronicamente, se possível com certificado digital ICP-Brasil.

**CENÁRIO 2**

- A mesmas considerações do cenário 1.
- Observe que, normalmente, os provedores disponibilizam um arquivo criptografado (extensão GPG, Segurança da Privacidade GNU) e, dentro deste, um arquivo zipado (ZIP, 7z). Ocorre que o original é o arquivo criptografado, e não propriamente o zipado, pois o dado disponibilizado foi o da extensão *"GPG"*, e será ele o certificado. Normalmente, o *hash* presente no ofício de resposta do provedor será sobre o arquivo GPG.
- Calcule novamente o *hash* dos dados baixados e compare com o *hash* disponibilizado no ofício de resposta do provedor.

- Se o provedor não fornecer o *hash*, deve-se documentar o *hash* calculado na certidão para garantir o marco inicial do reconhecimento e da coleta.

## CENÁRIOS 3 E 4

- Se o provedor não fornecer o *hash*, deve-se documentar o *hash* calculado na certidão para garantir o marco inicial do reconhecimento e da coleta.

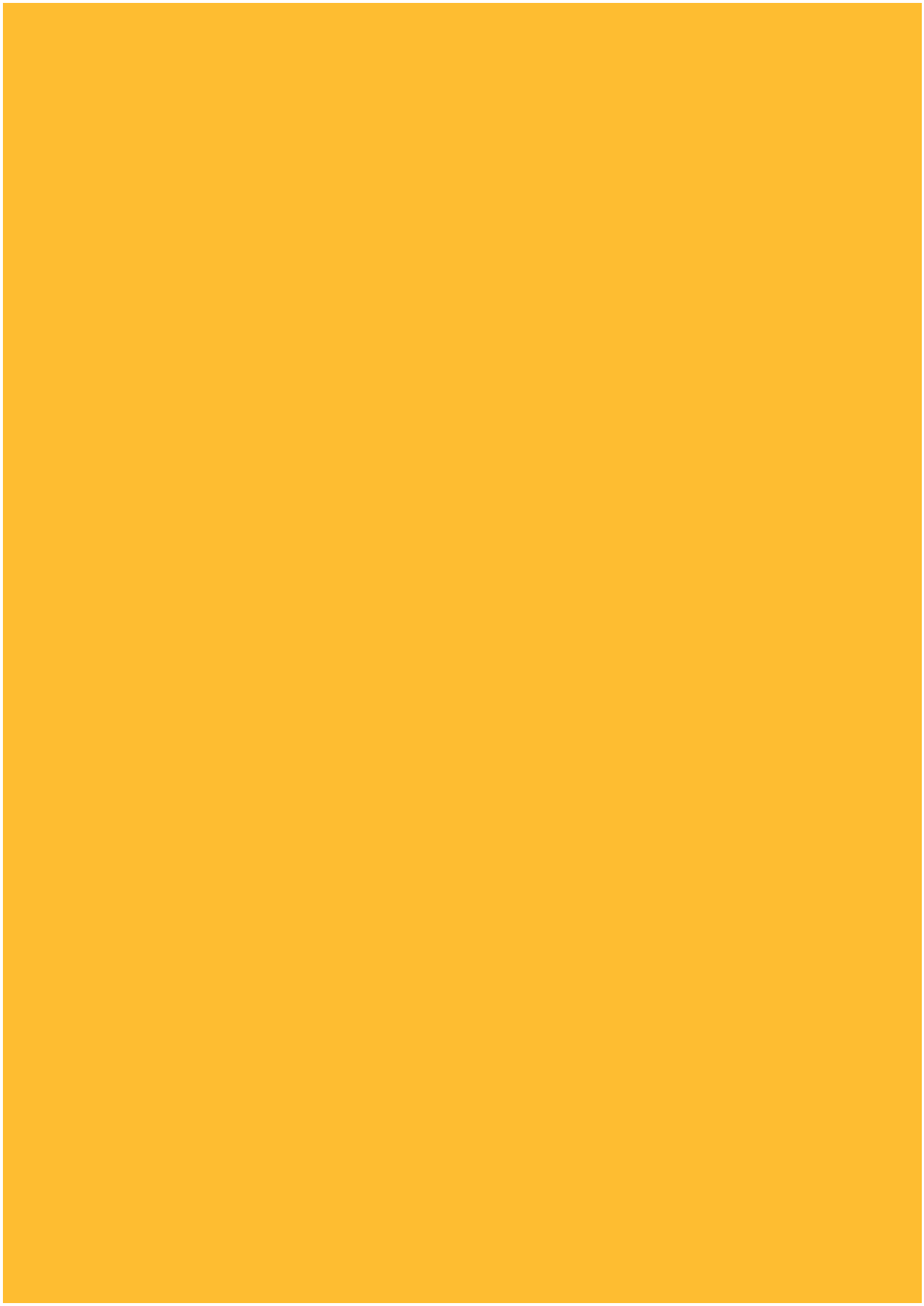
- Considerações de isolamento e certificação do cenário 1. Nesse caso, não será problema a existência de um *firewall*, mas sim do antivírus ou de qualquer ferramenta presente no computador que tenha autorização de acesso aos dispositivos de armazenamento.

- Sempre utilize um bloqueador de escrita para conectar o dispositivo de armazenamento. Bloqueadores de escrita são utilizados para evitar que qualquer programa possa modificar o conteúdo dos dispositivos de armazenamento.

- Existem dois tipos de bloqueadores de escrita: por *software* e por *hardware*. Os bloqueadores por *hardware* costumam ter elevado custo. Caso não estejam disponíveis, recomenda-se a utilização de bloqueadores de escrita por *software*, que desempenham papel similar.

## CENÁRIO 5

- Além das recomendações de certificação apresentadas no cenário 1, é necessário coletar mais informações, como domínio, IP do site ou provedor (quando esta for hospedagem compartilhada), entre outros dados. No capítulo 2 deste manual, serão apresentadas as ferramentas necessárias para a coleta dessas informações.



# CAPÍTULO 2

# IDENTIFICAÇÃO, ISOLAMENTO, COLETA E PRESERVAÇÃO DOS VESTÍGIOS DIGITAIS

## 2.1 Introdução

Conforme mencionado no capítulo 1, toda a coleta de materialidade deve ser acompanhada do cálculo de *hash* dos arquivos coletados. Considerando a possibilidade de ocorrer a chamada colisão de *hashes*, sugerimos que a coleta, sempre que possível, seja realizada usando o algoritmo SHA256 e, caso este ou um superior não esteja disponível, deve-se fazer uso de dois algoritmos, como o MD5 e o SHA1.

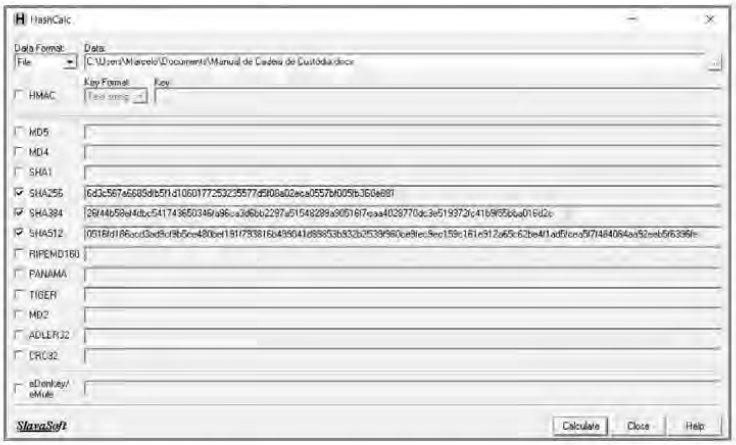



***Figura 1:*** *A ferramenta HashCalc é gratuita e pode ser utilizada no Windows*

A formalização da coleta e a garantia de integridade dessas informações podem ser feitas por meio da emissão de uma Certidão de Coleta e Integridade de Dados ou, ainda, por meio de uma Certidão de Cadeia de Custódia.

Após a coleta, o(s) arquivo(s) pode(m) ser gravado(s) em extensões como ZIP, TXT, DOC, PST. PDF, PNG etc. Esses procedimentos devem ser realizados por uma equipe habilitada. No MPF, os atos normativos que determinam os servidores que estão capacitados para fazer essas atividades estão listados em https://portal.mpf.mp.br/intranet/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/normativos.

Uma certidão deve conter, no mínimo, a data de coleta, os procedimentos utilizados, o *status* da página, o cálculo dos *hashes* e a assinatura dos responsáveis pelo

procedimento, de preferência usando certificado ICP-Brasil. Esses dados gerados são usualmente gravados no sistema Único, aba íntegra ou, ainda, gravados em mídia não regravável lacrados, acompanhados pela respectiva certidão.

Maiores detalhes sobre a preservação da Cadeia de Custódia estão em *Orientações para a Preservação da Cadeia de Custódia de Vestígios Digitais (com base na Lei Anti-crime nº 13.964/2019)* da Sppea/PGR disponível em http://intranet.mpf.mp.br/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios.

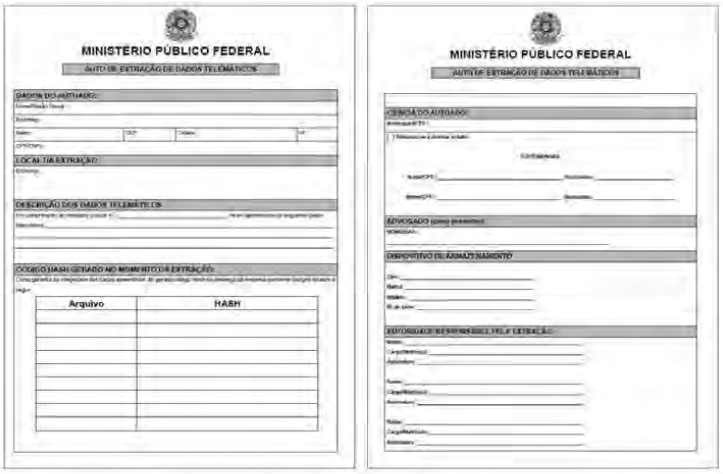



***Figura 2:*** *Exemplo de uma Certidão de Cadeia de Custódia*

### 2.1.1 Redes Sociais e Provedores de Serviço

#### 2.1.1.1 Facebook/Instagram/Messenger

##### 2.1.1.1.1 Coleta de dados

As coletas de perfis ou grupos que estão com os dados abertos e on-line, podem ser realizadas com o uso de programas específicos, ou utilizando extensões de navegadores que fazem um printscreen da tela ou, ainda, fazendo uma impressão em formato PDF do endereço denunciado.

Um exemplo é a extensão Nimbus Screenshot para o navegador Firefox (https://addons.mozilla.org/pt-BR/firefox/addon/nimbus-screenshot/).

É importante observar que na notícia crime deve constar a URL exata denunciada para que seja realizada especificamente a coleta do conteúdo supostamente ilícito.


*Figura 3: O Nimbus permite coletar páginas inteiras e gravar em vários formatos*

**DICA:** Caso a página a ser coletada esteja fora do ar, podemos usar recursos como o site http://archive.org ou ainda usar o Termo de Cooperação Técnica e Operacional do MPF com a ONG Safernet para tentar recuperar esses dados já apagados da internet, mas com possibilidade de terem sido gravados anteriormente e mantidos nessas bases de dados. O MPF, por meio do NTCCC da PR/SP, possui acesso à base de dados da ONG Safernet.

#### 2.1.1.1.2 Pedido de preservação

A ferramenta *Law Enforcement Online Requests*, acessada pelo endereço eletrônico: https://www.facebook.com/records, permite solicitar preservação de dados por até 90 dias, com possibilidade de dilação de prazo após o vencimento deste.

Para o acesso inicial, é necessário digitar um e-mail institucional, como: fulano@mpf.mp.br. Esse e-mail pode ser da autoridade policial, da autoridade administrativa ou ainda do servidor do Ministério Público ou do Judiciário. Após alguns minutos, a autoridade/servidor receberá um e-mail contendo um link que permite o acesso à plataforma *Law Enforcement*.

Para solicitar a preservação, é necessário que a autoridade possua o perfil ou grupo do Facebook/Instagram que se deseja preservar ou, ainda, no caso de comentários, é necessário que se aponte o endereço específico de cada comentário cuja preservação se deseja requisitar. Se existirem, por exemplo, 40 comentários com conteúdo ilícito, o requerente deverá indicar o URL de cada um dos 40 comentários para a respectiva preservação.

Exemplos de endereços URL do Facebook:

- **Perfil de usuário pelo id:**
  https://www.facebook.com/profile.php?id=000000000000000.
- **Perfil do usuário pelo nome:**
  https://www.facebook.com/FulanoDeTal2394
- **Grupo:**
  https://www.facebook.com/groups/0000000000000000.
- **Publicação de uma foto:**
  https://www.facebook.com/IBDDIG/photos/a.1466886163599258.1073741827.1465228183765056/1496430570644817/?type=1&theater.

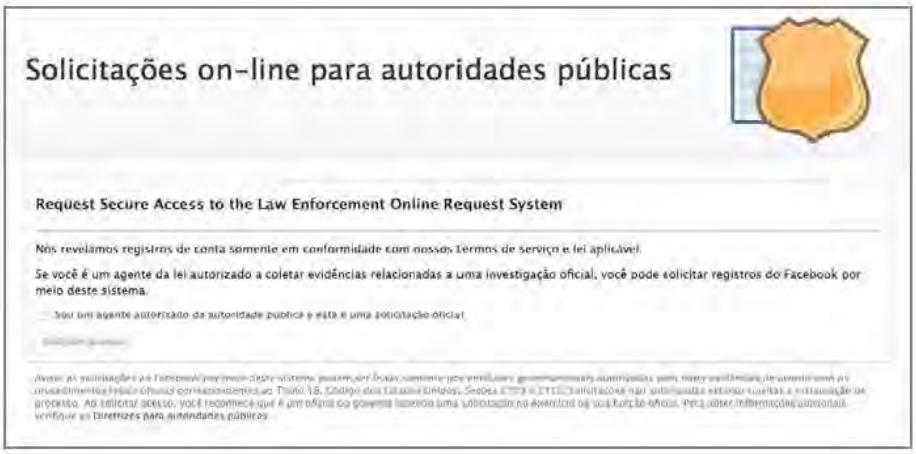



***Figura 4:*** *Formulário on-line para requisições de preservação e quebra telemática do Facebook*

Dados que podem ser preservados e posteriormente requisitados (esta lista não é exaustiva):

- **Dados do usuário:** nome, e-mail, data de nascimento, número de telefone celular etc.;
- **Telefone:** caso o usuário tenha realizado a verificação em duas etapas ou tenha indicado um número de telefone celular no ato de sua inscrição na rede social;
- **Endereço IP da conexão usada:** para realização do cadastro inicial no Facebook;
- **Endereço MAC:** da placa de rede da estação no momento do cadastro inicial no Facebook;

- **Listagem dos amigos adicionados;**
- **Listagem dos grupos de que o usuário participa:** este dado é particularmente importante nas investigações de pedofilia e racismo;
- **Mensagens trocadas entre usuários:** Correio Eletrônico, sendo, também, necessário indicar o período;
- **Mensagens instantâneas trocadas entre usuários**, com indicação do período (datas);
- **Páginas administradas pelo usuário.**

**IMPORTANTE:** A maioria dos provedores norte-americanos comunica o alvo da quebra telemática quanto às informações requisitadas por autoridades. Dessa maneira, é importante constar no pedido do MP ou da Justiça, a necessidade de SIGILO DE DADOS. Nos casos em que será demandado o apoio dos peritos da ANPTIC para o *download*, geração de *hashes* e indexação do conteúdo, deve ser verificado o procedimento do operador que irá fornecer os dados, pois, em alguns casos, é necessário informar antecipadamente se a quebra será compartilhada com algum outro e-mail, sendo, nesse caso, necessário contatar a ANPTIC para obter o e-mail do compartilhamento. No momento de desenvolvimento deste manual, tal procedimento era necessário nas quebras da Microsoft e da Google.


*Figura 5: Na requisição da autoridade é necessário possuir o endereço do perfil, grupo ou comentário alvo da investigação*

#### 2.1.1.1.3 Dicas de pesquisa

A ferramenta para autoridades do Facebook https://www.facebook.com/records permite, além de solicitar preservação de dados, fazer pesquisas utilizando e-mail ou telefones cadastrados para verificar se existem perfis ou grupos relacionados a essas informações. Trata-se de uma importante pesquisa realizada quando se tem somente um e-mail ou número de celular do investigado.

Conforme veremos a seguir, inserimos números de telefones de investigados na ferramenta do Facebook e imediatamente recebemos a informação de que existe algum perfil que utilizou esses números para realizar cadastro na plataforma.

Com esse retorno positivo, a autoridade pode requisitar dados adicionais para o provedor de serviço:

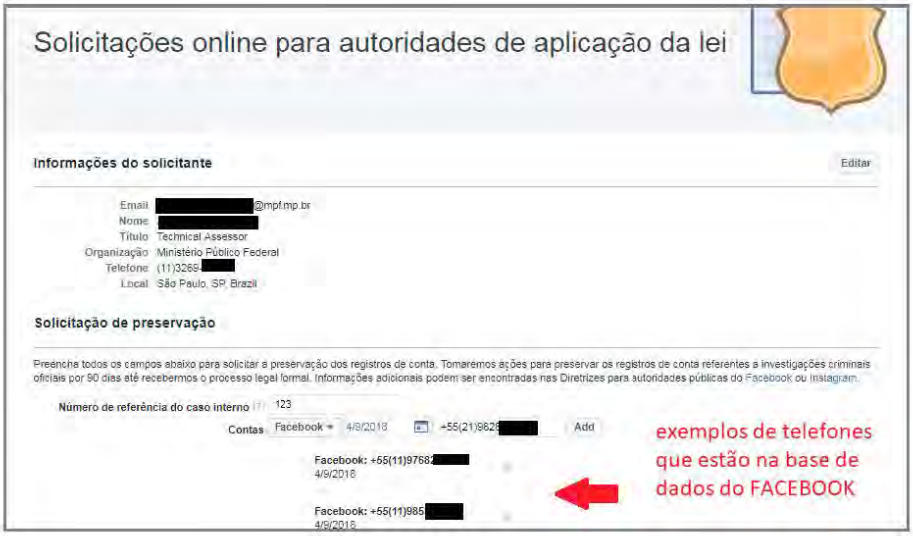



*Figura 6: Exemplo de um retorno "positivo" quanto à existência de um celular na base de dados do Facebook*

A seguir, consta o exemplo de um erro por meio de mensagem que recebemos quando tentamos pesquisar um celular ou e-mail que não tem nenhum relacionamento com perfis ou grupos do Facebook:


*Figura 7: Celular pesquisado não está cadastrado na base de dados do Facebook*


*Figura 8: E-mail pesquisado não está cadastrado na base de dados do Facebook*

### 2.1.1.2 WhatsApp

A ferramenta *Law Enforcement Online Requests*, acessada pelo endereço eletrônico: https://www.whatsapp.com/records, funciona de maneira muito similar à ferramenta do Facebook, pois permite solicitar preservação de dados por até 90 dias, com possibilidade de dilação desse prazo após o vencimento do período original.

Para o acesso inicial, é necessário digitar um e-mail institucional, por exemplo: fulano@mpf.mp.br. Esse e-mail pode ser da autoridade policial, da autoridade administrativa ou ainda do servidor do Ministério Público ou do Judiciário. Após alguns minutos, a autoridade/servidor receberá um e-mail contendo um link que permite o acesso à plataforma *Law Enforcement*.

*Figura 9: Ferramenta Law Enforcement do WhatsApp, acessível somente para autoridades*

Dados que podem ser requisitados diretamente ao WhatsApp pelo Ministério Público e por autoridades policiais via ofício: telefone, nome, modelo do aparelho, versão do aplicativo, data inicial e final e status da conexão.

Dados que podem ser requisitados ao WhatsApp com ordem judicial: informações de grupo, mudança de números, contatos, fotos do perfil, status antigos, último número IP conectado e extrato de mensagens (metadados).

***Figura 10:*** *No caso de identificação de fake news, a coleta do endereço da URL da mensagem é exigência do WhatsApp*

O extrato de mensagens ou "Programa de Interceptação de Mensagens" é um serviço disponível para autoridades desde agosto de 2019. Nessa requisição, a cada 24h, durante 15 dias, uma autoridade recebe Extratos de Mensagens (metadados) de até 10 alvos, contendo números de origem/destino, data, hora, IP com porta lógica e tipo de mensagem. ATENÇÃO: não é fornecido conteúdo.

Obs.: O WhatsApp NÃO coleta IMEI de celulares e o aplicativo WhatsApp WEB não coleta o número IP do computador.


***Figura 11:*** *Exemplo da Interceptação de Metadados do WhatsApp*

**IMPORTANTE:** Caso esteja lidando com uma situação que envolva ameaça concreta e iminente de morte ou danos físicos a um indivíduo, a maioria dos provedores de

serviço fornece tratamento prioritário. Verifique se no portal ou no formulário de pedido consta essa informação. Os critérios utilizados por esses provedores seguem as leis norte-americanas 18 U.S.C. § 2702(b)(8) e § 2702(c)(4).

### 2.1.1.3 Twitter

A ferramenta para autoridades fornecida pelo Twitter é acessível pelo endereço eletrônico: https://legalrequests.twitter.com/form/landing_disclaimer.

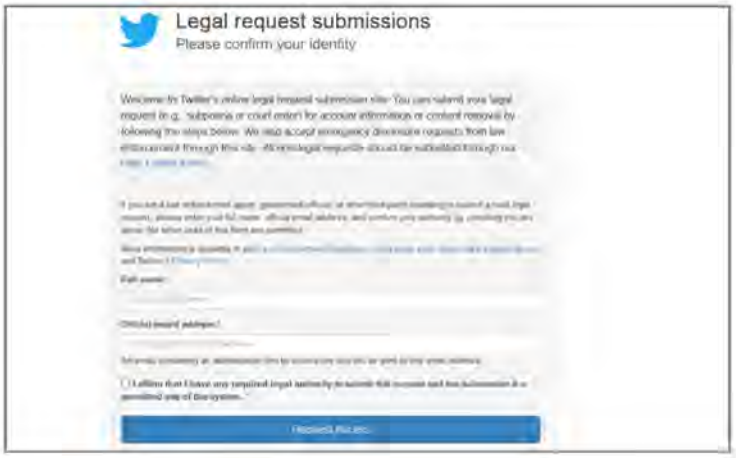



***Figura 12:*** *Ferramenta do Twitter fornecida para autoridades*

De acordo com o Twitter, os dados dos usuários são guardados por 18 meses. As seguintes informações poderão ser requisitadas à plataforma:

- nome, sobrenome, senha, e-mail e nome de usuário;
- localização, foto da conta e do fundo, localização;
- número de celular para recebimento de SMS e catálogo de endereços;
- *tweets*, as contas seguidas, *tweets* favoritos;
- coordenadas exatas da localização dos tweets;
- endereços IPs, data/hora/fuso, navegador utilizado, domínio referente, páginas visitadas, operadora do dispositivo móvel, dispositivo móvel, IDs de aplicativos e termos de buscas;
- links visitados e quantidade de vezes que foi clicado.

### 2.1.1.4 Google (YouTube, Google Photos)

A ferramenta para autoridades fornecida pelo Google é acessível pelo endereço eletrônico: https://lers.google.com.


***Figura 13:*** *A ferramenta Google LERs somente para autoridades*

Ao contrário das outras ferramentas, o Google exige a criação de uma conta no padrão Fulano@lers.google. Uma vez criada essa conta, o acesso ao serviço fica fixo.

É possível requisitar à Google dados do Google Drive, desde que a autoridade possua o número do celular + IMEI. Exemplos de informações que podem ser obtidas: informações de *backup* de aparelhos, conversas por aplicativos, WhatsApp, Telegram (armazenadas na nuvem), e-mails, anotações pessoais, localizações de GPS, lista de contatos, arquivos e planilhas.

**DICA:** A ferramenta LERS da Google possui a opção de "Respostas Compartilhadas" que permite que as respostas sejam encaminhadas para diferentes autoridades (exemplo, Judiciário e MPF).

### 2.1.1.5 Microsoft (Skype, Xbox, Hotmail)

A Microsoft está trabalhando para fornecer um portal on-line para autoridades, mas ainda não foi concluído, até o momento de disponibilização do presente material. Por isso, todas as requisições de preservação ou obtenção de dados serão realizadas via ofícios, que deverão ser encaminhados à Microsoft Corporation, por meio do correio eletrônico lelatam@microsoft.com ou de outro canal indicado pela Sppea em seu Portal Eletrônico.

Pedidos relacionados ao serviço Skype, devem ser direcionados à Skype Communications Sarl (e-mail lerm@skype.net), por meio dos contatos indicados pela Sppea, também em seu Portal Eletrônico.

Dados que poderão ser solicitados no serviço Skype: dados cadastrais, dados de criação de conta, transações financeiras e interconexões com a rede PSTN.

Obs.: É importante mencionar na requisição que se trata de documento confidencial e que não poderá ocorrer a comunicação ao usuário do serviço, pois trata-se de exigência prevista na lei norte-americana.

#### 2.1.1.6 Apple (iCloud)

Seguindo o modelo do Google, é possível requisitar à Apple dados relativos a celulares iPhone. Nos casos em que a autoridade possua o número do celular e o IMEI do investigado, podemos requisitar informações de *backup* de aparelhos, conversas por aplicativos, WhatsApp, Telegram (armazenadas na nuvem), e-mails, anotações pessoais, localizações de GPS, lista de contatos, arquivos e planilhas.

O encaminhamento de ofícios ou requisições judiciais deve ser feito à Apple Brasil (e-mail: lawenforcement@apple.com), por meio dos contatos informados pela Sppea em seu Portal Eletrônico.

### 2.1.2 Páginas *on-line*

Ao contrário da coleta de perfis nas redes sociais, em determinadas situações é necessário realizar a coleta do SITE INTEIRO, com todo o código fonte da página e às vezes do conteúdo das mídias e dos arquivos armazenados na página.

Ilustramos dois métodos para coletar essas informações, sendo que também deve ser consultada a lista de softwares homologados pela Sppea:

a) **NAVEGADOR:** Exemplo no Firefox Menu Arquivo – Salvar Como – Página WEB completa (escolha um local onde serão gravados estes arquivos);

b) **Ferramenta HTTRACK:** Realiza o download completo da página (https://www.httrack.com/).

Após a coleta do site, é imprescindível seguir os procedimentos de cálculo de *hashes* (compacte todos os arquivos em um único ZIP ou RAR, por exemplo), bem como a elaboração da Certidão de Integridade e a devida disponibilização do conteúdo coletado conforme orientação da autoridade. Caso seja necessário manter sigilo no conteúdo do arquivo compactado, utilize a opção de criptografia AES do 7-ZIP, com uma senha de, no mínimo, 18 caracteres.


*Figura 14: O HTTRACK é gratuito e pode ser utilizado para fazer a cópia de um site completo*

### 2.1.3 E-mails

Uma mensagem de e-mail é composta por duas partes: o cabeçalho e a mensagem.

O cabeçalho do e-mail retém informações importantes como o ID da mensagem, o caminho percorrido pela mensagem, o sistema operacional utilizado, o serviço de mensagens utilizado, o número IP do remetente ou do serviço de e-mail, entre outras informações.

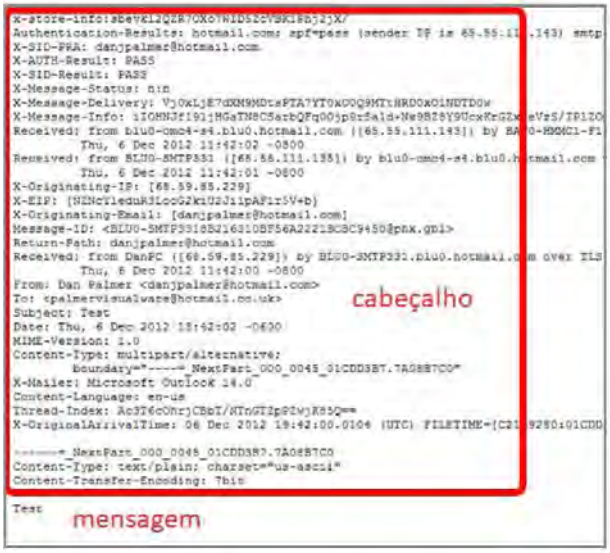



*Figura 15: O cabeçalho do e-mail é essencial para a análise da perícia, pois detém várias informações sobre o remetente da mensagem*

Para conservar o cabeçalho de um e-mail, o usuário pode encaminhar a mensagem completa para a autoridade ou equipe de coleta usando a opção "encaminhar como anexo", caso essa opção esteja disponível na aplicação utilizada.

Nos casos em que a mensagem está acessível por um serviço de e-mail, sempre existirá a opção do acesso ao cabeçalho do e-mail no menu dessas ferramentas. Exemplo: no serviço do GMAIL essa opção está no menu descrito como 'exibir código fonte da mensagem". No HOTMAIL, por sua vez, esta opção está identificada como "mostrar original".

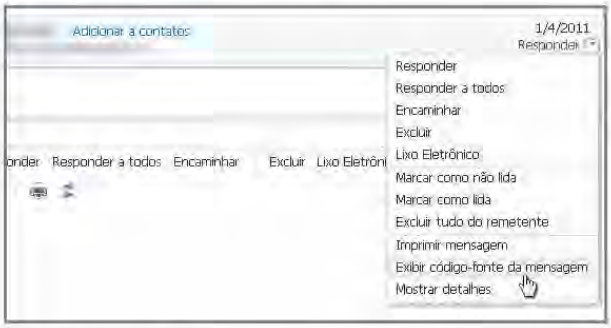



*Figura 16: O acesso do cabeçalho do e-mail na ferramenta do GMAIL*

Após a coleta dos dados, todos os procedimentos relativos ao cálculo de *hashes*, bem como a emissão de uma certidão de integridade devem ser seguidos pela equipe responsável pelos trabalhos.

### 2.1.A *Download* de quebras telemáticas

Alguns provedores de serviço disponibilizam as respostas às requisições de quebra telemática por meio do acesso a links encaminhados ao Judiciário ou ao MP.

Essas informações devem ser acessadas e devem seguir os procedimentos de cálculo de *hashes* e emissão de uma Certidão de Integridade para garantir a Cadeia de Custódia.

Cabe ressaltar que o procedimento correto seria que o próprio provedor sempre disponibilizasse as informações com o cálculo de *hashes* (vide figura a seguir). No entanto, nos casos em que estes dados chegam ao MPF sem os *hashes*, a equipe deverá fazer o cálculo e certificar a integridade dos dados, desde aquele momento.


*Figura 17: WhatsApp disponibiliza acesso aos dados já com o cálculo de hashes*

### 2.1.5 Mídias entregues no MPF

Todas as mídias entregues no MPF que sejam dispositivos de memória *flash* (*pen drive*), mídias óticas (CD/DVD/Blu-ray), fitas magnéticas ou discos rígidos, e que farão parte de um procedimento que requeira a validade da evidência, devem ser copiadas e acondicionadas seguramente no procedimento de investigação ou no local indicado pela autoridade. As análises de dados sempre devem ser feitas nas cópias dessas mídias.

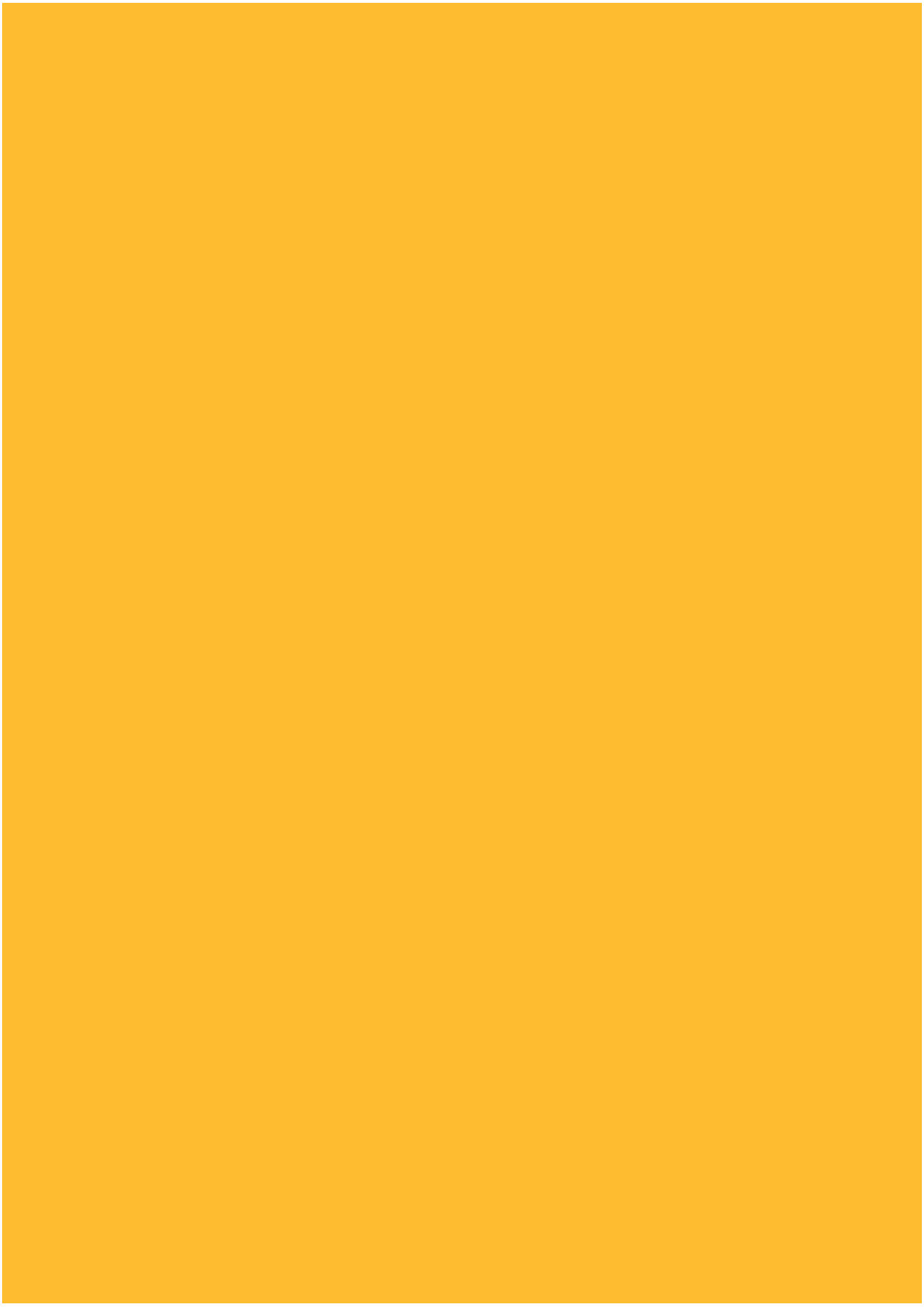
Entre os principais procedimentos de cópias de mídias, podemos citar as cópias utilizando equipamentos de duplicação forense (disponíveis na ANPTIC/Sppea), cópias utilizando um computador (Windows, Linux etc.) e cópias via interface externa. Durante os procedimentos de cópia, é indicado o uso de bloqueadores de escrita para evitar a alteração de dados.

Os mesmos procedimentos de cálculo de *hashes* para garantir a integridade de dados coletados nos outros exemplos citados neste manual devem ser seguidos nos casos de cópias de mídias.

Procedimentos relativos a cópias de mídias estão detalhados no *Manual de Procedimentos de Cópias Forenses de Mídias de Armazenamento Digital* (SPPEA/PGR, 2018) disponível em: http://intranet.mpf.mp.br/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios.

### 2.1.6 Coleta no local do crime (mandados de busca e apreensão)

Procedimentos relativos a buscas e apreensões estão detalhados no Memorando de Instrução – MI 002 – Sppea/PGR de agosto de 2017 (disponível no portal da Sppea).



# CAPÍTULO 3

# DISPONIBILIZAÇÃO DAS EVIDÊNCIAS DIGITAIS PARA O PROCEDIMENTO INVESTIGATÓRIO

Esta seção possui como objetivo apresentar aspectos básicos referentes à disponibilização das evidências digitais, com vistas a garantir a integridade e facilitar a sua utilização no procedimento investigatório, considerando as principais ferramentas utilizadas no âmbito do Ministério Público Federal.

## 3.1 Indexador e Processador de Evidências Digitais (IPED)

### 3.1.1 Principais funções da solução

O IPED é uma ferramenta forense de código aberto desenvolvida pela Polícia Federal, utilizada para processar e analisar evidências digitais. A solução, de forma nativa, prevê as seguintes funcionalidades:

a) tratamento de conteúdo em dispositivos físicos e imagens forenses em formato DD, 001, E01, vmdk, vhd, ISO e ZIP;

b) cálculo de *hashes* MD5, SHA-1, SHA-256, SHA-512 e edonkey;

c) reduplicação de arquivos conhecidos, a partir de base disponibilizada pelo Nist (*National Institute of Standards and Technology*);

d) análise de arquivos a partir das assinaturas;

e) categorização de arquivos;

f) expansão recursiva de contêiner de dezenas de formatos de arquivo;

g) criação de galeria de áudio, imagem e vídeo;

h) indicação de arquivos georreferenciados com plotagem em mapa (necessita de integração com a API Google Maps Javascript);

i) indexação dos arquivos processados, incluindo arquivos desconhecidos e espaços não alocados;

j) execução de *data carving*;

k) execução de OCR (*Optical Character Recognition*);

l) detecção de arquivos criptografados;

m) processamento a partir de perfis previamente criados;

n) execução de filtros baseados nos metadados;

o) detecção do histórico de navegação nos browsers Firefox, Chrome, Safari e Internet Explorer Edge;

p) detecção rápida de nudez;

q) interface de pesquisa intuitiva.

### 3.1.2 Diretrizes voltadas ao corpo pericial

Primeiramente, deve estar claro que a utilização do IPED está dividida basicamente em dois momentos:

a) execução do processamento da massa de dados, por parte do corpo pericial; e

b) execução da pesquisa/investigação, por parte do corpo investigativo.

Em relação à execução do processamento da massa de dados, algumas diretrizes técnicas definidas pela Assessoria Nacional de Perícia em TIC devem ser seguidas.

#### 3.1.2.1 Acesso à solução

O IPED, conforme termo de licenciamento da solução, trata-se de um software livre com redistribuição permitida sob os termos da GNU (*General Public License*) e está disponível para *download* em: https://github.com/sepinf-inc/IPED (Acesso em: 14 ago. 2020).

#### 3.1.2.2 Versão de uso

Recomenda-se ao corpo pericial a utilização da versão mais atual disponível. A figura a seguir ilustra o site GitHub, repositório mantenedor da solução:

***Figura 18:*** *Site de disponibilização da ferramenta IPED*

### 3.1.2.3 Considerações prévias ao processamento

Antes do início do processamento, convém ressaltar alguns pontos a serem observados pelo corpo pericial:

**a)** o processamento deve ser executado sobre a cópia forense da evidência. Portanto, intervenções diretas sobre o bem periciado devem ser sempre evitadas, como forma de preservar qualquer contaminação ou manuseio indevido da potencial prova, o qual pode inclusive invalidar o seu uso;

**b)** antes de iniciar o processamento, deve ser calculado o resultado da função *hash* (preferencialmente no formato SHA-256) do arquivo imagem a ser processado. Essa informação deve obrigatoriamente constar no laudo, parecer ou relatório técnico;

**c)** o *software* antivírus da estação forense deve ser configurado para excluir a pasta que mantém a solução IPED do processo de varreduras por *malware*, bem como a pasta de saída do processamento;

**d)** o arquivo "LocalConfig.txt" contém as configurações globais de processamento. Adicionalmente, o arquivo "IPEDConfig.txt" apresenta as configurações relativas a cada profile de processamento.

### 3.1.2.4 Execução do processamento

Em relação ao início do processamento, existem algumas opções de comando que podem ser encontradas no documento de apoio da ferramenta (localizado no site da PF), no entanto o comando básico a ser executado a partir da pasta do IPED via *prompt* de comando, é este:

**iped.exe -profile [nome_profile] -d [caminho_entrada] -o [caminho_saída]**

Em que:

- [nome_*profile*] = nome do *profile* pretendido. Caso não seja utilizado esse parâmetro, será utilizado por padrão o profile padrão. Portanto, a utilização desse parâmetro não é obrigatória.
- [caminho_entrada] = caminho completo da pasta ou do arquivo onde está localizado o conteúdo a ser processado.
- [caminho_saída] = caminho completo da pasta a receber os dados processados.

Após isso, será iniciado o processamento, conforme indicado na ilustração a seguir:

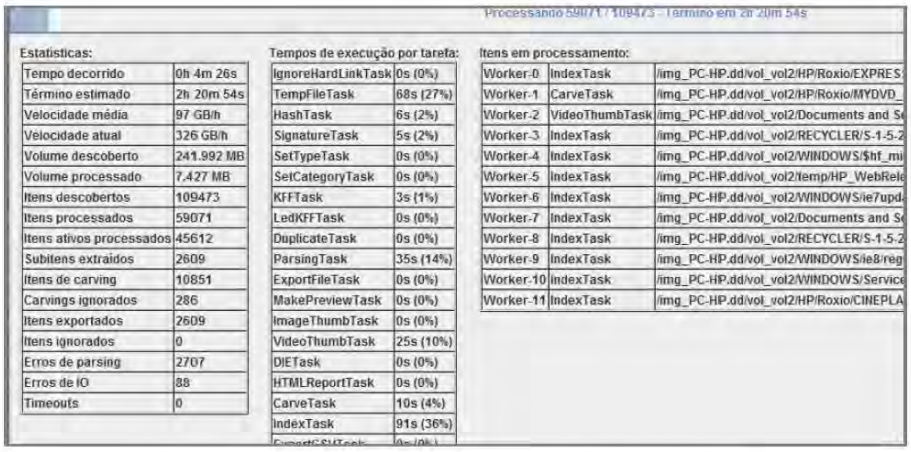



***Figura 19:*** *Ilustração do processamento na ferramenta IPED*

Após a conclusão do processamento, o corpo pericial irá se deparar com o caminho que foi definido pelo parâmetro "-o" com uma estrutura de arquivos conforme a apresentada pela figura a seguir:

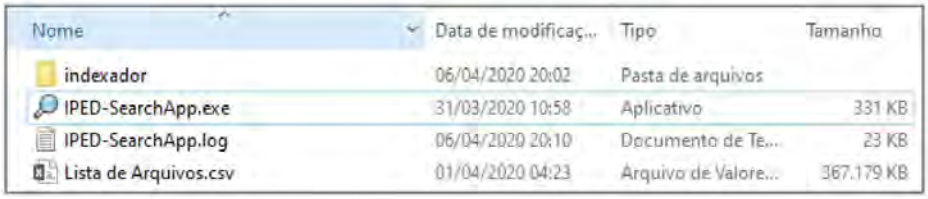



***Figura 20:*** *Estrutura de pasta pós-processamento IPED*

Cumpre destacar que deve ser calculado, com o auxílio de programa de geração de *hashes*, o resultado da função *hash* SHA-256 (ou superior) do arquivo "Lista de Arquivos.csv". Essa informação deve obrigatoriamente constar no laudo, parecer ou relatório técnico (em fonte Courier New). A tabela a seguir ilustra um esquema de apresentação dessa informação:

| Nome do arquivo | Função SHA-256 |
|---|---|
| Lista de Arquivos.csv | 40CA48BD4DB6B8D8EC965C49E7F7FA7458BE5554AFEBF0392CAD8EBB2EC98928 |

***Tabela 1:*** *Exemplo de apresentação da informação*

Após a conclusão do processamento, o corpo pericial enviará o laudo, parecer ou relatório técnico ao demandante, acompanhado da completa estrutura de arquivos, conforme figura anterior, por meio do sistema Único. Tal documento deve obrigatoriamente ser referenciado no Sistema Pericial.

Por fim, a interface de pesquisa e análise do IPED, ilustrada pela figura a seguir, deve ser acessada pelo corpo investigativo, a partir da execução do arquivo "IPED-SearchApp.exe".

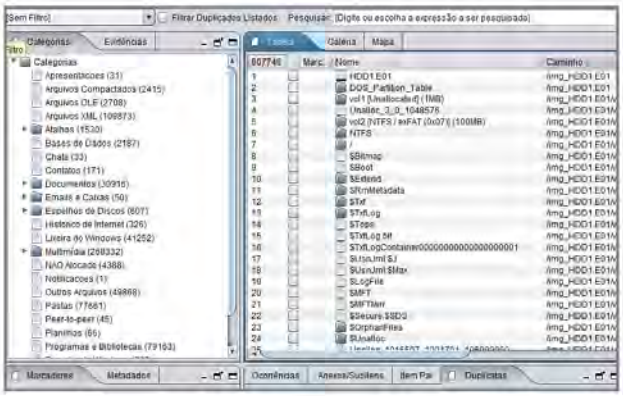


***Figura 21:*** *Interface de pesquisa do IPED*

## 3.2 Cellebrite UFED 4PC

### 3.2.1 Principais funções da solução

Essa solução realiza extrações físicas, lógicas, de sistemas de arquivos e de senhas[1] de diversos dispositivos móveis, por exemplo, em smartphones, HDs externos, *pen drives*, cartões de memória, GPS, cartões SIM e drones. Além disso, o UFED 4PC Ultimate detém as seguintes funcionalidades específicas:

a) extração de dados como registros de chamadas, agenda de contatos, mensagens de texto, imagens, vídeos, áudios, ESN, IMEI, ICCID e IMSI;

b) extração de dados ampla dos sistemas operacionais Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile e Palm OS;

c) clonagem do SIM ID; e

d) extração de dados do dispositivo móvel a partir de conexão via cabo (serial ou USB) ou Bluetooth.

Nesse contexto, acerca das modalidades de extração, o UFED 4PC Ultimate oferece as seguintes opções:

a) **Extração lógica:** apresenta-se como primeiro nível de extração e prevê a extração dos dados do usuário, por exemplo: SMS, registro de chamadas, imagens, vídeos, áudios, alguns dados de aplicações. Trata-se da extração mais rápida e com a menor quantidade de dados entre as extrações Lógica, de Sistema de Arquivos e Física;

b) **Extração do sistema de arquivos:** apresenta-se como segundo nível de extração e, em tese, prevê a captura de todos os dados da extração lógica e de alguns outros bancos de dados de aplicações, arquivos ocultos e arquivos deletados. Trata-se de uma extração de dados mais morosa que a extração lógica, no entanto, mais veloz do que a extração física;

1 O fabricante reporta que são possíveis extrações em mais de 7 mil dispositivos, sendo que esse número não abarca todos os aparelhos existentes no mercado. Além disso, nem sempre todas as extrações trazem todas as informações possíveis ou são bem-sucedidas, em função de elementos como chipsets dos dispositivos, versões dos aplicativos e do próprio sistema operacional.

c) **Extração física:** apresenta-se como a extração mais completa[2] (e mais lenta), pois é feita uma cópia bit a bit da memória *flash* do dispositivo, incluindo o espaço não alocado;

d) **Extração do cartão SIM:** trata-se da extração dos dados do cartão SIM ou USIM;

e) **Extração de senha:** vislumbra o desbloqueio e a exibição da senha de tela (*display password*) do dispositivo alvo;

f) Clonagem do SIM ID: prevê a cópia do SIM ID do cartão origem para outro cartão SIM;

g) Captura de imagens (screenshots): possibilita que o perito capture imagens ou grave um vídeo sobre o conteúdo da tela do dispositivo alvo.

O 4PC Ultimate Cellebrite é composto pelo *software* de extração, por um case com os cabos e adaptadores necessários e pelo dispositivo físico (*dongle*) de licenciamento. Recomenda-se que o *software* seja instalando sobre um computador com no mínimo a seguinte configuração:

| | |
|---|---|
| Processador | Processador I5, 2 GHz |
| Sistema operacional | Microsoft Windows 10, 64 bits ou Microsoft Windows 8.x, 64 bits |
| Memória RAM | 8 GB (Recomendado 16 GB) |
| Espaço em disco | 1,5 GB somente para a instalação |

***Tabela 2:*** *Requisitos de instalação do 4PC Ultimate Cellebrite*

2 O fabricante recomenda que, sempre que possível (o processo será mais lento), sejam realizadas extrações lógicas, sistema de arquivos e física para o mesmo aparelho, pois argumenta que algumas informações podem ser mais bem obtidas nos níveis de extração mais básicos, como o lógico. A ferramenta se encarrega de fazer a remoção dos duplicados automaticamente.

### 3.2.2 Diretrizes voltadas ao corpo pericial

Primeiramente, convém explicar o ciclo de investigação proposto pela Cellebrite. Segundo essa empresa, uma investigação contempla as etapas de identificação, coleta, exame, análise e resultados, conforme ilustrado pela figura a seguir:


***Figura 22:*** *Ciclo de investigação conforme a Cellebrite*

Nesse sentido, o Cellebrite UFED 4PC está inserido na etapa de exame, haja vista que a principal função dele é a extração de dados do dispositivo.

#### 3.2.2.1 Acesso à solução

O Cellebrite UFED 4PC, diferentemente da ferramenta IPED, não é uma solução gratuita, portanto, faz-se necessária a aquisição.

#### 3.2.2.2 Versão de uso

Sugere-se que a solução UFED 4PC Ultimate esteja em produção na versão mais recente disponibilizada pelo fabricante. Para tanto, é necessário que seja acessado o site https://community.cellebrite.com/, onde o usuário, que possui suas credenciais vinculadas à licença, poderá realizar o ***download*** das versões mais atuais dos ***softwares***, bem como dos manuais e de outros adicionais como os mapas ***off-line***:

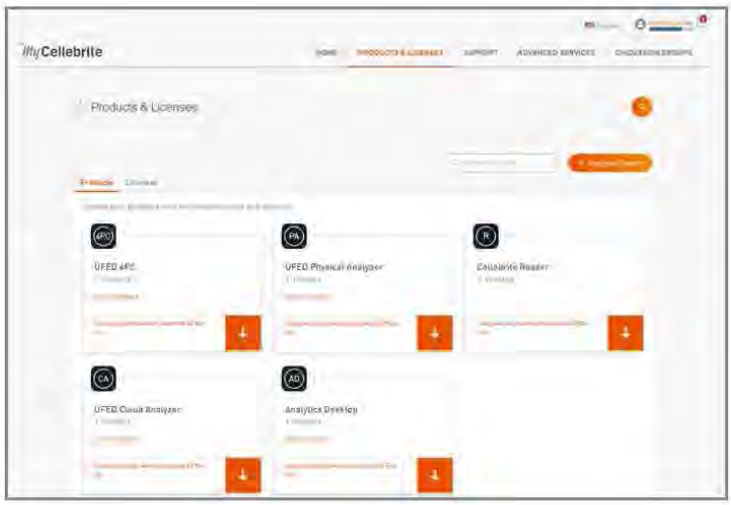



*Figura 23: Portal MyCellebrite*

### 3.2.2.3 Considerações prévias à extração

Antes do início da extração, alguns pontos devem ser observados pelo corpo pericial:

a) caso o equipamento alvo seja recebido pelo corpo pericial envolto em bolsa plástica lacrada, a bolsa deve ser rompida com cuidado e não descartada. Após a extração dos dados, ela deverá ser reaproveitada e inserida na nova bolsa plástica junto com o dispositivo;

b) o formulário de transporte deve ser atualizado ou, caso ele não exista, deve ser produzido imediatamente;

c) caso o equipamento esteja ligado, o modo avião deve ser ativado;

d) regra geral, o SIM Card deve ser removido antes do procedimento de extração, caso ainda esteja inserido no smartphone/celular;

e) a extração dos dados do SIM Card deve ser realizada em procedimento distinto à extração do smartphone/celular;

f) o equipamento deve ser identificado de forma precisa (fabricante, modelo, cor, número de série, IMEI, estado de conservação). Caso haja dúvidas, a aplicação UFED Phone Detective pode ser útil;

g) o equipamento principal e os acessórios devem ser registrados fotograficamente e essas imagens devem constar no laudo, parecer ou relatório técnico;

h) caso exista algum cartão de memória inserido no smartphone, este deve ser removido apenas para a devida identificação. Em seguida, o cartão deve ser reinserido. É recomendado que a extração de dados do cartão de memória aconteça com ele inserido no smartphone. Somente em situações muito específicas é que será necessário remover o cartão de memória original da evidência e inserir um cartão de memória vazio; e

i) a bateria do dispositivo deve ser recarregada ao máximo. Em alguns casos, a ferramenta irá informar. É necessário que o dispositivo esteja entre um intervalo específico de carga. Por isso, é muito importante sempre ler com muita atenção todas as instruções para uma correta extração.

### 3.2.2.4 Execução da extração

Em relação à execução da extração, alguns outros pontos devem ser observados pelo corpo pericial:

a) as determinações do UFED 4PC, principalmente as relativas aos ajustes no equipamento alvo e aos cabos de conexão, devem ser seguidas rigorosamente;

b) sugere-se, conforme definido pelo próprio fabricante, que a extração seja realizada nos três níveis (lógico, sistema de arquivos ou físico) ou em todos os níveis disponibilizados e possíveis pela ferramenta;

c) a versão em uso do 4PC Ultimate Cellebrite, bem como os tipos de extração executados (lógica, sistema de arquivos e/ou física) e os subtipos (Exemplos: ADB, Backup, Backup APK Downgrade, File System + Applications, Root etc.) devem ser registrados pelo corpo pericial no laudo, parecer ou relatório técnico;

d) qualquer informação relevante à extração deve ser registrada com evidências no laudo, parecer ou relatório técnico;

e) a extração deve ser destinada a uma mídia de armazenamento esterilizada (formatada em baixo nível);

f) deve-se certificar que o *hash* da extração foi gerado e está armazenado no arquivo destino, no caso das extrações físicas;

g) para as extrações lógica e de sistemas de arquivos, ou ainda, no caso de não ter sido gerado o *hash* na extração física, deverá ser calculado o *hash* SHA-256 dos arquivos gerados pela extração;

h) após a conclusão da extração, convém que o dispositivo seja envolto em plástico bolha para sua proteção; e

i) o dispositivo móvel deve ser armazenado em nova bolsa plástica identificável.

## 3.3 Cellebrite Physical Analyzer

### 3.3.1 Principais funções da solução

Essa ferramenta fornece uma visão amigável e detalhada da memória *flash* e RAM do dispositivo alvo, mediante a adequada decodificação dos dados previamente extraídos. Além disso, o Cellebrite Physical Analyzer detém as seguintes funcionalidades específicas:

a) decodificação de diversos formatos de arquivos, tais como: *.ufdx, *.ufd, *.ufdr, *.bin, *.pm, *.ipd, *.bbb, *.gdfs, *.cfg, *.xml, *.e01, *.zip;

b) reconstrução do sistema de arquivos do dispositivo;

c) recodificação de vários tipos de dados extraídos, tais como: lista de contatos, mensagens SMS, registros de chamadas, informações do dispositivo (IMEI, IMSI, ICCID, MSISDN), informações de aplicações, marcações de localização (GPS, Wi-Fi e rede móvel) etc.

d) leitura de arquivos ocultos, deletados e espaços não alocados;

e) visualização e acesso a arquivos de dados de usuário, tais como: imagens, vídeos, áudios, bases de dados etc.;

f) apresentação de interface de pesquisas por diversos parâmetros, inclusive mediante expressões regulares;

g) construção de linha do tempo;

h) detecção de *malware* no dispositivo; e

i) confecção de relatórios em diversos formatos, tais como: PDF, HTML, Excel, Word, XML e UFDR (formato proprietário Cellebrite).

O Cellebrite Physical Analyzer é composto pelo *software* e pelo dispositivo físico (dongle) de licenciamento. Recomenda-se que o *software* seja instalado sobre um computador com, no mínimo, a seguinte configuração:

| | |
|---|---|
| Processador | Compatível com Windows, processador I5, 2 GHz |
| Sistema operacional | Microsoft Windows 10, 64 bits ou Microsoft Windows 8.x, 64 bits |
| Memória RAM | 16 GB |
| Espaço em disco | 100 GB para instalação e manutenção das bases de dados<br>Disco SSD (recomendado) |
| Adicional | Microsoft .Net versão 4.6.2<br>Windows Media Player |

***Tabela 3:*** *Requisitos de instalação do Physical Analyser Cellebrite*

### 3.3.2 Diretrizes voltadas ao corpo pericial

Considerando o ciclo de investigação proposto pela empresa, o Cellebrite Physical Analyzer também está preponderantemente inserido na fase de exame. Dessa forma, é importante que o corpo pericial esteja atento às diretrizes de manuseio de evidências, conforme definidas pela ANPTIC/Sppea.

#### 3.3.2.1 Acesso à solução

O Cellebrite Physical Analyzer, assim como o Cellebrite UFED 4PC, não é uma solução gratuita, portanto, também se faz necessária a aquisição.

#### 3.3.2.2 Versão de uso

Sugere-se que a solução Cellebrite Physical Analyzer esteja na versão mais recente disponibilizada pelo fabricante. Do mesmo modo que UFED 4PC, é necessário que seja acessado o site https://community.cellebrite.com/ pelo detentor da licença, para o download da versão mais atual.

#### 3.3.2.3 Execução da decodificação

Em relação à execução da decodificação e a geração dos relatórios, alguns pontos devem ser observados pelo corpo pericial:

a) Após a decodificação, deve-se utilizar a opção de "desduplicação". Ela removerá dados redundantes entre as extrações lógica, de sistema de arquivos e física, quando mais de uma extração for realizada.

**b)** Em relação à preparação e produção dos relatórios, os seguintes pontos devem ser seguidos:

- Deve ser gerado relatório no formato UFDR (para utilização com o Cellebrite Reader[3] ou o Cellebrite Pathfinder) e, se for o caso, também no formato HTML, PDF ou algum outro solicitado.

- Quando solicitado, o campo "Nome do examinador" deve ser preenchido com o nome completo do perito; o campo "Número do caso" deve ser preenchido com o número de registro da demanda no Sistema Pericial, por exemplo, SPPEA 1000/2020; o campo "Organização" deve ser preenchido com "Ministério Público Federal" e o campo "Investigador" deve ser preenchido com o nome do membro que realizou o pedido no Sistema Pericial.

- Ainda durante a preparação dos relatórios, na seção "Report Dataset/Preferences", a opção "Calculate SHA-2 (256 bit) *hash*" e "Include Cellebrite Reader" devem ser selecionadas.

- Na fase final de preparação de geração do relatório, o campo "Cabeçalho do logotipo" deverá ser preenchido como ilustrado na figura a seguir:

Ministério Público Federal
Procuradoria Geral da República
Secretaria de Perícia, Pesquisa e Análise
Centro Nacional de Perícia

Fonte: Arial
Tamanho da fonte: decrescente, a partir da primeira linha
Alinhamento: Centralizado

***Figura 24:*** *Ilustração do cabeçalho do relatório a ser gerado via Physical Analyzer*

- No campo "Logotipo", selecione o arquivo de imagem indicado a seguir:

**MPF**
**Ministério Público Federal**

***Figura 25:*** *Logotipo a ser utilizado no relatório a ser gerado via Physical Analyzer*

3 O Cellebrite Reader é um *software* gratuito e que pode ser instalado em quaisquer equipamentos, sem a necessidade de aquisição. Ele possui funcionalidades básicas de pesquisa, que podem auxiliar em uma investigação.

- No campo "Rodapé do logotipo", preencha com as mesmas informações do campo "Cabeçalho do logotipo".

c) Após a geração do relatório, devem ser calculados os resultados da função *hash* SHA-256 dos relatórios. Essas informações devem obrigatoriamente constar no laudo, parecer ou relatório técnico (em fonte Courier New, tamanho 9). A tabela a seguir ilustra um esquema de apresentação dessa informação:

| Nome do arquivo | Função SHA-256 |
|---|---|
| Relatorio_Cellebrite.UFDR | 85CA48BD4DB6B8D8EC965C55E7F7FA7458BE5554AFEBF0392CAD8EBB2EC98928 |
| Relatorio_Cellebrite.PDF | 36CA48BD4DB6B8D8EC965C88E7F7FA7458BE5554AFEBF0392CAD8EBB2EC98928 |

***Tabela 4:*** *Exemplo de apresentação da informação*

d) Para o relatório no formato .HTML e visando facilitar a transmissão, pode-se fazer uso de compactação de todos os arquivos e pastas referentes ao relatório em questão, em que o arquivo compactado deve ser criptografado com senha no padrão AES (preferencialmente usando o programa 7-Zip) e no mínimo 18 caracteres, sendo o *hash* SHA-256 desse arquivo compactado também calculado e registrado no produto pericial.

e) A interface de pesquisa deve ser acessada pelo corpo investigativo a partir da execução do arquivo, recém-gerado, "Reader.exe".

## 3.4 Ferramentas para cálculo da função *hash*

Primeiramente, as indicações desta seção acontecem com base nas funcionalidades das ferramentas, facilidade de uso e termos de licenciamento, mas não limitam a utilização de outras, as quais devem constar na lista de softwares homologados da Sppea.

Assim, a título exemplificativo, são apresentadas como opções para o corpo pericial, (para as atividades relacionadas ao cálculo de função *hash*) as seguintes ferramentas: **SlavaSoft HashCalc, SlavaSoft FSUM e RHash.**

### 5.4.1 Principais funções das soluções

Essas ferramentas permitem agilizar o cálculo da função *hash* a partir de arquivos, *strings* de textos e *strings* hexadecimais, mediante a utilização dos padrões de algoritmos entre os mais comuns. Atualmente o padrão recomendado pela Sppea é o SHA-256. As figuras a seguir ilustram as funcionalidades específicas de cada uma das três ferramentas mencionadas:

Major Features:

- Support of 12 well-known and documented hash and checksum algorithms: **MD2, MD4, MD5, SHA-1, SHA-2( 256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, CRC32.**
- Support of a custom hash algorithm (**MD4**-based) used in **eDonkey** and **eMule** applications.
- Support of 2 modes of calculations: **HASH/CHECKSUM** and **HMAC.**
- Support of 3 input data formats: **files, text strings** and **hex strings.**
- Work with large size files. (Tested on file sizes up to 15 GB).
- Drag-and-drop support.
- Quick and simple installation.
- Calculates hash/checksum and HMAC for files of any type: music, audio, sound, video, image, icon, text, compression, etc., with the extensions: .mp3, .wav, .avi, .mpg, .midi, .mov, .dvd, .ram, .zip, .rar, .ico, .gif, .pif, .pic, .tif, .tiff, .txt, .doc, .pdf, .wps, .dat, .dll, .hex, .bin, .iso, .cpp, .dss, .par, .pps, .cue, .ram, .md5, .sfv, etc.

*Figura 26: Funcionalidades da ferramenta SlavaSoft HashCalc*

Major Features:

- Possibility to calculate a file message digest and/or a checksum using any of the 12 well-known and documented hash and checksum algorithms: **MD2, MD4, MD5, SHA-1, SHA-2( 256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, CRC32;**
- Support of a custom hash algorithm (MD4-based) used in **eDonkey** and **eMule** applications.
- Possibility to act recursively. FSUM can operate not only on files from a specific directory, but also on files from all subdirectories of the specified directory;
- Work with large size files. (Tested on file sizes of up to 15 GB);
- Full compatibility with md5sum utility;
- Full .MD5 and .SFV file formats support;
- Automatic recognition of checksum file format (.MD5 or .SFV) while checking;
- Generates/verifies hashes/checksums for files of any type: music, audio, sound, video, image, icon, text, compression, etc., with the extensions: .mp3, .wav, .avi, .mpg, .midi, .mov, .dvd, .ram, .zip, .rar, .ico, .gif, .pif, .pic, .tif, .tiff, .txt, .doc, .pdf, .wps, .dat, .dll, .hex, .bin, .iso, .cpp, .dss, .par, .pps, .cue, .ram, .md5, .sfv, etc.

*Figura 27: Funcionalidades da ferramenta SlavaSoft FSUM*

**RHash** (*Recursive Hasher*) is a console utility for computing and verifying hash sums of files. It supports CRC32, MD4, MD5, SHA1, SHA256, SHA512, Tiger, DC++ TTH, BitTorrent BTIH, ED2K, AICH, GOST R 34.11-94, RIPEMD-160, HAS-160, EDON-R 256/512, Whirlpool and Snefru-128/256 algorithms. Hash sums are used to ensure and verify integrity of large volumes of data for a long-term storing or transferring.

Features:

- Can calculate Magnet links.
- Output in a predefined (SFV, BSD-like) or user defined format.
- Ability to process directories recursively.
- Updating of existing hash files (adding sums of files missing in the hash file)
- Calculates several hash sums in one pass.
- Portability: the program works the same under Linux, *BSD, or Windows.

*Figura 28: Funcionalidades da ferramenta RHash*

### 3.4.2 Diretrizes voltadas ao corpo pericial

#### 3.4.2.1 Acesso às soluções

As ferramentas mencionadas para cálculos de *hash* podem ser obtidas a partir dos seguintes endereços:

a) SlavaSoft HashCal: https://www.slavasoft.com/hashcalc/

b) SlavaSoft FSUM: https://www.slavasoft.com/fsum/

c) RHash: http://rhash.sourceforge.net/

#### 3.4.2.2 Versão de uso

Sugere-se que as soluções em produção estejam nas versões mais recentes disponibilizadas pelos fabricantes.

#### 3.4.2.3 Cálculos de *hash*

Acerca dos procedimentos para cálculo das funções *hash*, o corpo pericial deve observar as seguintes determinações:

a) as mídias de armazenamento computacional ou os arquivos oriundos de quebras telemáticas periciados **devem ser submetidos a duas funções unidirecionais de resumo (*hash*)** visando a futuras verificações de integridade dos dados:

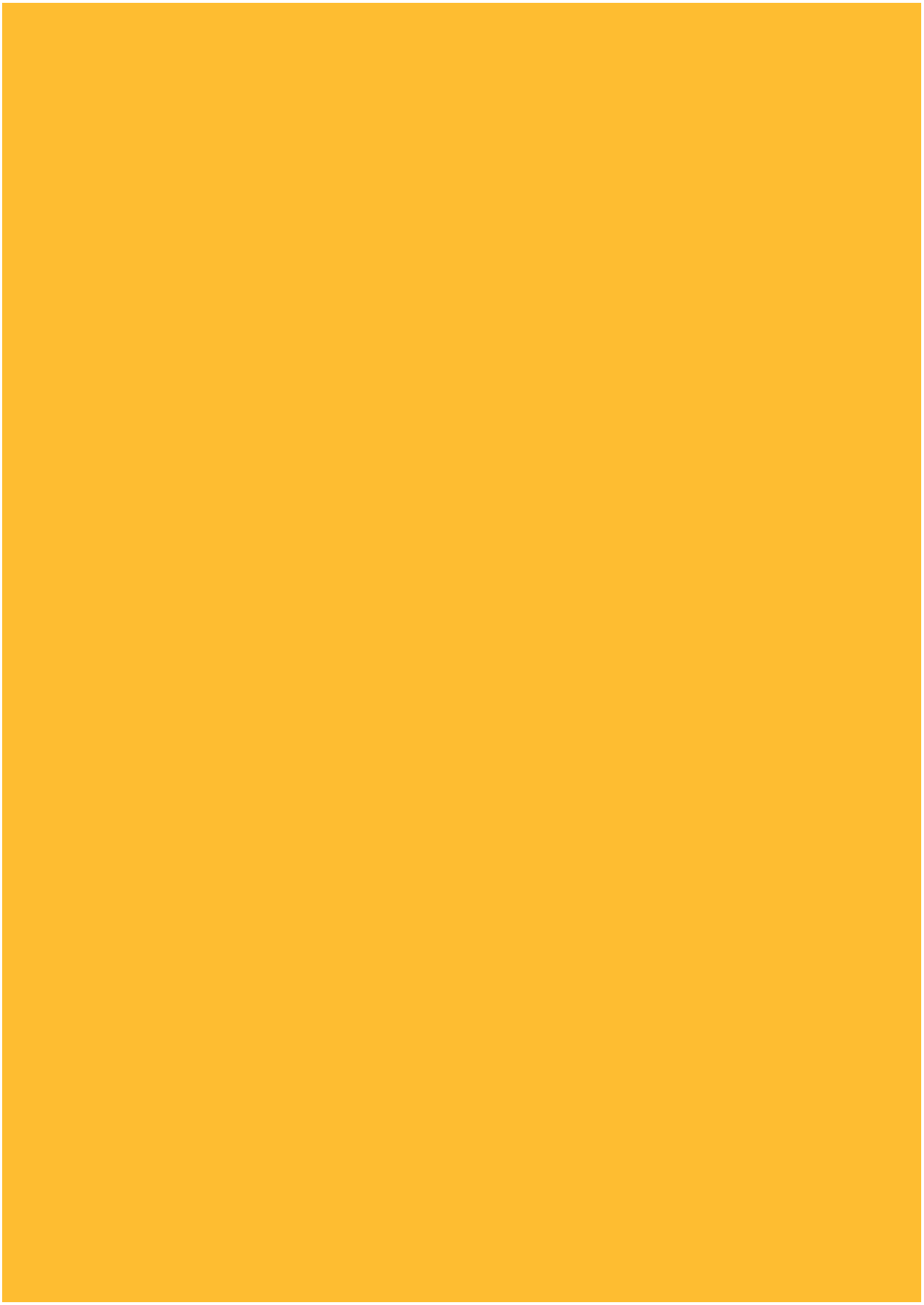
- Em primeiro lugar, deve ser calculado um único valor sobre o conteúdo integral (imagem da mídia ou da imagem dos dados telemáticos), utilizando-se o algoritmo SHA-256. Esse procedimento tem por objetivo possibilitar a verificação de integridade preliminar e afastar a possibilidade de argumentações de colisões. Nos casos de impossibilidades, devem ser calculados os *hashes* de cada um dos fragmentos do arquivo-imagem.

- Na sequência, deve ser calculado o valor da função *hash* SHA-1 ou MD5 sobre cada um dos arquivos identificados na mídia ou nos dados telemáticos. Esse procedimento tem por finalidade possibilitar a verificação detalhada do conteúdo e garantir a integridade parcial em caso de falha no cálculo do *hash* integral.

b) em relação às mídias óticas (CDs e DVDs) não deve ser feito o cálculo de *hash* descrito anteriormente. Devido a certas particularidades desse tipo de mídia, o *hash* calculado pode variar mesmo que o conteúdo da mídia não tenha sido alterado. Dessa forma, se possível, calcule a função *hash* SHA-256 para cada arquivo identificado. Caso seja inviável, calcule ao menos o valor da função *hash* SHA-1 ou MD5 para cada arquivo;

c) caso a mídia original apresente erro de leitura, o arquivo de *log*, listando os setores defeituosos também deverá ser incluído na mídia anexa ao documento científico;

d) sobre o cálculo de *hash* dos relatórios gerados pelas soluções IPED e Cellebrite, devem ser seguidas as determinações já expostas nas seções anteriores deste capítulo.



# CAPÍTULO 4

## CADEIA DE CUSTÓDIA DOS DADOS NO ÂMBITO DA LEGISLAÇÃO VIGENTE

Este capítulo aborda, sinteticamente, no âmbito do ordenamento jurídico pátrio, a inserção dos procedimentos que cuidam da preservação da Cadeia de Custódia, especialmente no que tange às evidências digitais.

Com a promulgação e publicação da Lei nº 13.964/2019 (denominada "Pacote Anticrime"), foram incluídos no Código de Processo Penal (CPP) os arts. 158-A e 158-F, que tratam das disposições relativas à perícia e à Cadeia de Custódia no contexto da prova pericial. Os referidos dispositivos[4], apesar de não inovarem na preocupação com a preservação dos vestígios, trouxeram um "aprimoramento dos procedimentos de preservação das evidências atreladas a um delito, fortalecendo a natureza científica e técnica do sistema probatório"[5].

Nessa perspectiva, o legislador, no art. 158-A do CPP, conceitua a Cadeia de Custódia esclarecendo que:

> [se] considera Cadeia de Custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Ainda no art. 158-A, esclarece-se o conceito de vestígio, que é "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal".

Cadeia de Custódia, portanto, é um mecanismo que visa assegurar que determinado vestígio não sofreu adulteração pelas autoridades, atestando a identificação de quem o manuseou e das ocasiões em que isso ocorreu.

A Cadeia de Custódia, por exemplo, garante que a moeda falsa apreendida durante uma prisão em flagrante é a mesma que foi periciada e é a mesma que está juntada aos autos, ou, ainda, que determinada prova digital foi extraída exatamente do computador do acusado.

4 A necessidade de preservação dos vestígios já era descrita em outros dispositivos do Código de Processo Penal, como nos arts. 6º e 170.

5 SANCHES (fl. 174 – seg. parágrafo)

Para melhor compreensão, transcrevemos os dispositivos do CPP referentes à Cadeia de Custódia:

> Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.
>
> § 1º O início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio.
>
> § 2º O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação.
>
> § 3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal.
>
> Art. 158-B. A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas:
>
> I – reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
>
> II – isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
>
> III – fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;
>
> IV – coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;
>
> V – acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;
>
> VI – transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII – recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII – processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX – armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X – descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Art. 158-C. A coleta dos vestígios deverá ser realizada preferencialmente por perito oficial, que dará o encaminhamento necessário para a central de custódia, mesmo quando for necessária a realização de exames complementares.

§ 1º Todos os vestígios coletados no decurso do inquérito ou processo devem ser tratados como descrito nesta Lei, ficando órgão central de perícia oficial de natureza criminal responsável por detalhar a forma do seu cumprimento.

§ 2º É proibida a entrada em locais isolados bem como a remoção de quaisquer vestígios de locais de crime antes da liberação por parte do perito responsável, sendo tipificada como fraude processual a sua realização.

Art. 158-D. O recipiente para acondicionamento do vestígio será determinado pela natureza do material.

§ 1º Todos os recipientes deverão ser selados com lacres, com numeração individualizada, de forma a garantir a inviolabilidade e a idoneidade do vestígio durante o transporte.

§ 2º O recipiente deverá individualizar o vestígio, preservar suas caracteristicas, impedir contaminação e vazamento, ter grau de resistência adequado e espaço para registro de informações sobre seu conteúdo.

§ 3º O recipiente só poderá ser aberto pelo perito que vai proceder à análise e, motivadamente, por pessoa autorizada.

§ 4º Após cada rompimento de lacre, deve se fazer constar na ficha de acompanhamento de vestígio o nome e a matrícula do responsável, a data, o local, a finalidade, bem como as informações referentes ao novo lacre utilizado.

§ 5º O lacre rompido deverá ser acondicionado no interior do novo recipiente.

Art. 158-E. Todos os Institutos de Criminalística deverão ter uma central de custódia destinada à guarda e controle dos vestígios, e sua gestão deve ser vinculada diretamente ao órgão central de perícia oficial de natureza criminal.

§ 1º Toda central de custódia deve possuir os serviços de protocolo, com local para conferência, recepção, devolução de materiais e documentos, possibilitando a seleção, a classificação e a distribuição de materiais, devendo ser um espaço seguro e apresentar condições ambientais que não interfiram nas características do vestígio.

§ 2º Na central de custódia, a entrada e a saída de vestígio deverão ser protocoladas, consignando-se informações sobre a ocorrência no inquérito que a eles se relacionam.

§ 3º Todas as pessoas que tiverem acesso ao vestígio armazenado deverão ser identificadas e deverão ser registradas a data e a hora do acesso.

§ 4º Por ocasião da tramitação do vestígio armazenado, todas as ações deverão ser registradas, consignando-se a identificação do responsável pela tramitação, a destinação, a data e horário da ação.

Art. 158-F. Após a realização da perícia, o material deverá ser devolvido à central de custódia, devendo nela permanecer.

Parágrafo único. Caso a central de custódia não possua espaço ou condições de armazenar determinado material, deverá a autoridade policial ou judiciária determinar as condições de depósito do referido material em local diverso, mediante requerimento do diretor do órgão central de perícia oficial de natureza criminal.

Os procedimentos abordados nos capítulos anteriores referem-se às principais etapas da Cadeia de Custódia descritas no CPP, especialmente à identificação, ao isolamento, à coleta e à preservação, bem como ao exame e ao Laudo Pericial.

As técnicas adotadas para a preservação da Cadeia de Custódia ocorrem em pedidos de busca e apreensão, em evidências digitais armazenadas em meio físico (discos rígidos, celulares, computadores etc.), bem como por meio de quebras de sigilo telemático, quando se tratar de armazenamentos não físicos (como mensageiros eletrônicos, arquivos em nuvem etc.).

Na identificação e no isolamento do vestígio digital em meio não físico (como em registros de conexão e de acesso a aplicações), a Lei nº 12.965/2014 (Marco Civil da Internet) autoriza o Ministério Público a requerer, cautelarmente, a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet e de conexão sejam guardados para que, posteriormente, mediante ordem judicial, possam ser disponibilizados. A forma e o pedido de preservação são detalhados no capítulo 2 deste manual.

É válido lembrar que, a depender do dado a ser requerido, não é necessária ordem judicial, especialmente quando se tratar de dados cadastrais (art. 10, § 3º, da Lei nº 12.965/2014).

Ainda em relação à Cadeia de Custódia, no tocante à sua preservação e às etapas posteriores, destacam-se as consequências da quebra da Cadeia de Custódia. A divergência se situa nos efeitos gerados pela quebra da Cadeia de Custódia.

Em que pesem posições em sentido contrário, o melhor entendimento parece ser aquele que considera que, mesmo havendo mácula à Cadeia de Custódia, a prova continua legítima e lícita, mas sua autenticidade e integridade poderá ser questionada. Caberá ao juiz a valoração dessa prova conforme a maior ou menor violação às regras da Cadeia de Custódia. A exclusão da prova só ocorrerá em hipóteses extremas, em que a violação às regras da Cadeia de Custódia impedir o contraditório e a ampla defesa.

De todo modo, a violação às regras da Cadeia de Custódia não torna a prova ilícita, já que não existem vícios instrumentais na sua obtenção. O que ocorre é uma mácula à sua custódia, que interfere na sua qualidade e que deve ser valorada pelo juiz conforme o caso concreto, podendo ocorrer a sua imprestabilidade em determinadas situações.

No âmbito da jurisprudência, podemos citar o Agravo Regimental no Recurso Especial nº 1.587.239/RS, em que o Superior Tribunal de Justiça (STJ) enfrentou situação semelhante.

Na ocasião, a 6ª Turma do STJ analisou o acesso direto à mídia apreendida antes da realização do espelhamento do material. A relatora, ministra Maria Thereza, concluiu que não havia:

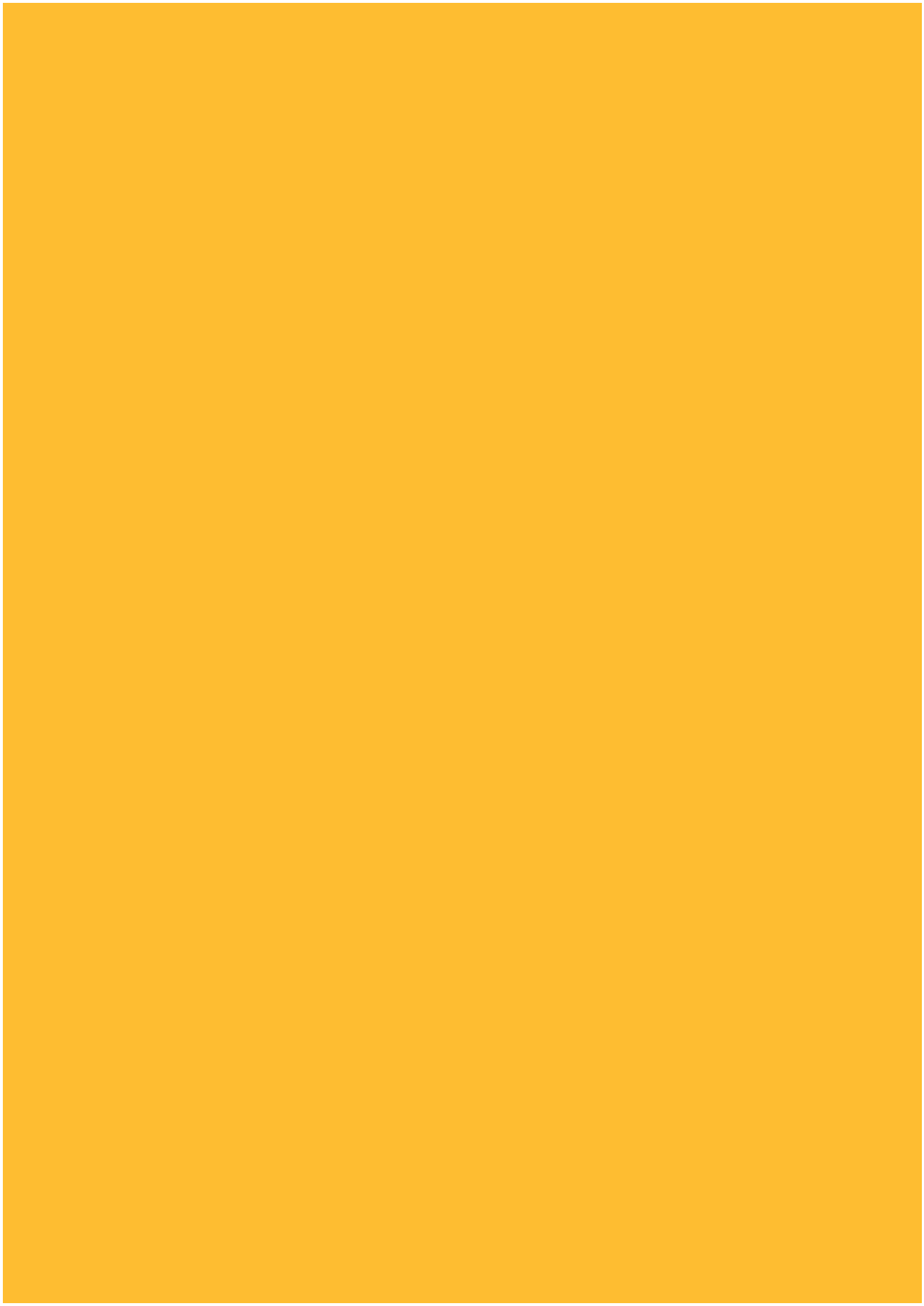
> elementos nos autos que autorizem a conclusão de que houve montagem de dados ou que a autoridade policial tenha apagado base de dados e, conquanto as partes tenham tido acesso ao espelhamento da mídia apreendida, não houve demonstração da existência de adulteração da prova ou de efetivo prejuízo ao exercício da defesa.

Desse modo, concluiu que:

> o acesso direto ao disco rígido pela Polícia não resultou em qualquer alteração de tudo o que já havia sido verificado e decidido acerca do assunto de modo que, ainda que tenha havido falhas na preservação do material apreendido, tais falhas não são suficientes para determinar a exclusão da prova porque não conduzem à sua ilicitude, ressaltando, acertadamente, que o espelhamento e o cálculo do algoritmo SHA-512 são providências de perpetuação da prova, destinadas a atestar, com a maior confiabilidade possível, a idoneidade da prova, mas não há determinação legal de que as mídias de informática não sejam acessadas diretamente.

Em sentido análogo, veja-se o REsp 1435421/RS, relatora Maria Thereza de Assis Moura, Sexta Turma, julgado em 16/6/2015, DJe 25/6/2015.

Diante disso, a conclusão é de que a quebra da Cadeia de Custódia pode levar ao enfraquecimento da evidência digital, de modo que a observância dos trâmites descritos neste manual é de fundamental importância para utilização da prova no processo judicial.



# CAPÍTULO 5

# FORMULÁRIOS DE CADEIA DE CUSTÓDIA, RELATÓRIOS TÉCNICOS E LAUDOS PERICIAIS

## 5.1 Introdução

Em geral, os membros do Ministério Público Federal (MPF) necessitam de suporte especializado em computação forense quando nos procedimentos investigatórios ou judiciais é necessário tratamento e exame de vestígios digitais. Esse suporte é prestado por peritos ou assistentes técnicos que exprimem suas opiniões por meio de duas espécies de documentos técnicos, a saber: I) Laudo Pericial; ou II) Parecer Técnico.

Para o registro completo da história cronológica do vestígio, além dos documentos citados e das certidões elencadas no capítulo 2, a Cadeia de Custódia exige a produção de outros documentos técnicos, a saber: I) Formulário de Transporte de Vestígio; II) Formulário de Recebimento de Vestígio; III) Formulário de Acompanhamento do Vestígio; e IV) Formulário de Descarte de Vestígio. O conjunto dos documentos processuais técnicos da Cadeia de Custódia possui o esboço a seguir.

## 5.2 Documentos Processuais Técnicos da Cadeia de Custódia

I. **Documentos Técnicos de Opinião:**

   a) Laudo Pericial; e
   b) Parecer Técnico.

II. **Documentos Técnicos de Registro:**

   a) Formulário de Transporte de Vestígio;
   b) Formulário de Recebimento de Vestígio;
   c) Formulário de Acompanhamento do Vestígio; e
   d) Formulário de Descarte de Vestígio.

A Secretaria de Perícia, Pesquisa e Análise disponibiliza para download os modelos dos documentos técnicos por meio do endereço eletrônico: https://portal.mpf.mp.br/intranet/intranet_mpf/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise.

## 5.3 Modelos de Documentos Processuais Técnicos da Cadeia de Custódia

Os documentos processuais técnicos da Cadeia de Custódia podem seguir os modelos apresentados neste capítulo. Alguns elementos constitutivos são comuns em todos os documentos, a saber: capa (*layout* padrão), cabeçalho e rodapé, formatação, tabelas, quadros, ilustrações (figuras, gráficos, fotografias, entre outras) e anexos.

### 5.3.1 Capa

A capa deve apresentar informações básicas sobre o documento técnico, tais como: tipo do documento, número do documento, referência (número do procedimento no sistema Único e número da guia no Sistema Pericial), unidade solicitante, autoridade requerente e ementa.


***Figura 29:*** *Capa padrão*

### 5.3.2 Cabeçalho e rodapé

O cabeçalho e o rodapé possuem informações de identificação complementares que apresentam a unidade e o órgão de produção do documento técnico, além do número do documento no sistema Único.


*Figura 30: Cabeçalho padrão*


*Figura 31: Rodapé padrão*

### 5.3.3 Formatação

O uso de fonte em tamanho adequado proporciona leitura confortável, o que não seria possível com fontes pequenas ou com tamanhos variados ao longo do texto. Além disso, mantém o padrão estético para documentos técnicos da mesma espécie.

Deve-se observar a seguinte formatação para o corpo do texto: I) fonte *Times New Roman*, tamanho 12; II) espaçamento entrelinhas de 1,5; III) margem esquerda 3 cm, margem direita 2 cm, margens superior e inferior 2 cm; IV) recuo de 1 linha do parágrafo 2,5 cm; e V) espaçamento entre parágrafos de 0,0 cm acima e 0,2 cm abaixo.

### 5.3.4 Tabelas, quadros e ilustrações

As tabelas, quadros e ilustrações (gráficos, figuras, imagens, fotografias, entre outras) constituem importante recurso para apresentação de informações e conferem mais clareza ao documento técnico.

As tabelas, quadros e ilustrações estarão próximos ao texto a que se referem. As fotografias devem ser nítidas e, se possível, demonstrar as descrições presentes no vestígio. Veja o exemplo da tabela com descrição e fotografia de um vestígio:

| VESTÍGIO<br>dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| **Número do item:** Item 1 do Termo de Apreensão XX/XXXX | **Descrição do item:** Disco rígido com capacidade de armazenamento de 1 TB (Terabytes). | |
| **Fabricante:** SEAGATE | **Modelo:**<br>BarraCuda | **Número de série:**<br>ST1000DM010 |
| **Data e hora da coleta:** Dia XX/XX/XXX, horas XX:XX | **Local da coleta:** Brasília | **Nome de quem coletou:** Agente de Polícia XXXXXXXXX |

***Tabela 5:*** *Descrição de um vestígio*

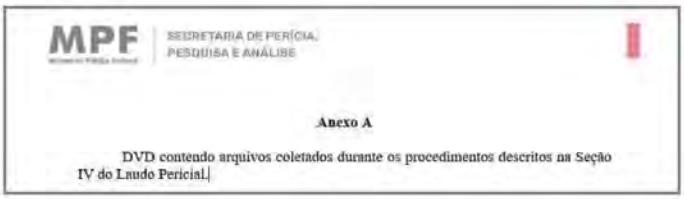

***Fotografia 1:*** *Disco Rígido (vestígio), descrição constante da Tabela 5*

### 5.3.5 Anexos

Os anexos são constituídos por documentos, imagens, CDs, DVDs, *pen drive*, entre outros materiais, e servem para complementar ou comprovar informações apresentadas no documento técnico. De um modo geral, os anexos são utilizados para encaminhar elementos de prova coletados nos exames periciais, a saber: I) planilhas; II) imagens; III) logs de acesso; IV) programas maliciosos; entre outros elementos de prova.

Os anexos eletrônicos devem garantir, quanto aos elementos apresentados como prova: I) a confidencialidade (com uso de criptografia); II) a integridade (cálculo de *hash* para cada arquivo eletrônico contido no CD, DVD, *pen drive* etc.) e a autenticidade (obtida por meio da assinatura digital do arquivo que contém a lista de hash).

Os anexos devem receber identificação única para permitir a referência inequívoca no corpo do documento técnico, por exemplo: I) Anexo A; II) Anexo I; e III) Anexo A1. Veja a figura a seguir:


MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

**Anexo A**

DVD contendo arquivos coletados durante os procedimentos descritos na Seção IV do Laudo Pericial.

*Figura 32: Modelo de Anexo*

## 5.4 Documentos Técnicos de Opinião

### 5.4.1 O Laudo Pericial e Parecer Técnico

O Laudo Pericial e o Parecer Técnico em computação forense são documentos processuais técnicos de opinião. Compõem a Cadeia de Custódia e respondem aos quesitos e/ou concluem algo, ou seja, expressam uma opinião técnica na área de tecnologia da informação e comunicação. Devem conter, entre outras informações: I) histórico; II) descrição do material examinado; III) objetivos; IV) exames; V) respostas aos quesitos/conclusões; e VI) quaisquer outros anexos que auxiliem na comprovação ou facilitem o entendimento do documento técnico.

Este manual aborda as seções do Laudo Pericial ou Parecer Técnico consideradas relevantes para demonstrar a Cadeia de Custódia do vestígio. Não trata de como realizar a descrição de uma metodologia científica adotada na perícia ou de como descrever os exames periciais realizados em determinada perícia.

### 5.4.2 Estrutura comum do Laudo Pericial e do Parecer Técnico

O Laudo Pericial e o Parecer Técnico podem apresentar as seguintes seções:

**Histórico:** I) reconhecimento e isolamento; II) fixação e coleta; III) acondicionamento e transporte; e IV) recebimento.

**Material:** listagem e descrição dos vestígios que serão examinados.

**Objetivos:** I) objetivos gerais da perícia; II) objetivos específicos: lista de quesitos que serão respondidos.

**Exames:** descrição dos métodos científicos adotados e dos exames realizados;

**Conclusões e respostas aos quesitos:** I) lista de todos os quesitos; II) resposta aos quesitos; e III) conclusões (geralmente no Parecer Técnico).

A diferença comum entre o Laudo Pericial e o Parecer Técnico, em termos de estrutura, é o fato de o Parecer Técnico apresentar uma opinião conclusiva, mas não responder a quesitos.

### 5.4.3 Histórico

O Histórico deve demonstrar o caminho percorrido pelo vestígio até chegar ao momento do exame pericial. Para tanto, deve descrever as etapas de reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte e recebimento.

a) **Reconhecimento e isolamento:** descrição dos procedimentos realizados para distinção de um elemento como de potencial interesse para a produção da prova pericial, bem como os procedimentos adotados para evitar a alteração do estado das coisas no local de coleta do vestígio. Veja o exemplo a seguir:

**I.HISTÓRICO**

**1.1.Do reconhecimento e isolamento (art. 158-B, I e II, do CPP)**

Aos *DIA* dias do mês de *MÊS* do ano de dois mil e vinte, foi realizada busca e apreensão na residência do senhor(a) *RÉU*, no *ENDEREÇO*, em cumprimento da *DECISÃO*. Durante os procedimentos o senhor *AGENTE* identificou o disco rígido como vestígio de potencial interesse para a produção de prova pericial. Foram adotadas todas as medidas adequadas para o isolamento do local da busca e apreensão.

*Figura 33: Exemplo de texto dos procedimentos para reconhecimento e isolamento*

b) **Fixação e coleta:** descrição dos procedimentos realizados para coleta do vestígio e descrição detalhada do vestígio coletado. Importante ressaltar que é indispensável a descrição do vestígio no Laudo Pericial, conforme estabelece o art. 158-B, inciso III, do Código de Processo Penal. Veja exemplo do texto:

**1.2.Da fixação e coleta (art. 158-B, III e IV, do CPP)**

Após o reconhecimento, os agentes relatam que o vestígio, disco rígido, estava guardado em um armário localizado no quarto do réu. O senhor *AGENTE* realizou a coleta do vestígio, adotando as medidas de segurança necessárias à preservação das características e integridade do vestígio. Em seguida, realizaram a descrição detalhada do vestígio no *TERMO DE APREENSÃO*, a saber:

**Tabela 1**: descrição do item apreendido.

| **Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros)** | | |
|---|---|---|
| Número do item: **(Identificação única para o item no termo de apreensão)** | Descrição do item: **(Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras)** | |
| Fabricante: **(Nome do fabricante do dispositivo)** | Modelo: **(Modelo do dispositivo)** | Número de série: **(Número de série do dispositivo)** |
| Data e hora da coleta: **(Data e hora da coleta do vestígio)** | Local da coleta: **(Local da coleta do vestígio)** | Nome de quem coletou: **(Nome completo de quem realizou a coleta)** |

*Figura 34: Exemplo de texto dos procedimentos de fixação e coleta*

c) **Acondicionamento e transporte:** descrição dos procedimentos por meio dos quais cada vestígio coletado é embalado de forma individualizada e transportado de um local para outro. Veja o exemplo a seguir:

**1.3.Do acondicionamento e transporte (art. 158-B, V e VI, do CPP)**

Concluída a descrição e coleta, o *AGENTE* realizou o acondicionamento do vestígio em recipiente adequado, embalado de forma individualizada e devidamente identificado, conforme formulário de acompanhamento de vestígio *XV/XXXX*. Concluído o procedimento de acondicionamento, o vestígio foi transportado, de forma segura e com garantia de integridade, para a central de custódia, conforme formulário de transporte de vestígio *XV/XXXX*.

*Figura 35: Exemplo de texto dos procedimentos de acondicionamento e transporte*

d) **Recebimento:** descrição do ato formal de transferência da posse do vestígio. Veja o exemplo:

**1.4.Do recebimento (art. 158-B, VII, do CPP)**

O vestígio foi recebido na central de custódia, em *XX/XX/XXXX*, após transporte seguro, conforme formulário de recebimento de vestígio *XX/XXXX* e formulário de transporte de vestígio *XX/XXXX*.

Após abertura de pedido de exame pericial, o vestígio foi transportado do Departamento de Polícia Federal no *XX* para a Secretaria de Perícia, Pesquisa e Análise, conforme formulário de transporte de vestígio *XX/XXXX* e formulário de recebimento de vestígio *XX/XXXX*.

*Figura 36: Exemplo de texto dos procedimentos de acondicionamento e transporte*

### 5.4.4 Material

Nesta seção, o analista descreverá o vestígio sob exame, ou seja, o material questionado. É relevante a descrição detalhada do vestigio. Para tanto, o analista utilizará a descrição contida no termo de apreensão – Formulário de Recebimento de Vestígio – além da descrição própria, obtida por meio da observação do vestígio. Haverá também complementação das descrições do procedimento de fixação, da seção anterior, uma vez que o analista poderá retificar ou complementar as descrições já apresentadas. Além disso, o analista poderá utilizar fotografias para exibir o vestígio. Veja o exemplo a seguir:

**II.MATERIAL (vestígio)**

Os exames periciais serão realizados em cópia forense obtida do seguinte vestígio:

**Tabela 2:** descrição do vestígio que será examinado.

| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item:<br>Item X do Termo de Apreensão XX/XXXX. | Descrição do item:<br>**Pen drive com capacidade de armazenamento de 16GB (Gigabytes);**<br>**Possui formado de cartão de crédito com as seguintes descrições: Platinum; 4018 0400 7000 7007; 10/04; 09/07; XIAOPING SONG; e VISA.**<br>**Relativo à Fotografia 1.** | |
| Fabricante:<br>**Não consta.** | Modelo:<br>**Não consta.** | Número de série:<br>**Não consta.** |
| Data e hora da coleta:<br>XX/XX/XXX às XX:XX | Local da coleta:<br>Brasília, DF. | Nome de quem coletou:<br>Agente XXXXXXX. |


**Fotografia 1:** Pen drive, descrição constante da Tabela 2.

*Figura 37: Exemplo de descrição de vestígio*

### 5.4.5 Objetivos

Nesta seção, o analista descreverá os objetivos do exame pericial. Podem estar relacionados ao atendimento de quesitos específicos ou genéricos, ou, ainda, relacionados à constatação de algum fato. Veja o exemplo a seguir:

**III. OBJETIVOS**

Extração e exame do material contido no vestígio para constatação da existência, ou não, de imagens e vídeos com conteúdo de pornografia infanto-juvenil.

Os objetivos específicos são: resposta aos quesitos apresentados pelo Procurador da República XXXXX:

a) 1ª quesito: Existem imagens com pornografia infanto-juvenil no disco rígido?
b) 2ª quesito: As imagens estão relacionadas a qual usuário do sistema operacional? e
c) 3ª quesito: Quais as datas de acesso ou modificação dos arquivos de imagens?

*Figura 38: Exemplo de objetivos de Laudo Pericial*

### 5.4.6 Exame

Nesta seção, o analista descreverá os métodos científicos adotados para o processamento e o exame pericial. Importante consignar a manutenção da integridade do vestígio original, permitindo contraperícia em momento posterior. Veja o exemplo a seguir:

**IV. EXAMES**

A princípio, foi realizada cópia forense do material para posterior processamento e exame pericial sobre a cópia, preservando o vestígio original de qualquer alteração para posterior contra perícia, caso necessário.

**Tabela 3**: descrição da imagem forense.

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: **00/00/0000** | Criador: **(Nome do criador da imagem)** | Método usado: **(Método utilizado para criação da imagem)** | Nome da imagem: **(Nome único da imagem forense)** | Quantidade de segmentos: **(Quantidade de segmentos da imagem forense)** |
| Dispositivo em que a imagem está armazenada: **(Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense)** | | Hash da imagem: **(Hash 256 da imagem forense)** | | |

Os exames preliminares demonstraram que o usuário XXXX utilizava o Sistema Operacional Windows 10, release XXXX, com diversos softwares instalados, em especial:

a) navegador web Google Chrome, versão XX;
b) software eMule, versão XX;
c) softwares Kazaa;

*Figura 39: Exemplo de texto descrevendo parte o exame*

### 5.4.7 Respostas aos quesitos ou conclusões

Nesta seção, o analista apresentará resposta aos quesitos formulados ou emitirá opinião técnica sobre fato ou assunto, tendo como base as análises realizadas na Seção Exames. Veja o exemplo de resposta aos quesitos:

**V. CONCLUSÕES E RESPOSTAS AOS QUESITOS**

A partir dos exames realizados, conforme Seção IV, é possível apresentar respostas aos seguintes quesitos:

a) **1ª quesito**: Existem imagens com pornografia infanto-juvenil no disco rígido?
**Resposta**: existem um total de 10.000 (dez mil) imagens pornográficas, das quais cerca de 5.000 (cinco mil) estão relacionadas à pornografia infanto-juvenil.

d) **2ª quesito**: As imagens estão relacionadas a qual usuário do sistema operacional?
**Resposta**: As imagens estavam armazenadas no diretório local C:\Sistema\XXX\.figuras. O sistema operacional possuía apenas um usuário: XXXXXX.

b) **3ª quesito**:...

*Figura 40: Exemplo de respostas aos quesitos*

## 5.5 Documentos técnicos de registro

Os documentos processuais técnicos de registro compõem a Cadeia de Custódia e registram a história cronológica do vestígio. Os formulários registram o recebimento, o transporte, o acompanhamento e o descarte dos vestígios.

### 5.5.1 Formulário de Recebimento de Vestígio

O Formulário de Recebimento de Vestígio tem como objetivo registrar o ato formal de transferência da posse do vestígio quando ingressa a primeira vez no Ministério Público Federal. Deve ser preenchido somente uma vez, quando do recebimento do vestígio por membro ou servidor do MPF. Por exemplo, recebimento de vestígios de colaboradores, ou recebimento de vestígios de afastamento de sigilo telemático de provedores de serviço de internet, ou, ainda, recebimento de vestígio do Departamento de Polícia Federal. Todas as pessoas que participaram da entrega e recebimento dos vestígios estarão identificadas no formulário.

O preenchimento do formulário deve ser realizado com riqueza de detalhes e precisão. Observe a capa do Formulário de Recebimento de Vestígios:

MPF SECRETARIA DE PERÍCIA PESQUISA E ANÁLISE

Nº ÚNICO: PR/XX-000000000/0000

**Formulário de Recebimento de Vestígios**

**0/0000**

Número do procedimento:
0.000.000.00000/0000

Pessoa física ou jurídica remetente:
(Nome da empresa ou colaborador);

Autoridade ou servidor receptor:
Dr. XXXXXXX, Procurador da República.

Ementa: formulário de recebimento de vestígios apresentados como prova no âmbito do caso XXXXX da Procuradoria da República no Município de XXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e a qualificação.

*Figura 41: Capa do Formulário de Recebimento de Vestígio*

O formulário de recebimento apresenta campo para descrição dos vestígios e imagens forenses recebidas. O formulário poderá conter um ou mais vestígios, ou uma ou mais imagens forenses. Quando não existir imagem forense, o quadro descritivo da imagem permanecerá em branco.

| **Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros)** | | |
|---|---|---|
| Número do item: **(Identificação única para o item no termo de apreensão)** | Descrição do item: **(Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras)** | |
| Fabricante: **(Nome do fabricante do dispositivo)** | Modelo: **(Modelo do dispositivo)** | Número de série: **(Número de série do dispositivo)** |
| Data e hora da coleta: **(Data e hora da coleta do vestígio)** | Local da coleta: **(Local da coleta do vestígio)** | Nome de quem coletou: **(Nome completo de quem realizou a coleta)** |

| **Imagem Forense** | | | | |
|---|---|---|---|---|
| Data de criação: **00/00/0000** | Criador: **(Nome do criador da imagem)** | Método usado: **(Método utilizado para criação da imagem)** | Nome da imagem: **(Nome único da imagem forense)** | Quantidade de segmentos: **(Quantidade de segmentos da imagem forense)** |
| Dispositivo em que a imagem está armazenada: **(Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense)** | | Hash da imagem: **(Hash 256 da imagem forense)** | | |

*Figura 42: Descrição do vestígio e da imagem forense*

O formulário de recebimento também apresenta local para qualificação das pessoas envolvidas no ato de transferência da posse do vestígio. Veja o quadro de qualificação:

| **Qualificação do remetente (quem está entregando o vestígio):** | |
|---|---|
| Nome completo (pessoa física ou jurídica): | **(Razão social da empresa)** |
| Endereço: | **(Endereço completo da empresa)** |
| CPF/CNPJ: | **00.000.000/0000-00 (número do CNPJ da empresa ou CPF da pessoa física)** |
| Nome do advogado: | **(Nome completo do advogado)** |
| CPF do advogado: | **000.000.000-00 (número do CPF)** |
| OAB: | **0000-XX (número da OAB)** |
| Local / Data: | **(local e data de assinatura do documento)** |
| Assinatura:<br>Documento com assinatura digital. | |

| **Qualificação do receptor (Membro ou servidor que recebe o vestígio):** | |
|---|---|
| Nome completo: | **(Nome completo do Membro ou servidor)** |
| Matrícula: | **(Matrícula do Membro ou servidor)** |
| Cargo: | **(Nome do cargo)** |
| Local / Data: | **(Local e data de assinatura do documento)** |
| Assinatura:<br>Documento com assinatura digital. | |

*Figura 43: Qualificação*

### 5.5.2 Formulário de Transporte de Vestígio

O Formulário de Transporte de Vestígio tem como objetivo registrar o ato formal de transferência da posse do vestígio durante o procedimento de transporte. Deve ser preenchido sempre que o vestígio for transportado interna ou externamente ao Ministério Público Federal. Por exemplo, quando ocorre a transferência de posse interna entre as unidades do Ministério Público Federal, ou externamente entre o MPF e a Polícia Federal. Com isso, todas as pessoas que tiveram a posse do vestígio no processo de transporte estarão registradas.

O preenchimento do formulário deve ser realizado com riqueza de detalhes e precisão. Observe a capa do formulário de transporte:


MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

Nº ÚNICO: PR/XX-000000000/0000

Formulário de Transporte de Vestígios
00/0000

Referência: 0.000.000.00000/0000

Unidade ou órgão remetente: Procuradoria da República no Município de XXXXXX – XX.

Autoridade Requerente: XXXXXXXX, Procurador da República.

Ementa: formulário de transporte de vestígio para exames periciais de uma unidade de disco rígido de 1TB (Terabyte) e instrução processual, referente ao caso XXXX da Procuradoria da República no Município de XXXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e o rol de assinaturas da cadeia de custódia.

*Figura 44: Capa do Formulário de Transporte de Vestígio*

O Formulário de Transporte de Vestígio apresenta campo para descrição dos vestígios e imagens forenses transportados. O formulário poderá conter um ou mais vestígios, ou uma ou mais imagens forenses. Quando não existir imagem forense, o quadro descritivo da imagem permanecerá em branco.

| Vestígio<br>(dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item:<br>**(Identificação única para o item no termo de apreensão)** | Descrição do item:<br>**(Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras)** | |
| Fabricante:<br>**(Nome do fabricante do dispositivo)** | Modelo:<br>**(Modelo do dispositivo)** | Número de série:<br>**(Número de série do dispositivo)** |
| Data e hora da coleta:<br>**(Data e hora da coleta do vestígio)** | Local da coleta:<br>**(Local da coleta do vestígio)** | Nome de quem coletou:<br>**(Nome completo de quem realizou a coleta)** |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação:<br>**00/00/0000** | Criador:<br>**(Nome do criador da imagem)** | Método usado:<br>**(Método utilizado para criação da imagem)** | Nome da imagem:<br>**(Nome único da imagem forense)** | Quantidade de segmentos:<br>**(Quantidade de segmentos da imagem forense)** |
| Dispositivo em que a imagem está armazenada:<br>**(Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense)** | Hash da imagem:<br>**(Hash 256 da imagem forense)** | | | |

*Figura 45: Descrição do vestígio e da imagem forense*

Veja o exemplo do preenchimento do formulário de transporte com o registro das alterações de posse dos vestígios durante o transporte.

| Cadeia de Custódia | | | | |
|---|---|---|---|---|
| Passo | Data/Hora | Remetente: | Destinatário: | Motivo: |
| 1 | Data:<br>**00/00/0000** | Nome:<br>**(Nome completo do remetente)** | Nome:<br>**(Nome completo do destinatário)** | **(Descrição sucinta do motivo do transporte do vestígio, por exemplo, para realizar exame pericial)** |
| | Hora:<br>**00:00** | Cargo e matrícula/CPF:<br>**(Cargo e matrícula do remetente)** | Cargo e matrícula/CPF:<br>**(Cargo e matrícula do destinatário)** | |
| | Origem/Destino:<br>**(Local de origem e local de destino)** | Assinatura:<br>**(Assinatura do remetente)** | Assinatura:<br>**(Assinatura do destinatário)** | |

| Cadeia de Custódia | | | | |
|---|---|---|---|---|
| Passo | Data/Hora | Remetente: | Destinatário: | Motivo: |
| 2 | Data:<br>**00/00/0000** | Nome:<br>**(Nome completo do remetente)** | Nome:<br>**(Nome completo do destinatário)** | **(Descrição sucinta do motivo do transporte do vestígio, por exemplo, para realizar exame pericial)** |
| | Hora:<br>**00:00** | Cargo e matrícula/CPF:<br>**(Cargo e matrícula do remetente)** | Cargo e matrícula/CPF:<br>**(Cargo e matrícula do destinatário)** | |
| | Origem/Destino:<br>**(Local de origem e local de destino)** | Assinatura:<br>**(Assinatura do remetente)** | Assinatura:<br>**(Assinatura do destinatário)** | |

*Figura 46: Descrição da cadeia de posse*

### 5.5.3 Formulário de Acompanhamento de Vestígio

O Formulário de Acompanhamento de Vestígio tem como objetivo registrar cada rompimento de lacre do recipiente do vestígio. Observe a seguir a capa do Formulário de Acompanhamento de Vestígio.


*Figura 47: Capa do Formulário de Acompanhamento de Vestígio*

O Formulário de Acompanhamento de Vestígio apresenta campo para descrição dos vestígios e das imagens forenses contidos no recipiente. O formulário conterá apenas um vestígio, ou uma ou mais imagens forenses. Quando não existir imagem forense, o quadro descritivo da imagem permanecerá em branco.

| Vestígio<br>(dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item:<br>(Identificação única para o item no termo de apreensão) | Descrição do item:<br>(Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras) | |
| Fabricante:<br>(Nome do fabricante do dispositivo) | Modelo:<br>(Modelo do dispositivo) | Número de série:<br>(Número de série do dispositivo) |
| Data e hora da coleta:<br>(Data e hora da coleta do vestígio) | Local da coleta:<br>(Local da coleta do vestígio) | Nome de quem coletou:<br>(Nome completo de quem realizou a coleta) |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação:<br>00/00/0000 | Criador:<br>(Nome do criador da imagem) | Método usado:<br>(Método utilizado para criação da imagem) | Nome da imagem:<br>(Nome único da imagem forense) | Quantidade de segmentos:<br>(Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada:<br>(Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense) | | Hash da imagem:<br>(Hash 256 da imagem forense) | | |

*Figura 48: Descrição do vestígio e da imagem forense*

A cada rompimento de lacre, deve-se fazer constar na ficha de acompanhamento de vestígio o nome e a matrícula do responsável, a data, o local, a finalidade, bem como as informações referentes ao novo lacre utilizado. Com isso, todas as informações sobre as pessoas que romperem o lacre do recipiente do vestígio serão registradas.

| Registro de abertura do recipiente do vestígio<br>(Sempre incluir o lacre violado dentro do novo recipiente) | | | | |
|---|---|---|---|---|
| Abertura | Data/Hora | Quem abriu: | Números dos lacres: | Finalidade: |
| 1 | Data:<br>00/00/0000 | Nome:<br>(Nome da pessoa que abriu o recipiente lacrado) | Número do lacre violado:<br>(Identificação única do recipiente aberto) | (Descrição sucinta do motivo da abertura do recipiente do vestígio, por exemplo, para realizar exame pericial) |
| | Hora:<br>00:00 | Cargo/matrícula:<br>(Cargo e matrícula da pessoa que abriu o recipiente lacrado) | Número do novo lacre:<br>(Identificação única do novo recipiente que será utilizado) | |
| | Local:<br>(Local de abertura do recipiente) | Assinatura:<br>(Assinatura da pessoa que abriu o lacre) | Observação:<br>(Alguma observação sobre abertura ou novo lacre, caso seja necessário) | |

*Figura 49: Registro de rompimento do lacre do recipiente do vestígio*

### 5.5.4 Formulário de Descarte de Vestígio

O Formulário de Descarte de Vestígio tem como objetivo registrar o ato formal de transferência da posse do vestígio durante o procedimento de descarte, ou seja, procedimento de liberação do vestígio. Como exemplos, podemos citar a devolução de um aparelho celular ao seu proprietário, a devolução de um computador, entre outras situações. Com isso, registra-se o momento em que o vestígio foi descartado e não deverá ser utilizado para novos exames periciais. Veja a capa do Formulário de Descarte de Vestígio.


MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

Nº ÚNICO: PR/XX-000000000/0000

Formulário de Descarte de Vestígios

0/0000

Número do procedimento:
0.000.000.00000/0000

Pessoa física ou jurídica receptora do vestígio:
(Nome da empresa ou colaborador);

Autoridade que descarta o vestígio:
Dr. XXXXXXX, Procurador da República.

Decisão da autoridade:
O descarte do vestígio será realizado no cumprimento da decisão judicial, XXXX, que determinou a devolução dos vestígios

Ementa: formulário de descarte de vestígios apresentados como prova no âmbito do caso XXXXX da Procuradoria da República no Município de XXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e a qualificação.

*Figura 50: Capa do Formulário de Descarte de Vestígio*

O Formulário de Descarte de Vestígio apresenta campo para descrição dos vestígios e das imagens forenses descartados. O formulário poderá conter um ou mais vestígios, ou uma ou mais imagens forenses. Quando não existir imagem forense, o quadro descritivo da imagem permanecerá em branco.

| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: (Identificação única para o item no termo de apreensão) | Descrição do item: (Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras) | |
| Fabricante: (Nome do fabricante do dispositivo) | Modelo: (Modelo do dispositivo) | Número de série: (Número de série do dispositivo) |
| Data e hora da coleta: (Data e hora da coleta do vestígio) | Local da coleta: (Local da coleta do vestígio) | Nome de quem coletou: (Nome completo de quem realizou a coleta) |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: 00/00/0000 | Criador: (Nome do criador da imagem) | Método usado: (Método utilizado para criação da imagem) | Nome da imagem: (Nome único da imagem forense) | Quantidade de segmentos: (Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada: (Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense) | | Hash da imagem: (Hash 256 da imagem forense) | | |

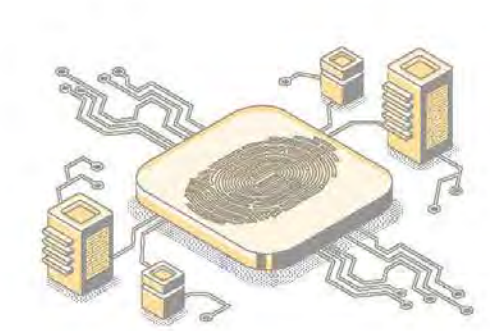
*Figura 51: Descrição do vestígio e da imagem forense*

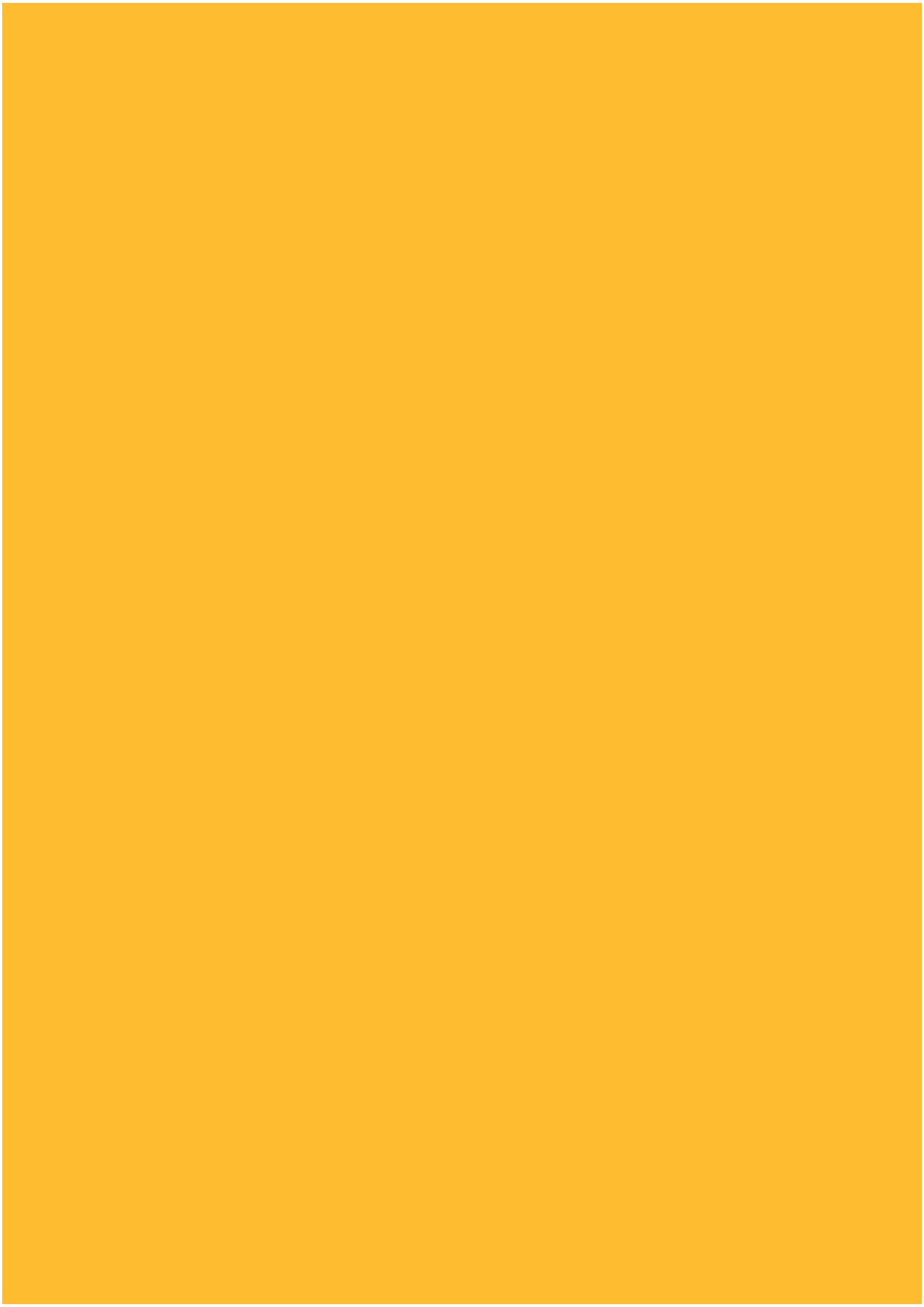
O Formulário de Descarte de Vestígio também apresenta local para qualificação das pessoas envolvidas no ato de transferência da posse do vestígio. Veja o quadro de qualificação:

| | |
|---|---|
| Nome completo: | (Nome completo do Membro ou servidor) |
| Matrícula: | (Matrícula do Membro ou servidor) |
| Cargo: | (Nome do cargo) |
| Local / Data: | (Local e data de assinatura do documento) |
| Assinatura: Documento com assinatura digital. | |

| Qualificação do receptor do vestígio (quem está recebendo o vestígio descartado): | |
|---|---|
| Nome completo (pessoa física ou jurídica): | (Razão social da empresa) |
| Endereço: | (Endereço completo da empresa) |
| CPF/CNPJ: | 00.000.000/0000-00 (número do CNPJ da empresa ou CPF da pessoa física) |
| Nome do advogado: | (Nome completo do advogado) |
| CPF do advogado: | 000.000.000-00 (número do CPF) |
| OAB: | 0000-XX (número da OAB) |
| Local / Data: | (local e data de assinatura do documento) |
| Assinatura: Documento com assinatura digital. | |

*Figura 52: Qualificação no descarte*





# CAPÍTULO 6

## SOLICITAÇÃO DE SERVIÇO PERICIAL OU DE SUPORTE EM TIC

Conforme dispõe a Instrução de Serviço nº 05/2019/Sppea, toda solicitação de serviço pericial ao Centro Nacional de Perícia da Secretaria de Perícia, Pesquisa e Análise (CNP/Sppea) deve ser formalizada exclusivamente pelo Sistema Pericial por membros do MPF. Complementarmente, demandas registradas por assessores designados deverão ser validadas pelo membro titular do respectivo Ofício.

Tal ato normativo está em linha com a Recomendação nº 10/2018, da Corregedoria-Geral do Ministério Público Federal, segundo a qual os membros devem formalizar "a solicitação de serviço pericial unicamente através do sistema informatizado disponibilizado no âmbito do Ministério Público Federal".

Atualmente, o Sistema Pericial pode ser acessado pelo endereço https://portal.mpf.mp.br/pericial ou a partir do ícone próprio localizado no Portal MPF (https://portal.mpf.mp.br). Após efetuar a autenticação (mediante endereço eletrônico de e-mail e senha pessoal), o demandante deparar-se-á com interface similar à figura a seguir:


*Figura 53: Interface após autenticação do Sistema Pericial*

Em seguida, o solicitante deverá clicar em "Solicitar" > "Perícia". Na sequência, o sistema exigirá que seja informado o número do Processo/Procedimento associado ao pedido, conforme figura a seguir:


*Figura 54: Solicitação do número do processo/procedimento por parte do Sistema Pericial*

Após a localização do processo/procedimento em questão, o Sistema Pericial apresentará o formulário de cadastro da demanda, que contém alguns campos para preenchimento. Em relação ao campo "Tipo da demanda", existem três opções:

a) Perícia: a Perícia se caracteriza por ser um trabalho técnico-científico sobre questões não jurídicas necessário para atuação do membro.

b) Planejamento de Perícia: serve como opção para registrar o contato inicial do membro com a área pericial para orientações quando houver uma adequada solicitação da perícia.

c) Suporte em TI: essa opção está relacionada aos trabalhos de TIC descritos a seguir no item Serviço Pericial, realizados por técnicos habilitados.

Para o registro da solicitação do serviço pericial de TIC, deve ser selecionada a opção "Perícia". No campo "Contextualização e Objetivos", devem ser descritos objetivo do exame pericial, eventual localização e demais informações que facilitem o entendimento do escopo do trabalho. A figura a seguir ilustra esses campos mencionados:

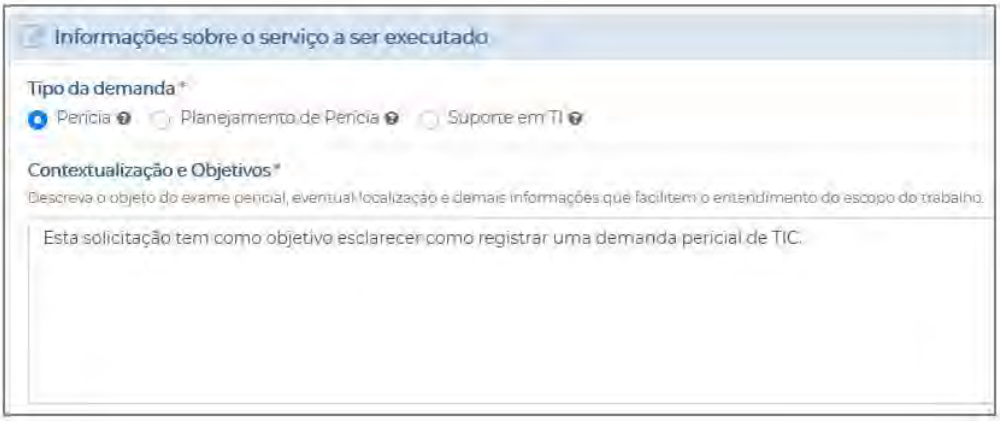



*Figura 55: Registro do tipo de manda e contextualização*

Na sequência, no campo "Serviço Pericial", deve ser selecionada a opção mais adequada ao caso concreto. Nos casos relacionados à perícia de TIC, na maioria dos casos, deve-se selecionar a opção "Assessoramento pericial" e/ou "Respostas a quesitos formulados". A figura a seguir ilustra essa ação:


*Figura 56: Especificação do registro da demanda.*

No campo "Área pericial", a opção "Tecnologia da Informação e Comunicação" deve ser selecionada, assim como a respectiva assessoria responsável pelo atendimento da demanda. Em seguida, o demandante deverá registrar claramente os quesitos. A figura a seguir ilustra um exemplo:

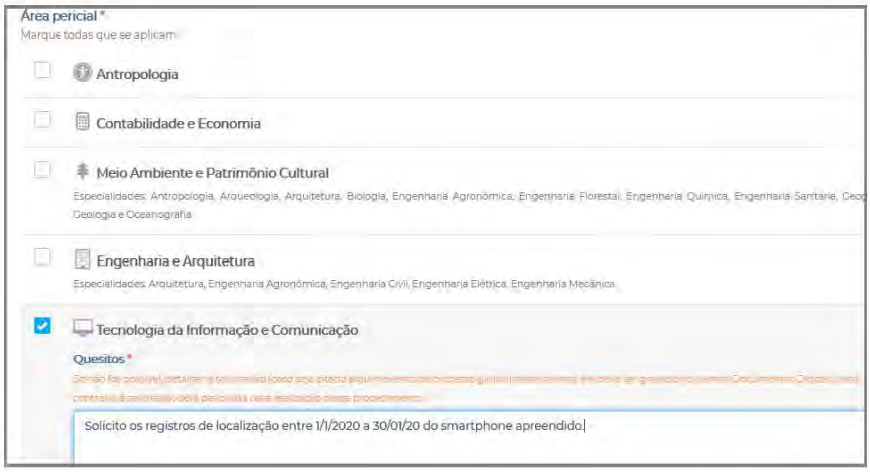



*Figura 57: Registro da especialidade da perícia e dos quesitos*

Posteriormente, há o campo "Risco do trabalho de campo". O demandante deve avaliar o caso concreto e selecionar a melhor opção. Em continuidade, a seção "Documentos a serem examinados" apresenta os campos "Documentos digitais" e "Documentos físicos".

Caso existam arquivos digitais importantes à perícia, eles devem ser adicionados mediante a opção "Adicionar arquivos". Além disso, caso seja pertinente o envio de documentos físicos ao corpo pericial, a opção adequada deve ser selecionada no campo "Documentos físicos". A figura a seguir ilustra um exemplo de preenchimento desses dois campos:

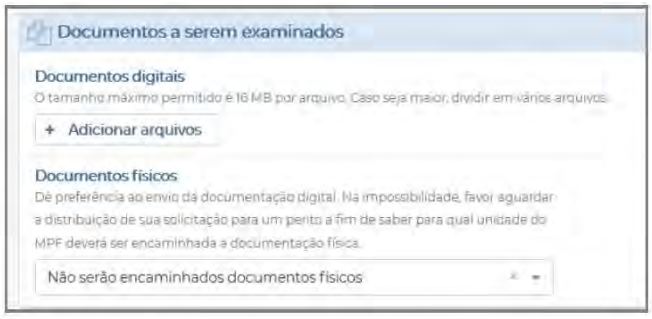


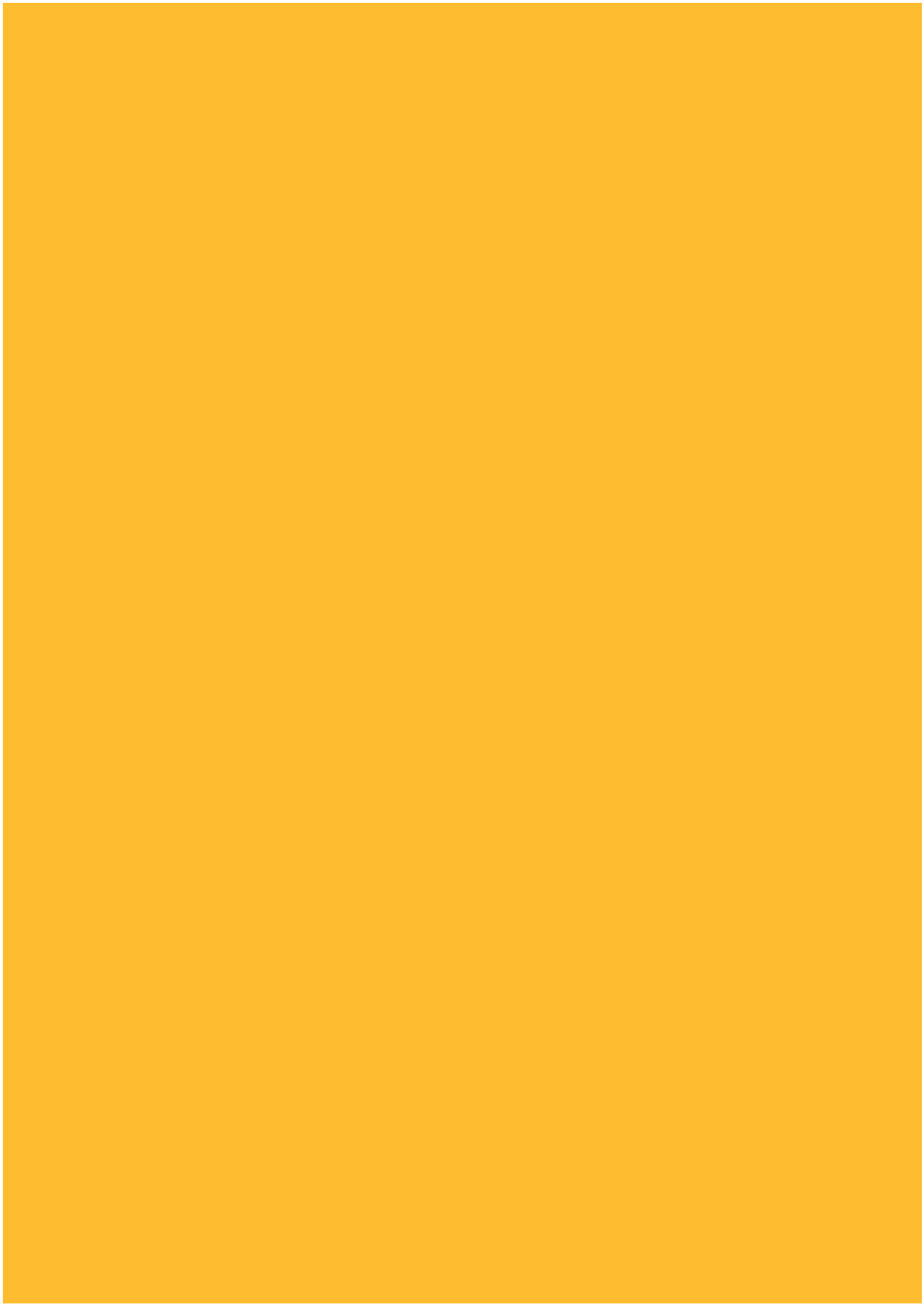

*Figura 58: Registro de documentos a serem encaminhados ao corpo pericial*

Em sequência, a seção "Ordem de atendimento" apresenta o campo "Classificação". Em regra, o demandante deve selecionar a opção "Demanda ordinária". Caso seja uma demanda emergencial, a opção "Demanda urgente" deve ser selecionada. Nesse caso, alguns critérios devem ser atendidos, conforme determinado pela IS nº 05/2019 MPF/PGR. No exemplo em tela, foi selecionada a opção "Demanda ordinária", conforme se observa da figura a seguir:


***Figura 59:*** *Classificação da demanda quanto à prioridade*

O último campo, "Telefone para contato", deve ser utilizado para o registro do número de contato com o demandante. Para encerrar, basta o envio da solicitação mediante o botão "Enviar".

Ressalta-se que o Sistema Pericial também deve ser utilizado para as solicitações de apoio para a coleta de vestígios e a geração de *hashes*, por meio da opção Suporte em TI. Nessa hipótese, não será realizada perícia, mas tão somente atividade com a finalidade precípua de coletar evidências digitais com as cautelas necessárias à preservação da integridade dos arquivos.



# GLOSSÁRIO[6]

**Análise:** processo amplamente automatizado de classificação, organização e tradução de dados. Muitas ferramentas forenses analisam uma imagem forense e fornecem resultados fáceis de revisar após classificar a maioria dos dados em categorias ou plotar dados em linhas e colunas.

**Aplicativo (App):** programa que é executado em um dispositivo móvel. *Softwares* como o Cellebrite geralmente oferecem suporte a aplicativos populares e analisam dados automaticamente. Outros aplicativos podem ser analisados manualmente para converter dados em formatos legíveis por humanos.

**AppleID:** conta usada para gerenciar dispositivos Apple. Um AppleID conectado a vários dispositivos geralmente compartilha ou sincroniza dados de um para outro. Os dados excluídos de um dispositivo podem ser encontrados em outro.

**Atualizações de *firmware*:** a maioria das atualizações corrige várias explorações usadas por ferramentas forenses. Pode demorar algum tempo para que as ferramentas consigam acompanhar as atualizações, a fim de garantir que os dados sejam analisados com precisão. Um banco de dados usado para armazenar mensagens de texto pode manipular dados de maneira diferente quando uma nova atualização é lançada.

**Autopsy:** uma plataforma forense digital leve e gratuita. Capaz de processar, realizar *data carving* e pesquisar.

**Axiom da Magnet:** anteriormente conhecido como IEF (*Internet Evidence Finder*), o Axiom é a principal ferramenta de análise de dados da web. O Axiom processa imagens forenses e outras fontes de dados e analisa dados relacionados à atividade na web, como histórico da web, cookies da web, histórico de downloads, bate-papo na web, webmail etc. O Axiom também simplifica o processo de análise de artefatos do sistema, como histórico de USB e histórico de documentos. O Axiom permite gerar relatórios em arquivos de carregamento, PDF, Excel, HTML e muito mais.

***Backups* de dispositivos móveis:** muitos fabricantes e fornecedores oferecem um sistema de *backup* proprietário.

6 Tradução adaptada de https://www.istmanagement.com/ist-discover-e-digital-forensic-terms.html.

***Backups* de PC em nuvem:** algumas empresas utilizam serviços de *backup*, como Carbonite, Azure e iDrive, para fazer *backup* de seu armazenamento em nuvem. Esses *backups* geralmente podem ser exportados para uma unidade externa e fotografados. Normalmente, são exportações simples, com dados armazenados em pastas em vez de uma imagem compactada ou formato proprietário.

**Banco de dados em celulares:** usado por aplicativos de celular para armazenar e recuperar informações. Mantém espaço livre no interior, o que potencialmente permite a recuperação de dados excluídos, como mensagens de texto e chamadas.

***BlackLight* da *BlackBag*:** uma poderosa plataforma de análise forense, como FTK e *EnCase*, o *BlackLight* pode lidar com evidências de várias fontes. A grande diferença entre o *BlackLight* e as outras ferramentas é sua capacidade de analisar imagens de computadores Apple (Mac) com análises mais inteligentes.

**Bloqueador de gravação USB:** o USB *Write Blocker* é uma ferramenta forense profissional para investigar dispositivos de armazenamento em massa USB, como *pen drives*, e atua como uma ponte entre os dispositivos USB e um computador para proteger as evidências de USB quando está conectado a um computador. Isso inclui unidades externas e unidades *flash*, e é utilizado por investigadores digitais, técnicos e equipe de TI.

**Cartões de memória:** pequenos cartões de memória *flash* usados para expandir o armazenamento em telefones celulares, câmeras digitais etc. Ex.: MicroSD, SD, Sony Memory Stick Pro Duo, CF, SDHC.

**Cellebrite UFED:** às vezes chamado de UFED, Touch Ultimate ou UFED 4 PC, o Cellebrite é uma poderosa ferramenta de coleta e análise de dispositivos móveis. O Cellebrite é capaz de extrair dados de telefones, tablets, unidades de GPS, drones etc. É capaz de vários tipos de extrações e fornece um poderoso ambiente de revisão para realizar análises. O Cellebrite armazena a maioria das extrações nos formatos .UFD, .ZIP e .BIN. e oferece relatórios poderosos de dados em vários formatos: Word, PDF, Excel, HTML e UFED Reader (UFDR). O Cellebrite apresenta-se nas versões de hardware e software, com vários adaptadores e cabos que permitem a conexão a quase todos os dispositivos de bolso lançados nos últimos 10 anos.

**Conta do Google:** a conta usada para gerenciar dispositivos Android. Uma conta do Google conectada a vários dispositivos geralmente compartilha ou sincroniza dados de um para outro. Os dados excluídos de um dispositivo ainda podem ser encontrados em outro.

**Dados ativos:** arquivos que não foram excluídos e que podem ser coletados usando todos os métodos de imagem. Os dados ativos residem no espaço "alocado" em um disco.

**Dados excluídos:** dados residentes no "espaço livre". Quando um arquivo é excluído, o espaço no disco em que o arquivo reside é marcado como "livre" ou disponível para novas gravações e é removido da visualização. Isso informa ao sistema operacional que esse espaço agora pode ser usado para gravar novos dados.

**Disco rígido externo alimentado:** unidades externas com velocidades de gravação mais rápidas. Essas unidades requerem energia através de uma tomada e uma conexão USB a um computador. Geralmente possuem capacidade muito grande. Exemplos incluem o WD MyBook e o Seagate Backup Plus. Essas unidades geralmente são muito grandes (TB +).

**Disco rígido externo:** um disco rígido externo que se conecta a um computador via conexão USB. Os tempos de criação de imagens dependem da capacidade.

**Disco rígido interno para desktop:** unidades usadas em PCs *desktop*, iMacs e alguns servidores (disco magnético giratório, 3,5 polegadas). Conexão SATA.

**Disco rígido interno para laptop:** unidades usadas em *laptops* menores que os discos rígidos internos para *desktop* (disco magnético giratório, 2,5 polegadas). Conexão SATA. Encontrado nos formatos lógicos .AD1 e .L01 (FTK e EnCase, respectivamente).

**Duplicador forense:** os duplicadores forenses são a versão de hardware das ferramentas de criação de imagens de *software*. São unidades físicas do tamanho de uma viagem, aproximadamente do tamanho de um *modem*. A evidência (unidade de origem) está conectada de um lado (lado protegido contra gravação) e a unidade de destino no lado oposto (lado de gravação). No MPF possuímos duplicadores TX1 da Tableau, que podem criar clones de um disco, criar imagens e verificar a imagem. Os Tableaus são soluções de imagem rápidas e confiáveis para discos rígidos SATA, discos rígidos externos, dispositivos USB como unidades *flash* e muito mais. Os Tableaus possuem pequenos painéis LCD que exibem o progresso da imagem e o tempo estimado para a conclusão. Eles também fornecem um registro forense completo do processo de geração de imagens e verificação, que é armazenado na mesma pasta da imagem. Também notifica o usuário sobre erros. Os duplicadores geralmente podem ser usados para sanitizar (*wipe*) unidades forenses.

**Elcomsoft Phone Breaker:** ferramenta que possibilita a "quebra" da proteção por senha nos *backups* por telefone. Senhas simples podem ser quebradas em questão de minutos ou horas. Senhas complicadas podem levar semanas, meses ou até anos. Essa ferramenta também é usada para obter *backups* do iCloud de dispositivos Apple da nuvem. Ele nos permite acessar a conta do iCloud de um custodiante (credenciais necessárias). Os *backups* baixados são analisados no Cellebrite para análise e produção.

**EnCase da Guidance Software:** assim como o FTK, o EnCase processa e indexa dados para pesquisas e análises. Muitos examinadores usam um ou outro – até ambos.

**Espaço Alocado:** espaço em uma mídia de armazenamento em uso pelo sistema operacional em que os arquivos residem. Quando um arquivo é criado, um sistema operacional como o Windows procurará espaço livre no espaço alocado da unidade.

**Espaço livre:** espaço disponível em uma mídia de armazenamento onde os dados podem ser armazenados. Novos arquivos são gravados no espaço livre. Ou, ainda, o espaço não utilizado no final de um arquivo em um sistema de arquivos que usa *clusters* de tamanho fixo (portanto, se o arquivo for menor que o tamanho do bloco fixo, o espaço não utilizado será deixado sem uso). Frequentemente contém informações excluídas de usos anteriores do bloco.

**Espaço não alocado:** espaço em uma mídia de armazenamento que não é alocado ou em uso pelo sistema operacional (não usado para armazenar arquivos). Mesmo ao formatar um disco rígido, os dados perdidos ainda podem persistir no espaço não alocado.

**Extração do sistema de arquivos em dispositivos móveis:** extração mais comum na maioria dos telefones celulares. Ela permite que um examinador extraia bancos de dados e outros dados do sistema de um dispositivo móvel para análise no *software* de análise de dispositivos móveis, como o UFED Physical Analyzer da Cellebrite. Esses bancos de dados geralmente contêm dados excluídos. As extrações incluem dados do aplicativo. Além dos bancos de dados, essa extração pode acessar apenas o espaço alocado, o que significa que não há dados excluídos fora do que está contido nos bancos de dados ou em outros arquivos que atuam como contêineres.

**Extração física em dispositivos móveis:** esse tipo de extração é o único formato "imagem" verdadeiro entre todos os tipos de extração. É uma imagem verificada 1: 1 do chip de armazenamento interno do telefone. Ele permite que um examinador acesse espaço livre / não alocado para recuperar / executar *carving* dos dados excluídos. Esse tipo de extração geralmente não é suportado em dispositivos que executam patches de segurança recentes, versões de *firmware* ou compilações. Isso significa que a maioria dos dispositivos não permitirá uma extração física até meses depois de não serem atualizados.

**Extração lógica em dispositivos móveis:** uma extração básica de dados de um dispositivo móvel limitada às opções de exportação pré-configuradas do telefone. Geralmente definido pelo fabricante e geralmente muito limitado e fornece pouco ou nenhum dado excluído. Vários tipos de extração podem ser combinados em um. Por exemplo, atualmente os dispositivos Samsung Galaxy impedem que um examinador extraia mensagens usando os métodos de extração mais poderosos. No entanto, as mensagens podem ser extraídas usando um método lógico, e combinadas posteriormente.

**Faraday (Sacola / Gaiola):** uma sacola ou sala que bloqueia ondas de rádio, impedindo que os celulares se comuniquem com um sinal externo, como uma torre ou rede Wi-Fi. Útil em questões criminais, quando um suspeito pode enviar um sinal de limpeza remoto para um telefone inteligente.

**FTK – Kit de ferramentas forenses da AccessData:** poderoso programa de análise digital que processa e indexa dados de uma variedade de fontes e formatos. Ele permite aos peritos obter uma imagem forense de um computador e, ao final, processá-la. Uma vez processado, um examinador pode realizar pesquisas, filtrar dados e visualizar dados excluídos. O FTK é frequentemente usado para selecionar dados antes da ingestão em plataformas de descoberta eletrônica, como o Relativity. O FTK é capaz de reportar descobertas no formato Excel, PDF, HTML e muito mais. É incrivelmente poderoso, versátil e uma das ferramentas preferidas do setor.

**FTK Imager:** *software* de imagem gratuito e muito poderoso, porém leve. Geralmente colocado em uma unidade externa e conectado ao computador de evidências, o FTK Imager é capaz de criar imagens em vários formatos da maioria dos dispositivos. Ao criar imagens remotas, enviamos a unidade externa com o FTK Imager, juntamente com o software de acesso remoto. O FTK Imager pode criar imagens verificadas lógicas, físicas e direcionadas nos formatos .E01 e .AD1. O FTK Imager também pode abrir, navegar e montar imagens ou visualizar o espaço excluído em uma unidade ou imagem.

**Griffeye:** nova ferramenta de software forense que processa dados e permite análises inteligentes por meio do uso de analisadores personalizados e reconhecimento de foto com inteligência artificial. Oferece várias ferramentas analíticas personalizadas dentro da plataforma.

***Hash:*** identificador numérico exclusivo gerado por um algoritmo matemático para verificar se uma imagem é idêntica à mídia de origem (*hash* verificado). Depois que uma imagem é concluída, a próxima etapa do processo é a verificação de *hash* para garantir que a imagem forense contenha uma cópia exata dos dados que estão sendo copiados. O primeiro *hash* é gerado contra a evidência e um segundo *hash* é gerado contra a imagem forense concluída. No final do processo de criação de imagens, os dois *hashes* são comparados. Se os *hashes* corresponderem, a imagem é verificada e garantida. Um *hash* pode ser calculado usando muitos algoritmos diferentes, como MD5, SHA1 e SHA256.

**iChat:** permite que o iMessages seja enviado para iPhones e iPads (dispositivos iOS 5), além de trabalhar nas mesmas listas de amigos. O iChat sincroniza com dispositivos Apple vinculados ao mesmo AppleID. Isso permite que um usuário acesse o iMessages de seu telefone em um MacBook. O iChat geralmente arquiva as mensagens, persistindo após a exclusão em outros dispositivos.

**iCloud:** plataforma de *backup* em nuvem para dispositivos Apple. O iCloud possui os três *backups* mais recentes para dispositivos vinculados a um AppleID.

**Imagem direcionada:** cópia direcionada de pastas e/ou arquivos específicos. Assim como uma imagem lógica, uma imagem direcionada captura dados vivos e não excluídos. Isso geralmente é usado quando é necessário preservar arquivos específicos em um computador sem coletar todo o disco rígido. Isso resulta em um processo de imagem muito mais rápido.

**Imagem física:** cópia direta bit a bit 1: 1 de um dispositivo de armazenamento físico. Inclui todos os arquivos, pastas, espaço não alocado, espaço livre e espaço livre. Inclui arquivos ao vivo e excluídos. Imagens físicas são o tipo mais comum de imagem em computadores e unidades. É muito incomum quando se lida com telefones celulares. As imagens físicas geralmente têm o formato .E01 quando compactadas (mais comuns) ou .001, .BIN, .dd (não compactadas – cada vez mais incomum). Os arquivos .BIN são comuns ao lidar com imagens físicas de telefones celulares.

**Imagem lógica:** cópia forense de todos os dados "ativos" – ou não excluídos – em um disco rígido ou outra mídia. Normalmente, uma imagem lógica captura o que você veria ao navegar no seu computador. Tipicamente, espaço livre, arquivos excluídos e fragmentos não serão capturados. Por exemplo, ao criar uma imagem lógica de um computador com um disco rígido de 500 GB e 100 GB em uso para armazenar arquivos, a imagem resultante será 100 GB descompactada – apenas captura o espaço em uma mídia de armazenamento em uso.

**Imagem:** cópia forense verificada dos dados digitais. Geralmente compactada e criada usando várias ferramentas, dependendo do dispositivo. Às vezes chamada de aquisição, coleção ou extração. Uma imagem é comumente observada no formato .E01 devido ao amplo suporte para o formato. Uma imagem pode ser vista como um contêiner que contém e protege todos os dados extraídos de um dispositivo. Pode ser protegida por senha. As imagens podem ser segmentadas em partes especificadas (geralmente dividimos nossas imagens .E01 em segmentos de 2 GB).

**IMEI:** (*International Mobile Equipment Identity*) é um código exclusivo de 17 ou 15 dígitos usado para identificar um telefone celular individual em uma rede. O número IMEI é exclusivo para o celular.

**iMessage:** é um serviço de mensagens instantâneas criado e implementado pela Apple para dispositivos Apple. As iMessages geralmente são sincronizadas nos dispositivos Apple em uso pelo mesmo AppleID. Compartilham um banco de dados com mensagens SMS / MMS em dispositivos iOS. Nos relatórios, as mensagens são vinculadas às conversas por IDs de bate-papo.

***Jailbreak:*** modificação de um dispositivo móvel para remover as restrições impostas pelo fabricante ou operador. Permite a instalação de *software* não autorizado. Esse termo geralmente é usado ao descrever a modificação de dispositivos iOS. Um dispositivo iOS com *jailbreak* dará ao examinador acesso a mais dados.

**LCD:** é um painel atrás do vidro e do digitalizador em um dispositivo móvel que cria a tela. Se a evidência for descrita como danificada sem imagem / tela, o LCD poderá ser substituído.

**Limpeza remota (*remote wipe*):** os dispositivos Android e Apple podem ser limpos remotamente por meio do GooglePlay.com e iCloud.com. Isso pode ser feito efetuando login na conta do Google ou AppleID vinculada ao dispositivo. Os locais dos dispositivos conectados a essas contas podem ser rastreados e apagados ou bloqueados remotamente com o acionamento de um botão.

**Máquinas virtuais (ou *Virtual Machines* – VM):** as VMs podem ser adquiridas de duas maneiras. Primeira: dentro da VM, usando software de imagem forense, como o FTK Imager. Segunda: fora da VM, preservando o valor real.

**MD5:** algoritmo de *hash*. Seu uso não é o mais indicado, devendo, sempre que possível, ser usado o SHA256, ou superior. O seu sumário possui um tamanho de 128 bits.

**Mensagem de bate-papo:** mensagem trocada usando um aplicativo de terceiros como WhatsApp, Skype, Snapchat, Facebook Messenger etc. As ferramentas de análise forense geralmente separam SMS / MMS das mensagens de bate-papo. As mensagens de bate-papo residem em bancos de dados exclusivos vinculados ao aplicativo de terceiros.

**Microsoft Exchange:** servidor de e-mail e servidor de calendário desenvolvidos pela Microsoft. O e-mail do Exchange é armazenado nos bancos de dados .EDB. Esses arquivos .EDB podem ser preservados de servidores Exchange off-line. Ao executar uma imagem ao vivo de um servidor Exchange em execução, o banco de dados .EDB ficará inacessível. Por esse motivo, é melhor trabalhar com o departamento de TI da empresa. Exportar caixas de correio solicitadas usando o PowerShell ou um utilitário de *front-end* do Exchange que permita exportações.

**Microsoft Office365:** serviço on-line que fornece e-mail, armazenamento em nuvem, SharePoint, Skype, Office etc. O e-mail do Office365 pode ser coletado criando exportações de caixas de correio por meio de uma conta de administrador. Os dados exportados podem ser filtrados por caixa de correio e data. Várias caixas de correio podem ser exportadas ao mesmo tempo, permitindo que uma coleção do e-mail do Office365 de uma empresa inteira comece em alguns minutos.

**Mídia de armazenamento:** tudo o que armazena dados digitais – unidades *flash*, discos rígidos, CDs, DVDs, cartões SD e mais se enquadram nessa categoria (unidade, disco, disco). Os dados podem ser armazenados e recuperados.

**MMS:** mensagem multimídia. Como o SMS, uma mensagem MMS é enviada e recebida pela rede de uma operadora de telefone. As mensagens MMS contêm anexos como fotos, vídeo e áudio. SMS e MMS compartilham um banco de dados.

**Mobile Phone Examiner (MPE) da AccessData:** MPE é a resposta da AccessData à Cellebrite. Devido ao domínio da Cellebrite no mercado forense de telefonia móvel, muitas outras ferramentas dedicadas ficam aquém. O MPE, como outros concorrentes da Cellebrite, não suporta quase tantos dispositivos nem analisa tantos aplicativos quanto a Cellebrite.

**Montagem:** processo de obter uma imagem ou unidade forense e carregá-la no ambiente Windows por meio de uma ferramenta de montagem com a finalidade de gerar ou revisar imagens. Por exemplo, uma imagem de um computador pode ser montada e seu conteúdo navegado.

**Nuvem:** armazenamento remoto acessado via *web*. A maioria dos provedores de armazenamento em nuvem tem algum tipo de log de atividades disponível para assinantes premium. O conteúdo armazenado nas contas da nuvem pode ser sincronizado com um dispositivo como uma unidade externa e gravado ou coletado usando uma ferramenta forense.

**Partição:** seção de um disco usado para armazenar dados. Um único disco rígido pode ser dividido em várias partições. Cada partição geralmente serve a um propósito distinto. O Windows normalmente divide um disco rígido em várias partições: Inicialização, SO e Recuperação. Cada partição é independente das outras.

**ROM em dispositivos móveis:** memória somente leitura. A ROM armazena o sistema operacional dos dados do sistema telefônico.

***Rooting:*** de forma similar a um *jailbreak*, o *root* de um telefone celular fornece acesso a dados na "raiz" ou no nível mais alto do sistema de arquivos do telefone móvel. É equivalente a um *jailbreak*, mas possui algumas diferenças, sendo que esse termo (*rooting*) é usado quando se refere a modificação de dispositivos Android.

**Samsung *Backup*:** plataforma de backup da Samsung. Armazena mensagens, contatos, fotos etc.

**Servidor:** computador usado para compartilhar dados em uma rede com outros computadores (clientes). Os servidores geralmente têm uma capacidade de armazenamento muito maior. Devido à grande capacidade da maioria dos servidores e à necessidade ocasional de criar uma imagem de um servidor em uma rede, os tempos de criação de imagens são extremamente maiores. A imagem é executada em segundo plano e tem um impacto mínimo nos usuários que acessam dados em um servidor. Quando uma imagem do servidor for concluída, será gerada uma lista de exceções que fornece uma lista de arquivos que não puderam ser gerados em imagens. Eles podem ser tentados novamente como uma imagem menor separada, desde que os arquivos sejam fechados e não sejam utilizados por ninguém na rede.

**SHA1:** algoritmo de *hash*. Seu uso não é o mais indicado, devendo sempre que possível ser usado o SHA256, ou superior. O seu sumário possui tamanho de 160 bits.

**SHA256:** algoritmo de *hash*. Comumente usado e atualmente o mais recomendado. O seu sumário possui tamanho de 256 bits.

**SIFT:** ao contrário de vários dos programas listados aqui, o SIFT é um sistema operacional inteiro que roda no Linux, e desenvolvido pelo SANS Institute. É composto por várias ferramentas gratuitas e é popular entre as agências policiais e o setor privado.

**Sistema de arquivos:** usado para controlar como os dados são armazenados e recuperados em uma mídia de armazenamento. Frequentemente responsável por manter os metadados, como datas e local da criação.

**SMS:** mensagem curta ou comumente conhecida como mensagens de texto. O SMS normalmente é enviado e recebido pela rede de uma operadora de telefone usando o número de telefone do assinante. SMS e MMS compartilham um banco de dados.

**SSD M2:** unidade de estado sólido ainda mais rápido, usado para armazenamento em laptops e computadores. Alguns computadores, incluindo *laptops*, terão um único *stick* SSD M2 e um pequeno disco rígido de 2,5. Os MacBooks mais novos e sofisticados usam drives SSD.

**SSD:** unidade de estado sólido. 2,5 polegadas. Usa armazenamento de estado sólido em oposição a um disco magnético giratório. Conexão SATA. Sem partes móveis. As imagens no SSD são sempre mais rápidas.

**Suíte forense da Oxygen:** programa forense de dispositivos móveis. Geralmente com menos recursos em comparação com a Cellebrite, o Oxygen é capaz de extrair e analisar dispositivos móveis. Oxygen extrai os dados do telefone móvel no formato .OFB, que geralmente são convertidos para um formato compatível com a Cellebrite.

***Tablet* PCs:** geralmente são adquiridos de forma forense pelos mesmos métodos que usamos para uma imagem ao vivo. Os tempos de criação de imagens no armazenamento de estado sólido dos *Tablet* PCs variam de 25 minutos a 1,5 horas, normalmente.

***Tablet*:** a maioria dos *tablets* usa o mesmo *firmware* encontrado em telefones celulares – Android e iOS. Os tempos de imagem são semelhantes aos dos telefones.

**Telefones celulares:** a maioria dos telefones celulares pode ser adquirida e analisada. A capacidade do telefone está sempre aumentando e a quantidade de dados que os usuários estão armazenando também. É melhor proteger um telefone celular por pelo menos um dia. A extração média de um telefone inteligente é de 2 horas, no entanto, em casos extremos, pode durar até 10 horas. Isso acontece quando vários tipos de extrações são necessários para analisar os dados do usuário.

**Unidade *Flash*:** pequena mídia externa utilizando armazenamento *flash*.

**Universal da Paraben:** Paraben é outra empresa que oferece várias ferramentas que coletam e analisam os dispositivos mais comuns. O Paraben Universal é o FTK da Paraben, oferecendo pesquisa, processamento e muito mais para os dispositivos mais comuns.

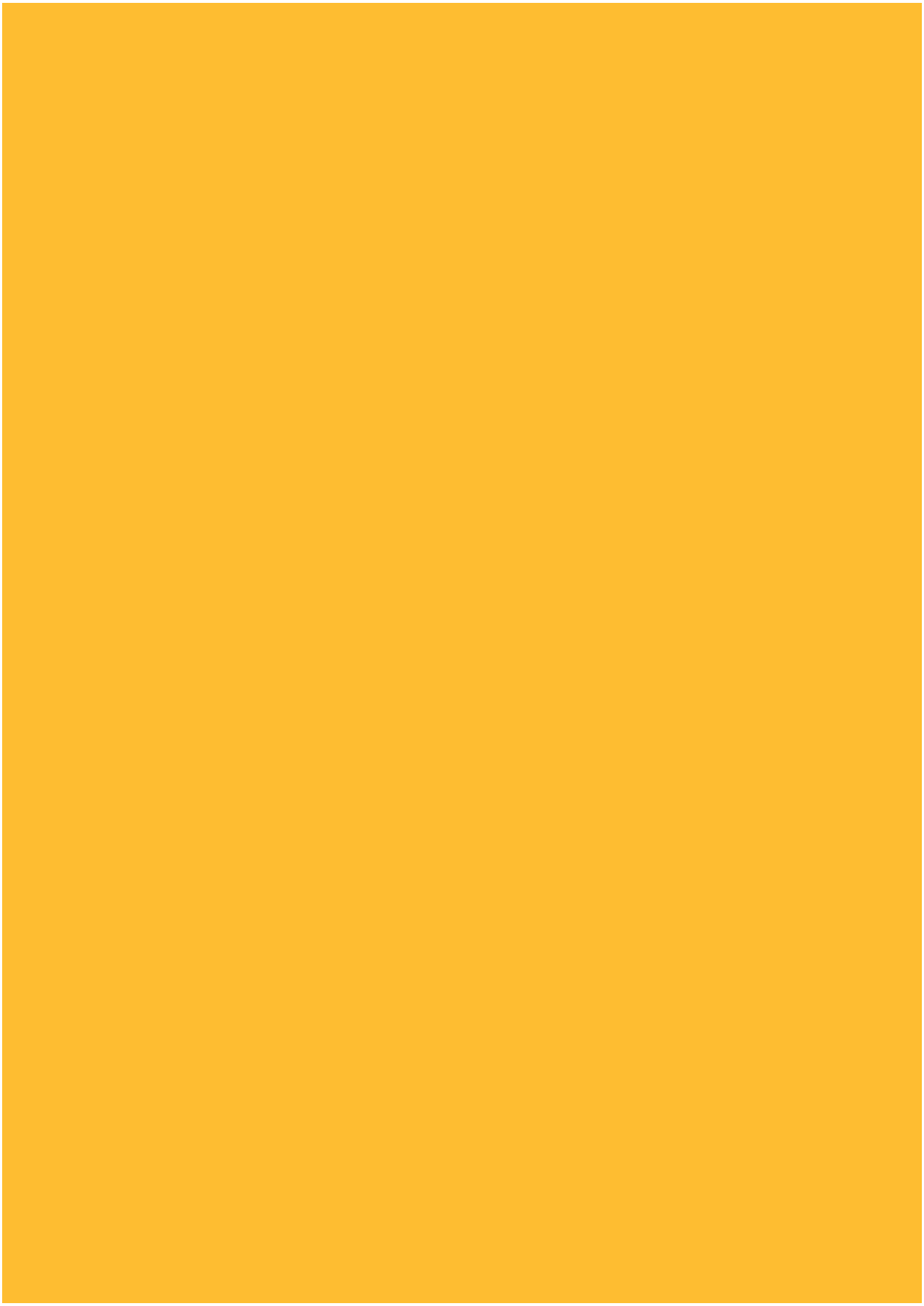
**Versão do *firmware* (Android):** versão do *firmware* em execução em um dispositivo móvel Android. O Android usa um número e uma sobremesa para expressar a versão. Por exemplo, a versão 8.0 do Android é Oreo e a versão anterior é 7.0 e Nougat.

**Versão do *firmware* (iOS):** versão do *firmware* em execução em um dispositivo móvel Apple. As atualizações de *firmware* da Apple têm uma base de instalação alta do usuário e variam entre diferentes dispositivos, versões e datas de lançamento.

***Webmail*:** quando o *webmail* é acessado por meio de um navegador da web, o e-mail enviado ou recebido não é armazenado no computador. Em vez disso, ele é carregado no servidor de *webmail* e visualizado no navegador. Dependendo do serviço de *webmail*, diferentes informações serão gravadas em vários artefatos do navegador da web. Às vezes, é possível determinar quais contas de *webmail* foram acessadas ou quais pastas foram visualizadas. Nem sempre é possível determinar quais e-mails foram visualizados, enviados ou recebidos.

**XRY:** um combo de *hardware* + *software*, o XRY é usado para extrair e analisar dados de dispositivos móveis, como Cellebrite e Oxygen.

**X-Ways:** outro conjunto forense completo, como o FTK e o EnCase, o X-Ways é capaz de processar dados digitais de várias fontes, porém possui menos recursos.



# REFERÊNCIAS

BRASIL. Superior Tribunal de Justiça. Processual Penal. Prova. Ilícita e ilegítima. Distinção. Ilegitimidade da prova na espécie. Nulidade. Não ocorrência. Desentranhamento dos autos. Desnecessidade. *Habeas Corpus* substitutivo de recurso ordinário. Ausência de flagrante ilegalidade. Não conhecimento. *Habeas Corpus* nº 213448 RS 2011/0165258-4. Relator: Ministro Sebastião Reis Júnior. **Diário de Justiça Eletrônico**, 13 set. 2013. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1208158&num_registro=201101652584&data=20130913&formato=PDF. Acesso em: 20 maio 2020.

BRASIL. Superior Tribunal de Justiça. Penal e Processual Penal. *Habeas Corpus* substitutivo de recurso ordinário. Utilização do remédio constitucional como sucedâneo de recurso. Não conhecimento do *writ*. Precedentes do supremo tribunal federal e do Superior Tribunal de Justiça. Quebra de sigilo telefônico e telemático autorizada judicialmente. Supressão de instância com relação a um dos pacientes. Presença de indícios razoáveis da prática delituosa. Indispensabilidade do monitoramento demonstrada pelo *modus operandi* dos delitos. Crimes punidos com reclusão. Atendimento dos pressupostos do art. 2º, i a iii, da lei 9.296/96. Legalidade da medida. Ausência de preservação da integralidade da prova produzida na interceptação telefônica e telemática. Violação aos princípios do contraditório, da ampla defesa e da paridade de armas. Constrangimento ilegal evidenciado. *Habeas Corpus* não conhecido. Ordem concedida, de ofício. *Habeas Corpus* nº 160.662 RJ 2010/0015360-8. Relatora Ministra Assusete Magalhães. **Diário de Justiça Eletrônico**, 17 mar. 2014. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1297583&num_registro=201000153608&data=20140317&formato=PDF. Acesso em: 20 maio 2020.

BRASIL. Superior Tribunal de Justiça. Penal e Processo Penal. Evasão de divisas. Dosimetria. Pena-base. Elevado montante evadido. Circunstância judicial negativa. Lei 12.850/13. Norma superveniente. Ausência de prequestionamento. Disco rígido. Acesso direto. Ilicitude. Inexistência. Recurso Especial nº 1435421 RS 2014/0029779-8. Relator: Ministra Maria Thereza de Assis Moura. **Diário de Justiça Eletrônico**, 25 jun. 2015. Disponível em: https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1411348&tipo=0&nreg=201400297798&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20150625&formato=PDF&salvar=false. Acesso em: 20 maio 2020.

CANCELA, A. G. **A prova digital:** os meios de obtenção de prova na Lei do Cibercrime. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Faculdade de Coimbra, Coimbra. Disponível em: https://core.ac.uk/download/pdf/43589323.pdf. Acesso em: 29 jan. 2021.

CAMARGO, Coriolano Almeida; CRESPO, Marcelo; SANTOS, Cleoberte. **Direito Digital:** Novas teses jurídicas. Rio de Janeiro: Editora Lumen Juris, 2019. v. 2.

MINISTÉRIO PÚBLICO FEDERAL MPF (Brasil). **Convenção sobre o Cibercrime.** Budapeste, 23 de novembro de 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 27 out. 2018.

PINHEIRO, Patrícia Peck. **Direito digital.** 5. ed. São Paulo: Saraiva, 2013.

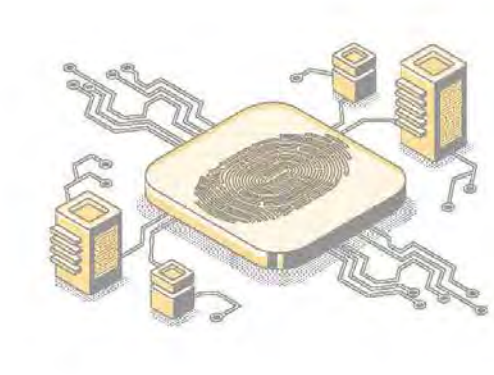
RAFFUL, Leonardo José; RAFFUL, Ana Cristina. Prova eletrônica. **Revista do Direito Público**, v. 12, n. 2, p. 48-76, 2017. Disponível em: http://www.uel.br/revistas/uel/index.php/direitopub/article/view/26212. Acesso em: 29 jan. 2021.

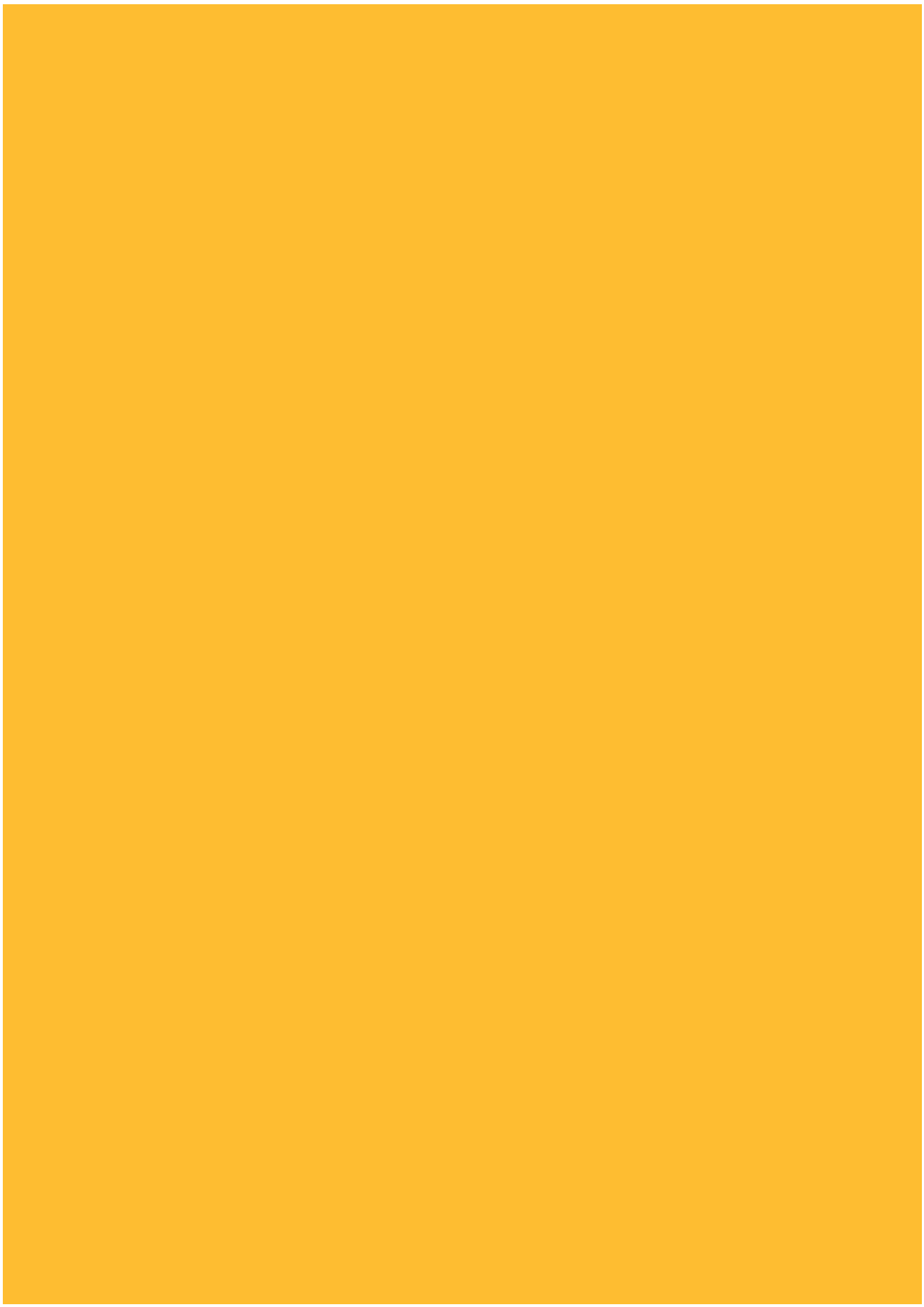
SANCHES, Rogério Cunha. **Pacote Anticrime – Lei 13.964/2019:** Comentários às alterações no CP, CPP e LEP. Salvador: Editora Juspodium, 2020.

VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/en.php. Acesso em: 29 jan. 2020.

VELHO, Jesus Antonio *et al.* **Tratado de Computação Forense.** São Paulo: Millenium Editora, 2016.

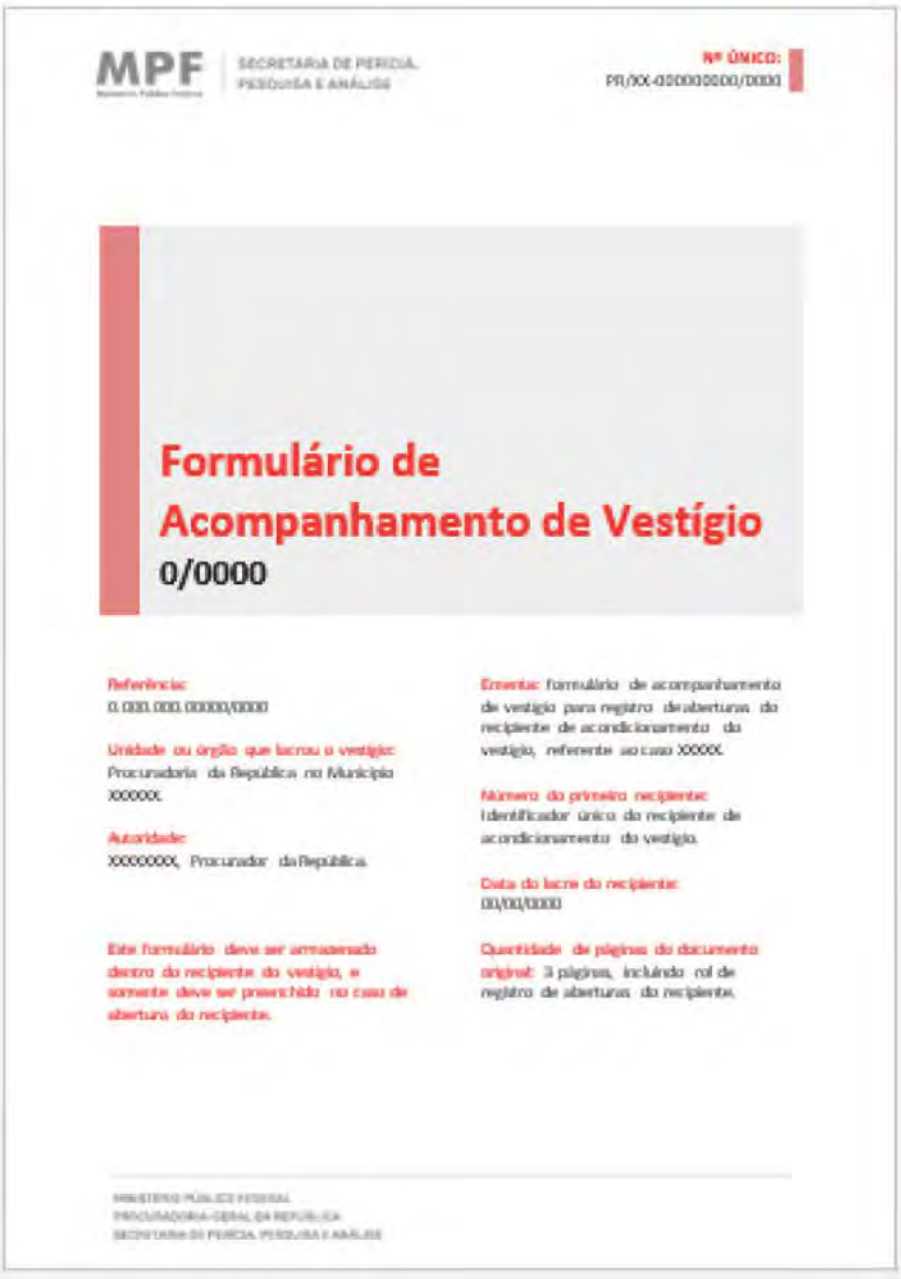
VELHO, Jesus Antonio; GEISER, Gustavo Caminoto; ESPÍNDULA, Alberi. **Ciências forenses.** Uma Introdução às principais áreas da Criminalística Moderna. v. 2, 2013. Disponível em: https://www.editorajuspodivm.com.br/cdn/arquivos/73f8a7f6a6ecf236cd8d86d310533974.pdf. Acesso em: 29 jan. 2021.





# APÊNDICES

## FORMULÁRIOS DA CADEIA DE CUSTÓDIA



MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

Nº ÚNICO:
PR/XX-000000000/0000

**Formulário de Acompanhamento de Vestígio**
**0/0000**

Referência:
0.000.000.00000/0000

Unidade ou órgão que lacrou o vestígio:
Procuradoria da República no Município XXXXXX

Autoridade:
XXXXXXXX, Procurador da República

Este formulário deve ser armazenado dentro do recipiente do vestígio, e somente deve ser preenchido no caso de abertura do recipiente.

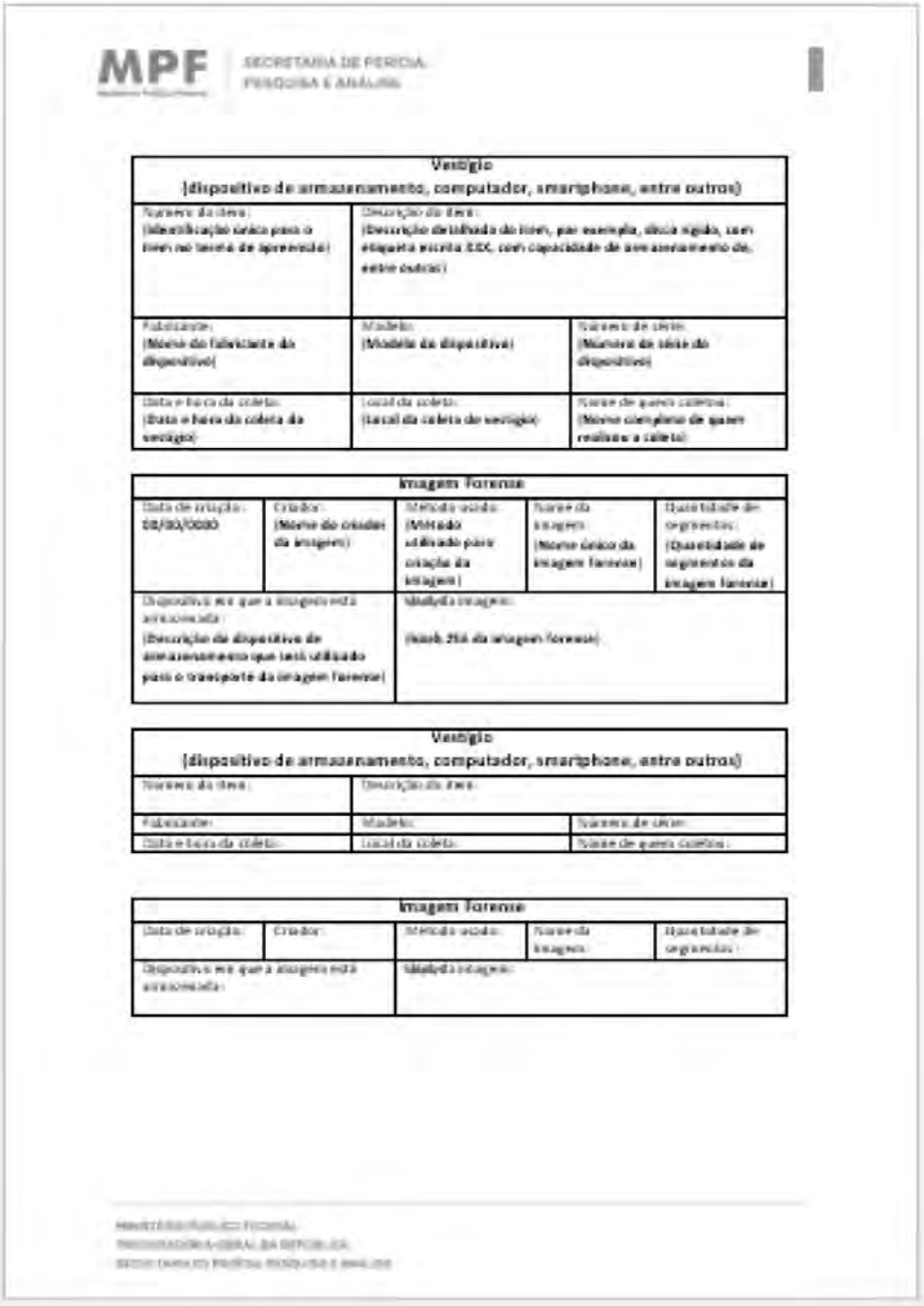
Ementa: formulário de acompanhamento de vestígio para registro de aberturas do recipiente de acondicionamento do vestígio, referente ao caso XXXXX.

Número do primeiro recipiente:
Identificador único do recipiente de acondicionamento do vestígio.

Data do lacre do recipiente:
00/00/0000

Quantidade de páginas do documento original: 3 páginas, incluindo rol de registro de aberturas do recipiente.

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE



MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Vestígio<br>(dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item:<br>(Identificação única para o item no termo de apreensão) | Descrição do item:<br>(Descrição detalhada do item, por exemplo, única rígida, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outros) | |
| Fabricante:<br>(Nome do fabricante do dispositivo) | Modelo:<br>(Modelo do dispositivo) | Número de série:<br>(Número de série do dispositivo) |
| Data e hora da coleta:<br>(Data e hora da coleta do vestígio) | Local da coleta:<br>(Local da coleta do vestígio) | Nome de quem coletou:<br>(Nome completo de quem realizou a coleta) |

| Imagem forense | | | | |
|---|---|---|---|---|
| Data de criação:<br>00/00/0000 | Criador:<br>(Nome do criador da imagem) | Método usado:<br>(Método utilizado para criação da imagem) | Nome da imagem:<br>(Nome único da imagem forense) | Quantidade de segmentos:<br>(Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada:<br>(Descrição do dispositivo de armazenamento que está utilizado para o transporte da imagem forense) | | Validade imagem:<br>(hash 256 da imagem forense) | | |

| Vestígio<br>(dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: | Descrição do item: | |
| Fabricante: | Modelo: | Número de série: |
| Data e hora da coleta: | Local da coleta: | Nome de quem coletou: |

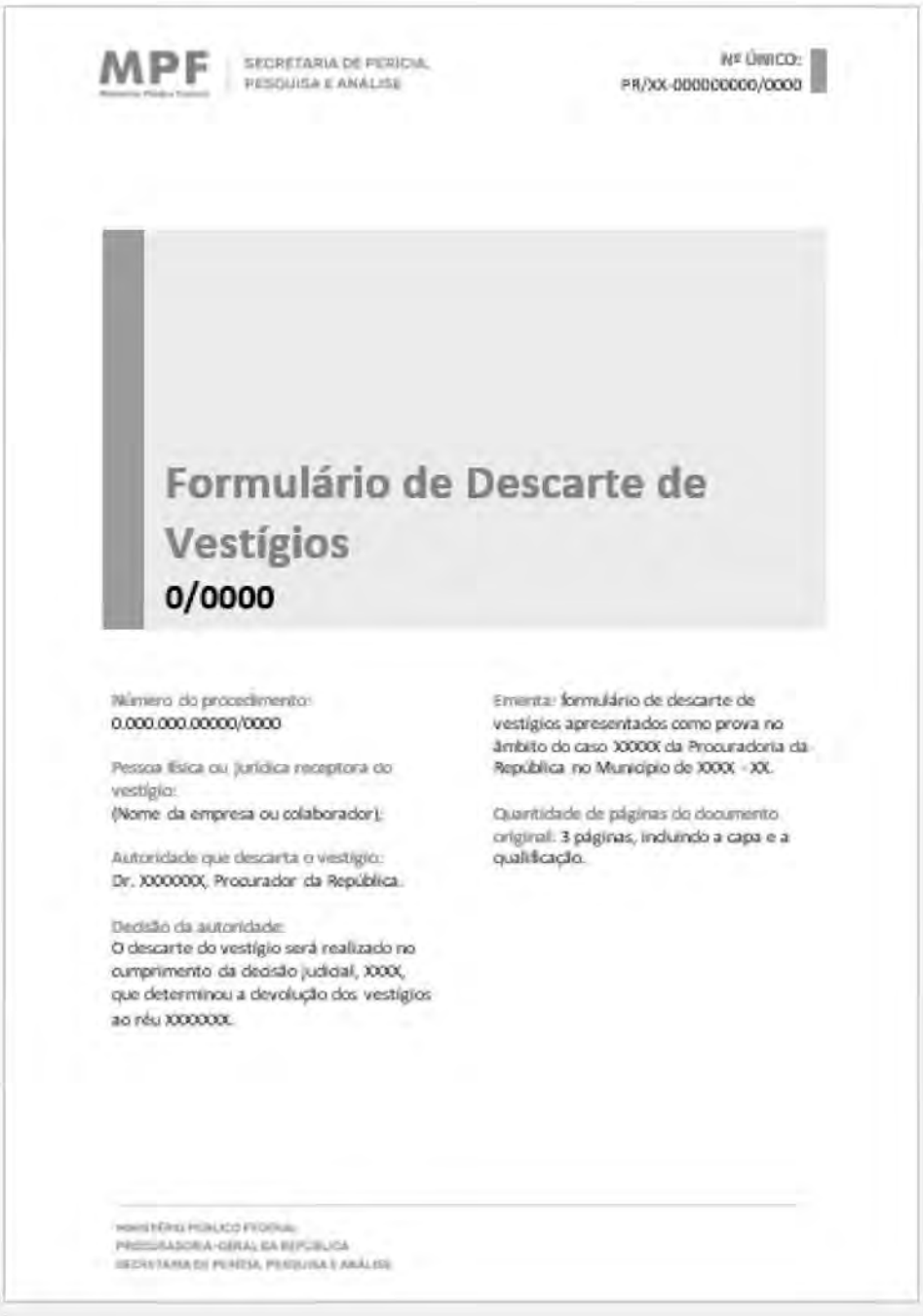
| Imagem forense | | | | |
|---|---|---|---|---|
| Data de criação: | Criador: | Método usado: | Nome da imagem: | Quantidade de segmentos: |
| Dispositivo em que a imagem está armazenada: | | Validade imagem: | | |

MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

**Registro de abertura do recipiente do vestígio**
(Sempre incluir o lacre violado dentro do novo recipiente)

| Abertura | Data/Hora | Quem abriu: | Números dos lacres: | Finalidade: |
|---|---|---|---|---|
| 1 | Data: 08/03/2021 | Nome: (Nome da pessoa que abriu o recipiente lacrado) | Número do lacre violado: (Identificação única do recipiente aberto) | (Descrição sucinta do motivo da abertura do recipiente do vestígio, por exemplo, para realizar exame pericial) |
| | Hora: 08:00 | Cargo e matrícula: (Cargo e matrícula da pessoa que abriu o recipiente lacrado) | Número do novo lacre: (Identificação única do novo recipiente que será utilizado) | |
| | Local: (Local da abertura do recipiente) | Assinatura: (Assinatura da pessoa que abriu o lacre) | Observação: (Alguma observação sobre abertura ou novo lacre, caso seja necessário) | |
| Abertura | Data/Hora | Quem abriu: | Números dos lacres: | Finalidade: |
| 2 | Data: | Nome: | Número do lacre violado: | |
| | Hora: | Cargo/matrícula: | Número do novo lacre: | |
| | Local: | Assinatura: | Observação: | |
| Abertura | Data/Hora | Quem abriu: | Números dos lacres: | Finalidade: |
| 3 | Data: | Nome: | Número do lacre violado: | |
| | Hora: | Cargo/matrícula: | Número do novo lacre: | |
| | Local: | Assinatura: | Observação: | |

PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE



MPF SECRETARIA DE PERICIA, PESQUISA E ANÁLISE

Nº ÚNICO:
PR/XX-00000000/0000

# Formulário de Descarte de Vestígios
## 0/0000

Número do procedimento:
0.000.000.00000/0000

Pessoa física ou jurídica receptora do vestígio:
(Nome da empresa ou colaborador).

Autoridade que descarta o vestígio:
Dr. XXXXXXX, Procurador da República.

Decisão da autoridade:
O descarte do vestígio será realizado no cumprimento da decisão judicial, XXXX, que determinou a devolução dos vestígios ao réu XXXXXXX.

Ementa: formulário de descarte de vestígios apresentados como prova no âmbito do caso XXXXX da Procuradoria da República no Município de XXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e a qualificação.

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: (Identificação única para o item no termo de apreensão) | Descrição do item: (Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outros) | |
| Fabricante: (Nome do fabricante do dispositivo) | Modelo: (Modelo do dispositivo) | Número de série: (Número de série do dispositivo) |
| Data e hora da coleta: (Data e hora da coleta do vestígio) | Local da coleta: (Local da coleta do vestígio) | Nome de quem coletou: (Nome completo de quem realizou a coleta) |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: 00/00/0000 | Criador: (Nome do criador da imagem) | Método usado: (Método utilizado para criação da imagem) | Nome da imagem: (Nome único da imagem forense) | Quantidade de segmentos: (Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada: (Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense) | | Hash da imagem: (Hash 256 da imagem forense) | | |

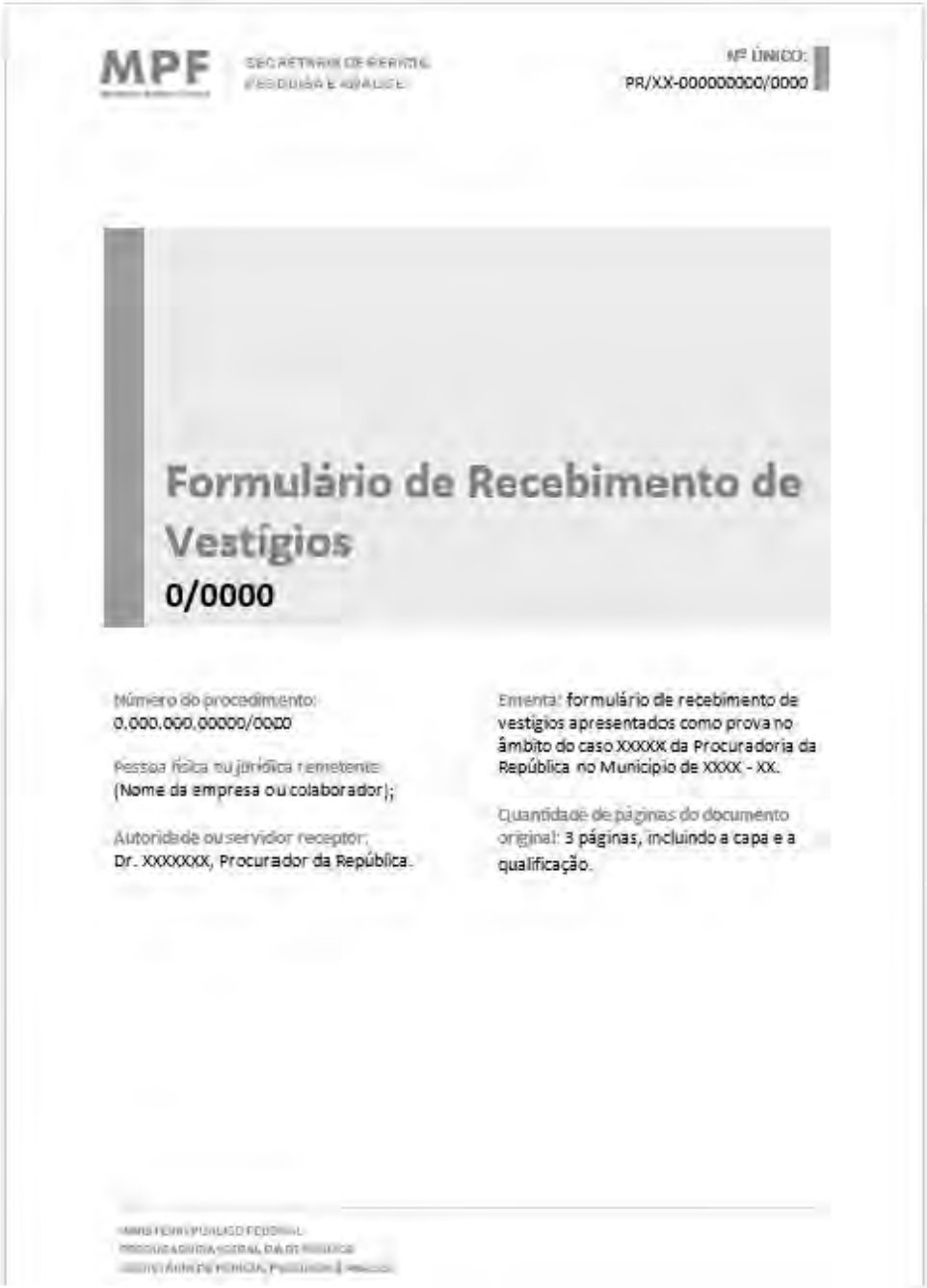
| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: | Descrição do item: | |
| Fabricante: | Modelo: | Número de série: |
| Data e hora da coleta: | Local da coleta: | Nome de quem coletou: |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: | Criador: | Método usado: | Nome da imagem: | Quantidade de segmentos: |
| Dispositivo em que a imagem está armazenada: | | Hash da imagem: | | |

MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Qualificação de quem descarta (Membro ou servidor que descarta o vestígio): | |
|---|---|
| Nome completo: | (Nome completo do Membro ou servidor) |
| Matrícula: | (Matrícula do Membro ou servidor) |
| Cargo: | (Nome do cargo) |
| Local / Data: | (Local e data de assinatura do documento) |
| Assinatura:<br>Documento com assinatura digital. | |

| Qualificação do receptor do vestígio (quem está recebendo o vestígio descartado): | |
|---|---|
| Nome completo (pessoa física ou jurídica): | (Razão social da empresa) |
| Endereço: | (Endereço completo da empresa) |
| CPF/CNPJ: | 00.000.000/0000-00 (número do CNPJ da empresa ou CPF da pessoa física) |
| Nome do advogado: | (Nome completo do advogado) |
| CPF do advogado: | 000.000.000-00 (número do CPF) |
| OAB: | 0000-XX (número da OAB) |
| Local / Data: | (local e data de assinatura do documento) |
| Assinatura:<br>Documento com assinatura digital. | |



MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

Nº ÚNICO:
PR/XX-000000000/0000

# Formulário de Recebimento de Vestígios

## 0/0000

Número do procedimento:
0.000.000.00000/0000

Pessoa física ou jurídica remetente:
(Nome da empresa ou colaborador);

Autoridade ou servidor receptor:
Dr. XXXXXXX, Procurador da República.

Ementa: formulário de recebimento de vestígios apresentados como prova no âmbito do caso XXXXX da Procuradoria da República no Município de XXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e a qualificação.

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: (Identificação única para o item no termo de apreensão) | Descrição do item: (Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras) | |
| Fabricante: (Nome do fabricante do dispositivo) | Modelo: (Modelo do dispositivo) | Número de série: (Número de série do dispositivo) |
| Data e hora da coleta: (Data e hora da coleta do vestígio) | Local da coleta: (Local da coleta do vestígio) | Nome de quem coletou: (Nome completo de quem realizou a coleta) |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: 00/00/0000 | Criador: (Nome do criador da imagem) | Método usado: (Método utilizado para criação da imagem) | Nome da imagem: (Nome único da imagem forense) | Quantidade de segmentos: (Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada: (Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense) | | Hash da imagem: (Hash 256 da imagem forense) | | |

| Vestígio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: | Descrição do item: | |
| Fabricante: | Modelo: | Número de série: |
| Data e hora da coleta: | Local da coleta: | Nome de quem coletou: |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: | Criador: | Método usado: | Nome da imagem: | Quantidade de segmentos: |
| Dispositivo em que a imagem está armazenada: | | Hash da imagem: | | |

MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Qualificação do remetente (quem está entregando o vestígio): | |
|---|---|
| Nome completo: (pessoa física ou jurídica): | (Razão social da empresa) |
| Endereço: | (Endereço completo da empresa) |
| CPF/CNPJ: | 00.000.000/0000-00 (número do CNPJ da empresa ou CPF da pessoa física) |
| Nome do advogado: | (Nome completo do advogado) |
| CPF do advogado: | 000.000.000-00 (número do CPF) |
| OAB: | 0000-XX (número da OAB) |
| Local / Data: | (local e data de assinatura do documento) |
| Assinatura: Documento com assinatura digital. | |

| Qualificação do receptor (Membro ou servidor que recebe o vestígio): | |
|---|---|
| Nome completo: | (Nome completo do Membro ou servidor) |
| Matrícula: | (Matrícula do Membro ou servidor) |
| Cargo: | (Nome do cargo) |
| Local / Data: | (Local e data de assinatura do documento) |
| Assinatura: Documento com assinatura digital. | |

MPF SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

Nº ÚNICO:
PR/XX-000000000/0000

# Formulário de Transporte de Vestígios
## 00/0000

Referência:
0.000.000.00000/0000

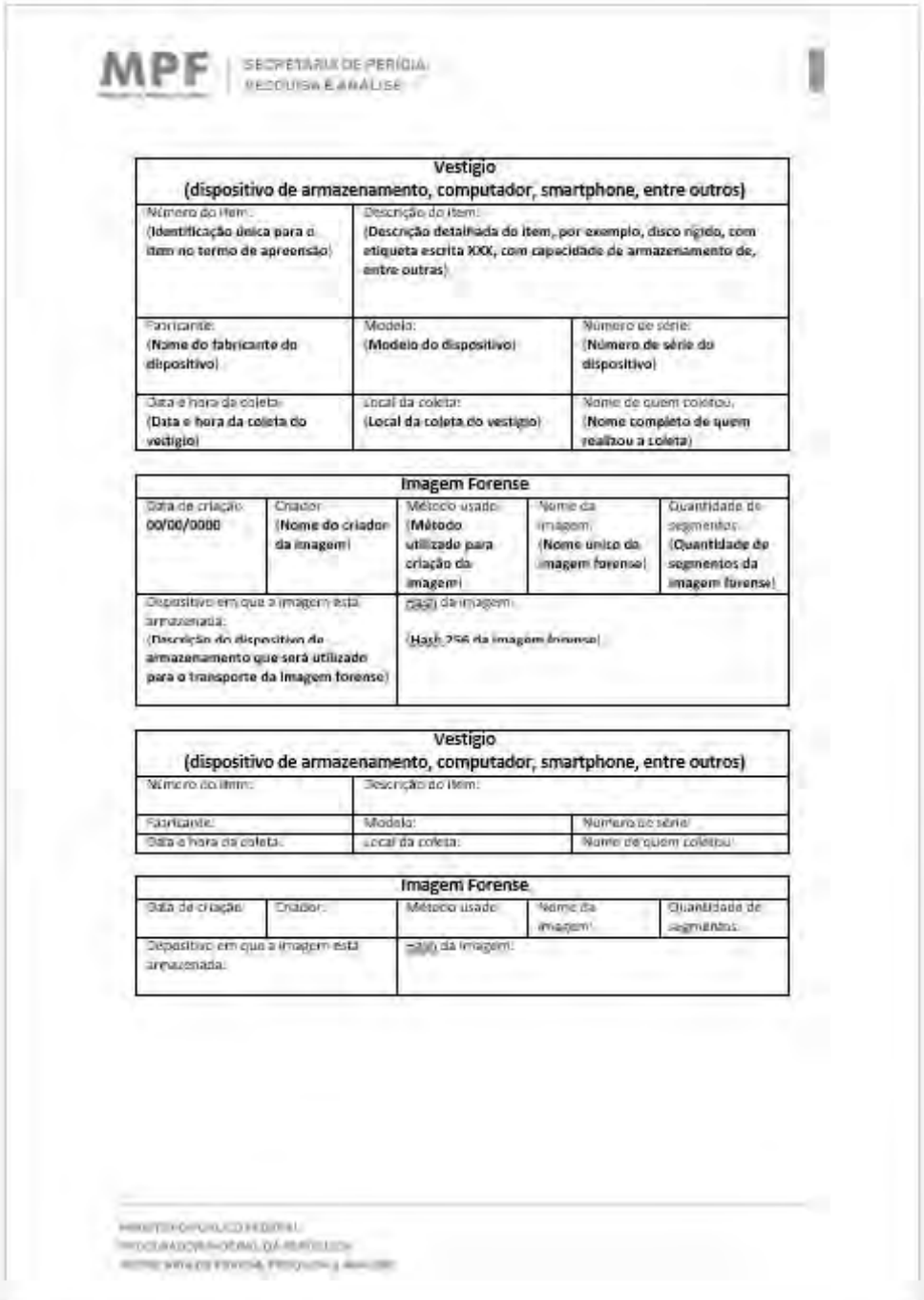
Unidade ou órgão remetente:
Procuradoria da República no Município de XXXXXX – XX.

Autoridade Requerente:
XXXXXXXX, Procurador da República.

Ementa: formulário de transporte de vestígio para exames periciais de uma unidade de disco rígido de 1TB (Terabyte) e instrução processual, referente ao caso XXXX da Procuradoria da República no Município de XXXXX - XX.

Quantidade de páginas do documento original: 3 páginas, incluindo a capa e o rol de assinaturas da cadeia de custódia

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA
SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE



MPF | SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE

| Vestigio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: (Identificação única para o item no termo de apreensão) | Descrição do item: (Descrição detalhada do item, por exemplo, disco rígido, com etiqueta escrita XXX, com capacidade de armazenamento de, entre outras) | |
| Fabricante: (Nome do fabricante do dispositivo) | Modelo: (Modelo do dispositivo) | Número de série: (Número de série do dispositivo) |
| Data e hora da coleta: (Data e hora da coleta do vestígio) | Local da coleta: (Local da coleta do vestígio) | Nome de quem coletou: (Nome completo de quem realizou a coleta) |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: 00/00/0000 | Criador: (Nome do criador da imagem) | Método usado: (Método utilizado para criação da imagem) | Nome da imagem: (Nome único da imagem forense) | Quantidade de segmentos: (Quantidade de segmentos da imagem forense) |
| Dispositivo em que a imagem está armazenada: (Descrição do dispositivo de armazenamento que será utilizado para o transporte da imagem forense) | Hash da imagem: (Hash 256 da imagem forense) | | | |

| Vestigio (dispositivo de armazenamento, computador, smartphone, entre outros) | | |
|---|---|---|
| Número do item: | Descrição do item: | |
| Fabricante: | Modelo: | Número de série: |
| Data e hora da coleta: | Local da coleta: | Nome de quem coletou: |

| Imagem Forense | | | | |
|---|---|---|---|---|
| Data de criação: | Criador: | Método usado: | Nome da imagem: | Quantidade de segmentos: |
| Dispositivo em que a imagem está armazenada: | Hash da imagem: | | | |

MPF | SECRETARIA DE PERÍCIA PESQUISA E ANÁLISE

| Cadeia de Custódia | | | | |
|---|---|---|---|---|
| Passo | Data/Hora | Remetente: | Destinatário: | Motivo: |
| 1 | Data: 00/00/0000 | Nome: (Nome completo do remetente) | Nome: (Nome completo do destinatário) | (Descrição sucinta do motivo do transporte do vestígio, por exemplo, para realizar exame pericial) |
| | Hora: 00:00 | Cargo e matrícula/SIAPE: (Cargo e matrícula do remetente) | Cargo e matrícula/SIAPE: (Cargo e matrícula do destinatário) | |
| | Origem/Destino: (Local de origem e local de destino) | Assinatura: (Assinatura do remetente) | Assinatura: (Assinatura do destinatário) | |

| Cadeia de Custódia | | | | |
|---|---|---|---|---|
| Passo | Data/Hora | Remetente: | Destinatário: | Motivo: |
| 2 | Data: 00/00/0000 | Nome: (Nome completo do remetente) | Nome: (Nome completo do destinatário) | (Descrição sucinta do motivo do transporte do vestígio, por exemplo, para realizar exame pericial) |
| | Hora: 00:00 | Cargo e matrícula/SIAPE: (Cargo e matrícula do remetente) | Cargo e matrícula/SIAPE: (Cargo e matrícula do destinatário) | |
| | Origem/Destino: (Local de origem e local de destino) | Assinatura: (Assinatura do remetente) | Assinatura: (Assinatura do destinatário) | |

| Cadeia de Custódia | | | | |
|---|---|---|---|---|
| Passo | Data/Hora | Remetente: | Destinatário: | Motivo: |
| 3 | Data: 00/00/0000 | Nome: (Nome completo do remetente) | Nome: (Nome completo do destinatário) | (Descrição sucinta do motivo do transporte do vestígio, por exemplo, para realizar exame pericial) |
| | Hora: 00:00 | Cargo e matrícula/SIAPE: (Cargo e matrícula do remetente) | Cargo e matrícula/SIAPE: (Cargo e matrícula do destinatário) | |
| | Origem/Destino: (Local de origem e local de destino) | Assinatura: (Assinatura do remetente) | Assinatura: (Assinatura do destinatário) | |

MPF
Ministério Público Federal