2024

PROCEDIMENTOS OPERACIONAIS PADRÃO

PERÍCIA CRIMINAL

INFORMÁTICA FORENSE

VOLUME 5

MJSP

2024

PROCEDIMENTOS OPERACIONAIS PADRÃO

PERÍCIA CRIMINAL

INFORMÁTICA FORENSE

VOLUME 5

DSUSP

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Presidente da República
Luiz Inácio Lula da Silva

Ministro da Justiça e Segurança Pública
Ricardo Lewandowski

Secretário Executivo
Manoel Carlos de Almeida Neto

Secretário Nacional de Segurança Pública
Mario Luiz Sarrubbo

Diretora do Sistema Único de Segurança Pública
Isabel Seixas de Figueiredo

Coordenadora-Geral de Modernização Tecnológica
Beatriz Marques de Jesus Figueiredo

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
Secretaria Nacional de Segurança Pública
Diretoria do Sistema Único de Segurança Pública

2024

PROCEDIMENTOS OPERACIONAIS PADRÃO

PERÍCIA CRIMINAL

INFORMÁTICA FORENSE

VOLUME 5

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA
Diretoria do Sistema Único de Segurança Pública
Coordenação - Geral de Modernização Tecnológica
Esplanada dos Ministérios, Bloco “T”, Anexo 2, 5° andar, sala 506
Telefone de contato: (61) 2025.9125
E-mail: cgmtec.senasp@mj.gov.br

Disponível em http://portal.mj.gov.br

Tiragem: 2.000 exemplares

Impresso no Brasil

COORDENAÇÃO
Christhiane Pinto Cutrim e Liliane Pires (coordenadora suplente).

REVISÃO DE CONTEÚDO
Ana Vitória Botelho, Christhiane Pinto Cutrim, Fabio Ferreira Real, Franciele Prete Bento, Francisca Dieimes Braga Miguéis Rapini Cleto, Liliane Pires, Rafael Friedrich Davet.

INTEGRANTES DO GRUPO DE TRABALHO
Henrique Galperin, Leandro Benfica, Marcelo Caldeira Ruback, Priscilla Duarte Bittar, Ronivaldo Veloso Pugas, Vander Oliveira Jampaulo.

DIAGRAMAÇÃO E PROJETO GRÁFICO
Ana Vitória Botelho, Christhiane Pinto Cutrim, Gabriel Silva Araújo, Franciele Prete Bento, Priscilla Duarte Bittar.

IMPRESSÃO
Senappen e Equipe do Projeto (Re) Integro.

341.4331
P441 Perícia criminal : informática forense / coordenadoras, Christhiane Pinto Cutrim, Liliane Pires. – Brasília : Secretaria Nacional de Segurança Pública, 2024.
67 p. -- (Procedimentos operacionais padrão ; v. 5)

ISBN 978-85-5506-250-6

1. Perícia criminal - 2. Informática forense – 3. Investigação criminal. I. Cutrim, Christhiane Pinto (coord.). II. Pires, Liliane (coord.). Brasil. Secretaria Nacional de Segurança Pública. III. Título. IV. Série.

CDD

Elaborada por Luciene Maria Sousa CRB1-1655

Ficha catalográfica elaborada pelo Ministério da Justiça e Segurança Pública.

SUMÁRIO

05 — INFORMÁTICA FORENSE

APRESENTAÇÃO

A Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública (Senasp) publicou pela primeira vez, em 2013, procedimentos operacionais padronizados (POPs) dedicados exclusivamente às atividades periciais. Tal passo estabeleceu um marco na disseminação de boas práticas na perícia criminal nacional, objetivando a uniformização do processo de produção da prova técnica no país, contribuindo para a garantia dos direitos de todas e de todos os envolvidos em processos criminais, seja na condição de vítima, seja na condição de autor.

Dando continuidade a este trabalho e reconhecendo o avanço da área pericial nos últimos anos, a Senasp agora lança a série Procedimentos Operacionais Padrão - Perícia Criminal. Esta nova coleção foi coordenada pela Diretoria do Sistema Único de Segurança Pública e foi elaborada com a colaboração de representantes do Conselho Nacional dos Dirigentes de Polícia Científica (CONDPC), das associações de profissionais de perícia criminal, da própria Senasp e de conceituados especialistas nos temas abordados.

Os procedimentos operacionais padrão incluídos nesta publicação têm abrangência nacional e visam servir como referência para as Unidades Federativas, respeitando a diversidade das atividades periciais e a necessidade de adaptação às mais diversas realidades locais. O trabalho envolveu a atualização e a elaboração de 56 POPs, que foram validados e testados pelas perícias dos Estados e do Distrito Federal. Foram incluídas abordagens específicas para novos temas prioritários como o feminicídio e os crimes contra o meio ambiente. Além disso, nesta edição, para uma melhor organização, os documentos foram distribuídos em 10 volumes temáticos.

A Senasp expressa sua gratidão a todos os profissionais que contribuíram para esta publicação, essencial para a elucidação de crimes, especialmente os violentos. Em resposta às novas demandas identificadas durante a elaboração deste trabalho, planejamos atualizações e revisões futuras e constantes. Esperamos que estes POPs se tornem um guia confiável, promovendo a eficiência, a coesão e a força das atividades periciais em todo o país, fortalecendo com isso a proteção inegociável dos direitos humanos.

Mario Luiz Sarrubo
Secretario Nacional de Segurança Pública

EXAME PERICIAL DE MÍDIAS DE ARMAZENAMENTO COMPUTACIONAL

POP N° 5.01 - INFORMÁTICA FORENSE

EXAME PERICIAL DE MÍDIAS DE ARMAZENAMENTO COMPUTACIONAL

FINALIDADE

Orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em mídias de armazenamento computacional.

PÚBLICO ALVO

Peritos Criminais afetos à atividade deste POP.

1. ABREVIATURAS E SIGLAS

BIOS: Basic Input/Output System
JBOD: Just a Bunch of Disks
OCR: Optical Character Recognition
RAID: Array of Independent Disks
SATA: Serial Advanced Technology Attachment
SED: Self-encrypted Drives
USB: Universal Serial Bus

2. RESULTADOS ESPERADOS

- Padronização dos exames periciais de mídias de armazenamento computacional.

3. MATERIAIS E EQUIPAMENTOS

- Equipamento que permita a realização de duplicação dos dados.
- Mídias externas de inicialização com sistemas operacionais forenses, tais como: Kali e CAINE.

- Estação de trabalho pericial (hardware + software) que permita o processamento, análise dos dados e a elaboração do laudo e seus anexos.
- Acesso irrestrito à Internet e privilégios administrativos na estação de trabalho pericial.
- Mídia de armazenamento computacional com capacidade livre superior ao da mídia a ser examinada.
- Armazenamento computacional com capacidade suficiente para os resultados dos exames.
- Ferramentas e materiais para reparo de mídias de armazenamento computacional.

4. PROCEDIMENTOS

4.1. Ações Preliminares

Esta etapa tem como objetivo determinar a viabilidade de realização do exame e organizar o material recebido. Para tanto, deve-se:

- atentar-se ao fato de que os equipamentos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados no manuseio, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue, etc.) ou outros materiais contaminantes;
- antes do deslacre, conferir se a descrição dos materiais e identificadores (em especial o número de lacre) constantes em documentação associada está de acordo com os objetos recebidos. Havendo inconsistência, adotar os procedimentos definidos pelas normas locais;
- recomenda-se a captura de imagens dos materiais devidamente lacrados;
- deslacrar, realizar nova conferência do material com sua descrição na documentação associada;
- estando a mídia de armazenamento computacional instalada em um equipamento, removê-la, quando viável;
- registrar em qual interface específica (ex: número da porta SATA) a mídia estava conectada;
- identificar e individualizar todo o material.

4.2. Duplicação dos Dados

Esta etapa visa a duplicar os dados contidos na mídia original para uma mídia de trabalho de forma a garantir a preservação dos dados.

- O exame deve ser efetuado sobre a cópia. Somente em caso de inviabilidade de realização de cópia deve o exame ser realizado diretamente na mídia original.
- Caso a mídia não possa ser removida ou não haja ferramenta para conectar sua interface, a cópia pode ser realizada utilizando o equipamento original, por meio de uma mídia externa de inicialização com sistema operacional forense que monte as mídias do dispositivo periciado no modo somente leitura. A ordem de inicialização do sistema deve ser configurada na BIOS de modo a impedir a inicialização da mídia instalada no equipamento.
- Se o dispositivo estiver com defeitos que impeçam a duplicação dos dados e existam ferramentas, materiais e conhecimento técnico necessários, realizar o reparo do equipamento.
- Verificar, usando um bloqueador de escrita, se a mídia de armazenamento está criptografada e se depende do equipamento em que estava instalada para a decifragem.
    - Caso o equipamento original seja necessário para a decifragem, a duplicação a ser realizada deve ser a do tipo "mídia para mídia" (espelhamento bit a bit) e a mídia de destino deve ser reinserida no equipamento original para a tentativa de acesso aos dados criptografados. Deve-se sempre realizar a sanitização da mídia de destino nos espelhamentos do tipo "mídia para mídia" antes de seu uso, para evitar contaminação de dados previamente gravados.
        - Se for possível decifrar a mídia, seu conteúdo descriptografado deverá ser copiado integralmente (e não apenas os arquivos individuais) para uma mídia externa, caso tecnicamente viável.
- Recomenda-se o tipo de duplicação de dados "mídia para arquivo-imagem", em oposição ao tipo "mídia para mídia", devido à maior flexibilidade para se analisar diversas mídias simultaneamente e à maior facilidade para se manter a integridade dos dados.
- A duplicação pode ser feita de duas formas: por meio de equipamento forense específico para esse fim ou utilizando-se um computador. Neste último caso, é imperativo impedir que ocorra qualquer alteração nos dados da mídia original, utilizando-se bloqueadores de escrita por hardware ou software.
- Após a conclusão da duplicação, recomenda-se a verificação do hash da imagem duplicada comparando-o com o da mídia original. Isso pode ser feito de forma automática a depender da ferramenta utilizada.

4.3. Processamento dos dados

Esta etapa visa à preparação dos dados para a análise e inclui, a depender do interesse pericial e da disponibilidade de ferramentas, os seguintes procedimentos, dentre outros:

- recuperação de arquivos apagados;
- indexação de dados;
- categorização de arquivos (por exemplo, por tipo);
- cálculo de hashes;
- detecção de criptografia de arquivos;
- expansão de arquivos compostos (.zip, .pst);
- reconhecimento ótico de caracteres (OCR);
- uso de inteligência artificial para:
  - identificação de conteúdo de imagens e vídeos;
  - transcrição de áudio.

4.4. Análise dos dados

- Esta fase consiste no exame das informações processadas na fase anterior, a fim de identificar e selecionar vestígios relacionados ao escopo pericial. Em relação ao resultado pretendido, há tipicamente dois tipos de análise:

4.4.1. Extração direta de arquivos

- O objetivo deste tipo de análise é buscar, identificar, extrair e converter para um formato facilmente legível o maior número possível de dados que possam ser de interesse para as investigações. Esses dados são aqueles produzidos, copiados ou alterados pelos usuários, tais como mensagens de e-mail, documentos de texto, fotos, dados de navegação na Internet, etc.

4.4.2. Elucidação técnico-pericial

- Este tipo de análise é realizado quando se pretende o esclarecimento de alguma questão pontual técnico-pericial sobre o material encaminhado. Os quesitos devem ser os mais objetivos possíveis, sempre buscando delimitar bem a questão desejada, e deve ser fornecido o máximo de informações disponíveis sobre o assunto. A falta de informações que

delimitem claramente o trabalho a ser realizado implica em aumento considerável no tempo de atendimento da solicitação de perícia, visto que leva à necessidade de exame de um universo maior de arquivos e dados. O Perito Criminal, assim, foca suas buscas em arquivos específicos, correlacionando os vestígios encontrados e elaborando conclusões precisas.

- Exemplos deste tipo de exame:
  - esclarecer se um determinado arquivo foi enviado ou recebido pelo usuário do computador examinado;
  - determinar quando o computador foi utilizado pela última vez;
  - determinar quais arquivos foram acessados pelo usuário mais recentemente;
  - determinar a existência de programas maliciosos.

4.5. Tratamento de dados criptografados

- Caso sejam identificados arquivos, pastas, volumes ou discos criptografados, é possível utilizar alguns métodos para se tentar descriptografar os dados, como:
  - **recuperação direta:** método que utiliza alguma falha já conhecida, seja do algoritmo criptográfico ou do aplicativo utilizado;
  - **rainbow tables:** método que utiliza uma tabela com hashes de senhas pré-calculadas por força bruta. Uma vez criada, essa tabela é consultada para se encontrar rapidamente a senha desejada;
  - **força bruta simples:** método de busca exaustiva em que todas as combinações possíveis de determinado grupo de caracteres são testadas;
  - **dicionário:** método em que todas as palavras contidas em um dicionário são testadas, uma a uma, na tentativa de se encontrar a senha desejada. A geração do dicionário pode utilizar informações encontradas no local de busca, senhas comumente utilizadas, senhas recuperadas do caso investigado, de outros casos, de dados biográficos dos indivíduos envolvidos, dentre outras fontes. Além disso, pode-se optar por aplicar regras de alteração aos dicionários disponíveis, como alterações de capitalização, substituição de letras por símbolos e números (como “a” por “@”), adição de dígitos ou símbolos no início, meio ou fim de cada ocorrência, concatenação de palavras do dicionário e inversão das letras das palavras

4.6. Elaboração do laudo

Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames.Tópicos a serem observados:

- A descrição do material deve conter todos os dados para a sua correta identificação e individualização, tais como marca, modelo e número de série.
- Recomenda-se a inclusão de fotos do material, especialmente em casos em que haja danos físicos ao equipamento.
- Informar se os exames foram realizados diretamente sobre a mídia original ou sobre a cópia; no primeiro caso, deve-se explicar quais foram os motivos e os procedimentos utilizados para garantir a integridade dos dados.
- Relatar, se for o caso, que foram utilizados procedimentos de recuperação de dados apagados ou corrompidos (dentre outros) e que os exames foram feitos não apenas sobre os arquivos diretamente acessíveis, mas também sobre aqueles apagados (fragmentados, corrompidos, etc.) e passíveis de recuperação.
- Descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa.
- Recomenda-se especificar os softwares utilizados durante os exames para permitir a compreensão dos procedimentos adotados ou para futuras verificações dos resultados.
- Descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses.
- Mencionar eventuais alterações (físicas ou lógicas) promovidas no material examinado além daquelas normalmente realizadas por ferramentas de extração de dados ou manipulação básica do equipamento.
- Na existência de anexo eletrônico ao laudo, os arquivos devem ser submetidos a uma função de hash, e o hash desta lista de hashes deve estar presente no laudo, juntamente com a explicação de seu propósito para a garantia de integridade.
- O material deve ser novamente lacrado, o novo número de lacre deve ser informado no laudo e o lacre rompido deverá ser acondicionado no interior do novo recipiente.

4.7. Geração de anexo eletrônico

- Caso haja grande volume de dados, é aconselhável o envio de ferramenta de indexação de palavras-chave junto ao anexo eletrônico (IPED, por exemplo).
- A integridade dos dados contidos no anexo eletrônico deve ser garantida por meio de utilização de uma função de hash criptograficamente segura.
- Não se recomenda a gravação de programas de cálculo de hash no anexo eletrônico gerado, exceto quando objeto dos exames.

5. PONTOS CRÍTICOS

- O vestígio deve ser examinado apenas por peritos criminais com conhecimento específico para esse propósito. No caso de órgãos periciais que tenham auxiliares de perícia, a manipulação de evidências por parte destes dar-se-á somente se devidamente capacitados e supervisionados por peritos criminais.
- A inicialização do equipamento estando a mídia original nele instalada só deve ser realizada em casos específicos em que não haja outra possibilidade de acesso aos dados.
- Atentar-se para a possibilidade da existência de mais de um disco no equipamento com o uso de algum tipo de arranjo de discos (RAID, JBOD).
- Deve-se verificar a existência de dados criptografados, podendo ser:
  - **arquivos ou pastas:** somente o conteúdo de um arquivo ou pasta encontra-se criptografado por meio do uso de ferramenta nativa do sistema operacional ou formatos específicos como ZIP ou DOCX;
  - **partição ou disco virtual:** nesse caso, um arquivo (contêiner) ou uma partição estão criptografados. Após o fornecimento da senha, o arquivo ou a partição são montados, disponibilizando ao usuário os arquivos e pastas ali contidos;
  - **disco completo:** nesse método a totalidade dos dados do disco é criptografada, podendo existir apenas alguns setores responsáveis pela inicialização descriptografados. Pode ser implementado no próprio dispositivo (como mídias externas com criptografia embutida ou HDs com suporte a SED) ou então gerenciados por software.
- Observar a ordem de inicialização no BIOS quando a mídia não puder ser removida do equipamento (por exemplo, mídias soldadas na placa-mãe) ou não haja ferramenta para conectar sua interface. Nesses casos, a duplicação deve ser feita utilizando-se o próprio equipamento, através de suas interfaces externas (como USB) e a inicialização por meio de uma mídia

externa com sistema operacional forense.

- Atentar-se ao fato de que mídias de armazenamento computacional podem conter credenciais de acesso a dados em nuvem. Caso haja autorização judicial para tal, e não seja possível oficiar o provedor de nuvem para fornecimento dos dados, as credenciais podem ser usadas em ferramentas forenses para a obtenção dos arquivos.
- Levar em consideração as configurações de fuso horário presentes no equipamento, incluindo configurações de horário de verão e sua eventual mudança durante o uso do aparelho, pois podem influenciar diretamente na temporalidade das evidências encontradas.

6.ESTRUTURA BÁSICA DO LAUDO

- Preâmbulo
- Histórico (opcional)
- Material
- Objetivo
- Exame
- Conclusão/Resposta aos Quesitos
- Considerações Técnico-Periciais (opcional)
- Anexos (opcional)

7. REFERÊNCIAS

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**

Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941. ·DITEC/DPF. Instrução Técnica nº 003/2010 e respectivos manuais. Brasília, 2010.

DITEC/DPF. **Manual de Procedimentos Periciais – Exames Periciais em Informática.** 1ª. ed. rev. e atual. – Brasília: Instituto Nacional de Criminalística: 2013.

KUPPENS, Luciano L. (2012). **Utilização de Dicionários Probabilísticos Personalizados para decifrar arquivos em análises periciais.** Dissertação de Mestrado, Publicação PPGENE.DM – 090 A/12, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília/DF, 99p, Brasil.

Relatório final: câmaras técnicas de cadeia de custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019 (Portaria Senasp/MJSP n. 282, de 21 de maio de 2021) / Ministério da Justiça e Segurança Pública, Secretaria Nacional de Segurança Pública. – Brasília: O Ministério, 2023. ISBN digital 978-65-87762-56-2.

8. GLOSSÁRIO

ALGORITMO/FUNÇÃO DE HASH: gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações em uma pequena sequência de bits (hash). Esse hash se altera se um único bit da entrada for alterado, acrescentado ou retirado.

ARQUIVO-IMAGEM: arquivo contendo cópia integral da mídia original.

ARQUIVOS COMPOSTOS: arquivos que contêm outros arquivos.

BLOQUEADOR DE ESCRITA: equipamento ou software que previne a escrita de dados em uma mídia de armazenamento computacional e, assim, garante que os dados não serão alterados durante os procedimentos periciais.

IPED (Indexador e Processador de Evidências Digitais): É um software de código aberto, originalmente e ainda desenvolvido pela Polícia Federal, que pode ser utilizado para processar e analisar evidências digitais.

MÍDIA DE ARMAZENAMENTO COMPUTACIONAL: qualquer meio que possa ser utilizado para o armazenamento de dados digitais. Exemplos incluem discos rígidos, SSDs, mídias óticas, pendrives e cartões de memória.

MÍDIA DE TRABALHO/DESTINO: mídia de armazenamento computacional onde será armazenada a cópia dos dados da mídia original.

MÍDIA ORIGINAL: mídia de armazenamento computacional encaminhada para exame.

9. ANEXOS

- Não consta.

EXAME PERICIAL DE DISPOSITIVOS COMPUTACIONAIS MÓVEIS

POP N° 5.02 - INFORMÁTICA FORENSE

EXAME PERICIAL DE DISPOSITIVOS COMPUTACIONAIS MÓVEIS

FINALIDADE

Orientar o profissional de perícia da área de informática a realizar exames que envolvam dados contidos em dispositivos computacionais móveis.

PÚBLICO ALVO

Peritos Criminais afetos à atividade deste POP.

1. ABREVIATURAS E SIGLAS

AFU: After First Unlock (ver glossário para detalhes)
eSIM: Embedded Subscriber Identity Module (ver glossário para detalhes)
ICCID: Integrated Circuit Card Identifier
IMEI: International Mobile Equipment Identity
MMS: Multimedia Messaging Service
PIN: Personal Identification Number
PUK: Personal Unblock Key
SIM: Subscriber Identity Module
SMS: Short Message Service

2. RESULTADOS ESPERADOS

- Padronização dos exames periciais de dispositivos computacionais móveis.

3. MATERIAIS E EQUIPAMENTOS

- Sala ou caixa isolada de sinais de radiofrequência (gaiola de Faraday) ou equipamento bloqueador de sinais (jammer)
- Ferramentas forenses contendo programas, cabos e dispositivos que permitam a realização da extração dos dados do dispositivo computacional móvel.

- Estação de trabalho pericial (hardware + software) preparada para a análise dos dados e a elaboração do laudo e seus anexos
- Acesso irrestrito à Internet e privilégios administrativos na estação de trabalho pericial
- Armazenamento computacional com capacidade suficiente para os resultados dos exames
- Ferramentas e materiais para reparo de dispositivos computacionais móveis

4. PROCEDIMENTOS

4.1. Ações Preliminares

Esta etapa tem como objetivo determinar a viabilidade de realização do exame e organizar o material recebido. Para tanto, deve-se:

- atentar-se que os dispositivos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue, etc.) ou outros materiais contaminantes;
- antes do deslacre, conferir se a descrição dos materiais e identificadores (em especial o número de lacre) constantes em documentação associada está de acordo com os objetos recebidos. Havendo inconsistência, adotar os procedimentos definidos pelas normas locais;
- recomenda-se a captura de imagens dos materiais devidamente lacrados;
- deslacrar, realizar nova conferência do material com sua descrição na documentação associada, identificar e individualizar todos os itens;
- preferencialmente remover o cartão SIM, caso esteja presente no equipamento, identificando em qual slot o cartão SIM estava caso o aparelho comporte mais de um cartão SIM;
- realizar a remoção de mídia de armazenamento computacional (memória Micro SD ou similares) do dispositivo apenas para fins de identificação e individualização reinserindo novamente para realização dos exames;
- caso o equipamento tenha sido encaminhado em modo AFU, manter o dispositivo em isolamento de radiofrequência (seja através de gaiola de Faraday ou modo avião) e conectar o dispositivo em carregador adequado do recebimento até o momento do exame.

4.2. Extração dos Dados

- Realizar a extração dos dados dos cartões SIM utilizando equipamento forense apropriado. Caso o cartão SIM esteja protegido por senha (PIN/PUK) e não sendo possível reavê-la diretamente com o proprietário ou com a autoridade requisitante, tentar o desbloqueio por meio do equipamento forense ou utilizando a senha padrão da operadora.
- Caso haja mídia de armazenamento computacional (memória Micro SD ou similares), remover do dispositivo, realizar sua duplicação forense e reinseri-lo em seu slot original.
- Garantir que a bateria do dispositivo esteja carregada. Caso haja impossibilidade de utilização da bateria que acompanha o material, avaliar a possibilidade de substituí-la por uma temporária, utilizar fontes de alimentação externas ou utilizar técnicas de extração que não necessitem de bateria.
- Se o dispositivo estiver com defeitos que impeçam a extração dos dados (como danos ao conector de dados ou à tela, dependendo do caso), e existam ferramentas, materiais e conhecimento técnico necessários, realizar o reparo do equipamento.
- Caso o aparelho possua suporte a eSIM, ligar o equipamento dentro de gaiola de Faraday (seja uma sala ou caixa) ou com bloqueador de sinais de radiofrequência (jammer) ativo. Após ligado, caso não seja possível colocá-lo em modo avião, mantê-lo protegido de sinais.
- Sempre que possível, os dispositivos devem ser colocados em modo avião. Verificar se todas as conexões foram efetivamente desabilitadas (Wi-Fi, Bluetooth, rede de telefonia móvel, etc.).
    - Alguns modelos e marcas só permitem a ativação do modo avião com o uso de senha ou se o aparelho estiver desbloqueado.
- Caso o dispositivo esteja protegido por senha, e não tendo sido fornecida, tentar o desbloqueio por meio de equipamento forense ou utilizando dicionários de senhas mais comuns e/ou com dados do proprietário. Considerar que alguns aparelhos podem estar configurados para realizar a restauração aos padrões de fábrica caso haja um excesso de tentativas incorretas de senha.
- Caso o aparelho esteja desbloqueado, desabilitar todos os seus alarmes, pois em alguns modelos o dispositivo é ligado automaticamente no horário programado.

- Priorizar sempre a extração mais completa possível (física para dispositivos sem criptografia ou com criptografia de disco, ou de sistema de arquivos completa para dispositivos com criptografia baseada em arquivos).
- Caso o equipamento esteja no modo AFU, após a extração verificar se ela se encontra íntegra antes de desligar ou reiniciar o aparelho.

4.3. Processamento dos dados

Esta etapa visa à preparação dos dados para a análise e inclui, a depender do interesse pericial e da disponibilidade de ferramentas, os seguintes procedimentos, dentre outros:

- interpretação de dados de aplicativos e de sistema;
- recuperação de arquivos apagado;
- indexação de dados;
- categorização de arquivos (por exemplo, por tipo);
- cálculo de hashes;
- detecção de criptografia de arquivos;
- reconhecimento ótico de caracteres (OCR);
- uso de inteligência artificial para:
  - identificação de conteúdo de imagens e vídeos;
  - transcrição de áudio.

4.4. Análise dos dados

- A análise dos dados consiste no exame das informações extraídas na fase anterior, a fim de garantir a qualidade do resultado a ser entregue e, caso pertinente, identificar e selecionar evidências digitais relacionadas ao escopo pericial. Dentre os possíveis vestígios de interesse, a depender do caso, podemos citar:

  - informações de usuário, por exemplo: agenda de contatos, listas de chamadas, calendário, notas, imagens, vídeos, gravações de áudio;
  - mensagens eletrônicas, por exemplo: SMS, MMS, correio eletrônico, aplicativos de comunicação instantânea;
  - dados de redes sociais;
  - informações de Internet, por exemplo: páginas favoritas, histórico de navegação, cookies;

- informações de localização, por exemplo: coordenadas geográficas, rotas;
- informações de conexão, por exemplo: dispositivos pareados, conexões sem fio;
- arquivos ou outros dados apagados, se passível de recuperação.

- Caso seja necessário o esclarecimento de alguma questão pontual técnico-pericial sobre o material encaminhado, os quesitos devem ser os mais objetivos possíveis, sempre buscando delimitar bem a questão desejada, e deve ser fornecido o máximo de informações disponíveis sobre o assunto. A falta de informações que delimitem claramente o trabalho a ser realizado implica em aumento considerável no tempo de atendimento da solicitação de perícia, visto que leva à necessidade de exame de um universo maior de arquivos e dados. O Perito Criminal, assim, foca suas buscas em arquivos específicos, correlacionando os vestígios encontrados e elaborando conclusões precisas.

4.5. Elaboração do Laudo

- Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames. Tópicos a serem observados:

  - a descrição do material (equipamento, bateria, cartão SIM, cartão de memória removível, etc.) deve conter todos os dados para a sua correta identificação e individualização, tais como marca, modelo, número de série, IMEIs, ICCID e operadora do cartão SIM;
  - recomenda-se a inclusão de fotos do material, especialmente em casos em que haja danos físicos ao equipamento;
  - descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa;
  - recomenda-se especificar os softwares utilizados durante os exames para permitir a compreensão dos procedimentos adotados ou para futuras verificações dos resultados;

- descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses;
- mencionar eventuais alterações (físicas ou lógicas) promovidas no material examinado além daquelas normalmente realizadas por ferramentas de extração de dados ou manipulação básica do aparelho;
- na existência de anexo eletrônico ao laudo, os arquivos devem ser submetidos a uma função de hash, e o hash desta lista de hashes deve estar presente no laudo, juntamente com a explicação de seu propósito para a garantia de integridade;
- o material deve ser novamente lacrado, o novo número de lacre deve ser informado no laudo e o lacre rompido deverá ser acondicionado no interior do novo recipiente.

4.6. Geração de anexo eletrônico

- Caso haja grande volume de dados, é aconselhável o envio de ferramenta de indexação de palavras-chave junto ao anexo eletrônico (como exemplo: IPED ou Cellebrite Reader).
- A integridade dos dados contidos no anexo eletrônico deve ser garantida por meio de utilização de uma função de hash criptograficamente segura.
- Não se recomenda a gravação de programas de cálculo de hash no anexo eletrônico gerado, exceto quando objeto dos exames.

5. PONTOS CRÍTICOS

- O vestígio deve ser examinado apenas por peritos criminais com conhecimento específico para esse propósito. No caso de órgãos periciais que tenham auxiliares de perícia, a manipulação de evidências por parte destes dar-se-á somente se devidamente capacitados e supervisionados por peritos criminais.
- Ligar o equipamento com alguma interface de comunicação habilitada e fora de uma gaiola de Faraday pode resultar em alteração remota dos dados do dispositivo ou sua restauração aos padrões de fábrica.
- Caso o aparelho seja encontrado em situações ou condições especiais (como necessidade de extração em modo AFU, contaminação por agentes biológicos, danos físicos significativos, etc.), deve-se tomar os

cuidados necessários durante a manipulação da evidência.

- A extração manual deve ser realizada somente como última alternativa e somente quando houver informações pertinentes ao motivo pericial, haja vista o risco de alteração acidental dos dados, a possibilidade de erro humano, o grande tempo despendido no processo e a impossibilidade de recuperação dos dados apagados.
- É possível existir inconsistência entre os registros contidos na memória do aparelho e os da operadora de telefonia, por exemplo, data e hora das chamadas, chamadas originadas do equipamento e imediatamente canceladas pelo usuário, ou registros apagados manualmente pelo usuário.
- Se o cartão SIM estiver bloqueado por PIN/PUK, prestar atenção ao número de tentativas possíveis. O PIN é bloqueado após 3 (três) e PUK após 10 (dez) tentativas.
- Estar atento ao fato de que alguns aparelhos podem estar configurados para realizar a restauração aos padrões de fábrica caso haja um excesso de tentativas incorretas de senha.
- Normalmente o número da linha telefônica não é armazenado nem no aparelho nem em seu cartão SIM, apesar de ser vinculado a este último. A obtenção do número da linha telefônica e demais dados cadastrais deve ser realizado através da operadora de telefonia.
- Geralmente as mensagens de correio de voz são armazenadas em servidores da operadora de telefonia, e não no próprio equipamento. Neste caso, há necessidade de autorização judicial para acesso às mensagens de correio de voz junto à operadora de telefonia.
- Tomar precauções necessárias caso a bateria do dispositivo apresente danos aparentes (estufada, por exemplo) e, se houver risco de explosão ou vazamento, realizar seu descarte ecológico, indicando tal fato no laudo.
- Atentar-se ao fato de que dispositivos computacionais móveis podem conter credenciais de acesso a dados em nuvem. Caso haja autorização judicial para tal, e não seja possível oficiar o provedor de nuvem para fornecimento dos dados, as credenciais podem ser usadas em ferramentas forenses para a obtenção dos arquivos.
- Levar em consideração as configurações de fuso horário presentes no equipamento, incluindo configurações de horário de verão e sua eventual mudança durante o uso do aparelho, pois podem influenciar diretamente na temporalidade das evidências encontradas.

- Os IMEIs impressos fisicamente podem ser diferentes dos gravados na memória do aparelho. Esta situação ocorre em equipamentos que sofreram adulteração, normalmente para contornar o bloqueio de IMEIs pelas operadoras.
- Podem estar configuradas áreas distintas de armazenamento de dados e de aplicativos do usuário, como segundo espaço, espaços paralelos, "cofres" de arquivos, diferentes usuários ou similares. Elas podem estar protegidas por senhas diferentes da principal, e exigir desbloqueio e extração em separado.

6. ESTRUTURA BÁSICA DO LAUDO

- Preâmbulo
- Histórico (opcional)
- Material
- Objetivo
- Exame
- Conclusão/Resposta aos Quesitos
- Considerações Técnico-Periciais (opcional)
- Anexos (opcional)

7. REFERÊNCIAS

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**

Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941.

Relatório final: câmaras técnicas de cadeia de custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019 (Portaria Senasp/MJSP n. 282, de 21 de maio de 2021) / Ministério da Justiça e Segurança Pública, Secretaria Nacional de Segurança Pública. – Brasília: O Ministério, 2023. ISBN digital 978-65-87762-56-2.

8. GLOSSÁRIO

AFU (After First Unlock): estado de um dispositivo que foi desbloqueado ao menos uma vez após ser ligado, possibilitando, em alguns casos, a extração dos dados do dispositivo utilizando ferramentas avançadas, sem o conhecimento da senha.

ALGORITMO/FUNÇÃO DE HASH: gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma

grande quantidade de informações em uma pequena sequência de bits (hash). Esse hash se altera se um único bit da entrada for alterado, acrescentado ou retirado.

BLOQUEADOR DE SINAIS (JAMMER): equipamento eletrônico que gera sinais de radiofrequência com o objetivo de interferir (bloquear) em sinais de comunicação.

CARTÃO SIM: cartão inteligente utilizado para identificar, controlar e armazenar dados de telefones celulares. Ele pode armazenar dados como informações do assinante, agenda, preferências, serviços contratados, SMS, dentre outras.

COFRE DE ARQUIVO: local de armazenamento de arquivos em dispositivos computacionais móveis, protegidos por senha específica e normalmente criptografados.

DISPOSITIVO COMPUTACIONAL MÓVEL: dispositivos eletrônicos como aparelhos de telefonia celular, smartphones e tablets (não incluem notebooks).

eSIM (Embedded SIM): uma forma de cartão SIM virtual que é embarcado diretamente no dispositivo, sem necessidade de cartão físico.

ESPAÇO PARALELO: local alternativo de instalação de aplicativos e armazenamento de arquivos separado do ambiente principal do usuário, podendo ser protegido por senha específica e/ou criptografado.

GAIOLA DE FARADAY: isolamento utilizado para bloquear campos eletromagnéticos, evitando a transmissão ou recepção de sinais de radiofrequência.

IPED (Indexador e Processador de Evidências Digitais): É um software de código aberto, originalmente e ainda desenvolvido pela Polícia Federal, que pode ser utilizado para processar e analisar evidências digitais.

MODO AVIÃO: função existente em dispositivos computacionais móveis que desabilita o acesso à rede celular da operadora de telefonia e, dependendo do equipamento, outras conexões sem fio, como Wi-Fi e Bluetooth.

SEGUNDO ESPAÇO: similar ao espaço paralelo, mas permite o uso de senha específica na tela de desbloqueio do aparelho para acesso direto à área de trabalho independente da principal.

9. ANEXOS

- Não consta.

EXAME PERICIAL DE LOCAL DE INFORMÁTICA

POP N° 5.03 - INFORMÁTICA FORENSE

EXAME PERICIAL DE LOCAL DE INFORMÁTICA

FINALIDADE

Orientar o profissional de perícia da área de informática a realizar exame pericial de local de informática.

PÚBLICO ALVO

Peritos Criminais afetos à atividade deste POP.

1. ABREVIATURAS E SIGLAS

BIOS: Basic Input/Output System
NVMe: Non-Volatile Memory Express
PATA: Parallel Advanced Technology Attachment
SAS: Serial Attached SCSI
SATA: Serial Advanced Technology Attachment
SCSI: Small Computer System Interface
SSD: Solid State Drive
EPI: Equipamento de Proteção Individual

2. RESULTADOS ESPERADOS

- Padronização dos exames periciais de local de informática.

3. MATERIAIS E EQUIPAMENTOS

- Câmera fotográfica
- Equipamento de duplicação pericial ou bloqueador de escrita (como os produtos das empresas OpenText Tableau, LogiCube, Atola, por exemplo)
- Mídias externas de inicialização com sistemas operacionais forenses, tais como: Kali, CAINE, e ferramentas forenses, tais como: FTK® Imager, NuDetective, Localizador de Evidências Digitais (LED), etc.

- Bases de hashes de conteúdo criminoso (como as bases de dados INTERPOL's Child Sexual Exploitation e National Center for Missing and Exploited Children)
- Dispositivos de armazenamento externos vazios
- Dispositivos de armazenamento internos vazios (caso necessário para uso com equipamento de duplicação pericial)
- Conjunto de cabos e adaptadores, tais como: M.2 (NVMe e SATA), PATA, SATA, SCSI, SAS, etc.
- Laptop equipado com softwares forenses
- Embalagens e lacres de tamanho compatível com equipamentos e mídias computacionais como HDs, gabinetes e laptops
- Embalagem antiestática para remessa de dispositivos cujos circuitos eletrônicos estejam expostos, tais como HDs e SSDs NVMe.
- Conjunto de ferramentas manuais (chaves philips, fenda, alicates, etc.)
- EPIs (luvas de látex e outras dependendo das peculiaridades esperadas)

4. PROCEDIMENTOS

4.1. Ações Preliminares

- Realizar um levantamento prévio a respeito do tipo de delito investigado e das peculiaridades do local a ser examinado, permitindo a escolha de equipamentos, embalagens e ferramentas, além da preparação de palavras-chave de busca específicas e lista de hashes.
- Em casos específicos de riscos à integridade das evidências através de acesso remoto, verificar a possibilidade de bloqueio de sinal de internet junto ao provedor de serviço durante os exames, mediante autorização judicial.

4.2. Ações Preliminares

- Atentar-se à existência de eventuais restrições legais, dando especial atenção às determinações de mandados de busca e apreensão.
- Reconhecer os equipamentos computacionais e infraestrutura de rede presentes no ambiente, e selecionar os que são de possível interesse.
- Providenciar o isolamento do local para evitar que pessoas estranhas à equipe de perícia criminal tenham acesso físico aos equipamentos de informática presentes. Do mesmo modo, promover o isolamento digital do local, bloqueando os acessos remotos ou as conexões de rede e internet, desde que não prejudiquem os exames.

- Realizar um levantamento do ambiente computacional (fixação), fotografando-o, se necessário. Tratando-se de empresa ou órgão público, recomenda-se solicitar o auxílio do responsável pela área de informática.
- Atentar-se que os equipamentos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue, etc.) ou outros materiais contaminantes.

4.3. Exame

- Devido à volatilidade de certos vestígios computacionais, restrições de apreensão de equipamentos ou constatação de flagrante delito, em determinadas situações torna-se necessária a análise de arquivos no local a ser periciado ou no local de busca.
- Pode-se classificar o exame de dados no local em dois tipos: quando o equipamento é encontrado ligado, podendo acarretar alteração de seu conteúdo; e quando realizado com o equipamento desligado, sem alteração de seu conteúdo.

4.3.1. Exame em computador ligado

- Ao encontrar um computador ligado, se os vestígios voláteis forem de interesse, os exames devem ser focados na sua preservação e extração. Para isto, deve-se:
    - preservar os dados, seguindo a ordem dos mais voláteis para os menos voláteis;
    - o dump da memória principal deve ser realizado quando houver interesse em seus dados, por exemplo, quando suspeitar-se de uso de criptografia. Para coleta deve-se utilizar softwares específicos, como por exemplo FTK Imager ou Volatility;
    - verificar programas em execução, como navegadores de Internet, aplicativos de comunicação instantânea e correio eletrônico, aplicativos de armazenamento de dados remotos, ferramentas de compartilhamento de arquivos (ponto-a-ponto), aplicativos para criptografia, etc;

- fixar o que foi encontrado, incluindo, se for o caso, fotografias, captura de telas, vídeos, etc;
- verificar se existem indícios de existência de partições criptografadas;
- verificar a existência de aplicativos instalados para criptografia de arquivos ou partições, como VeraCrypt;
- se for pertinente, utilizar bases de hashes para busca de arquivos suspeitos;
- havendo autorização judicial para cópias de arquivos em nuvem, atentar-se para aqueles que não estejam baixados no computador, além de possíveis casos de acesso a máquinas remotas.

- Caso seja necessária a apreensão do computador ou de suas mídias de armazenamento, deve-se desligar a energia do equipamento (se ele contiver bateria não removível, forçar o desligamento imediato).
- Sendo constatadas partições criptografadas, recomenda-se apreensão do equipamento completo, caso contrário é possível coletar somente as mídias de armazenamento.
- Se houver suspeita de que existam partições protegidas por algum tipo de criptografia, e estando estas abertas (montadas), deve-se copiar seu conteúdo de forma integral ou parcial, a depender do interesse (pode-se utilizar, por exemplo, o FTK® Imager).
- Em computadores do tipo servidor, sugere-se requisitar o auxílio do responsável pela área de informática para a extração dos dados relevantes, evitando, sempre que possível, a apreensão desses equipamentos. Confirmar se não há entre esses funcionários nenhum com suspeita de participação na prática delituosa investigada.

4.3.2. Exame em computador desligado

- Este exame no local a ser periciado ou local de busca é desaconselhável. Usualmente é realizado apenas quando há a possibilidade de constatar flagrante delito, quando apenas alguns arquivos específicos estão sendo buscados ou como forma de triagem de materiais a serem apreendidos.
- No exame em computador desligado, deve-se efetuar o acesso ao conteúdo das mídias preferencialmente sem a inicialização do sistema operacional instalado no equipamento, através de: i) uso de bloqueadores de escrita ou ii) inicialização de um sistema operacional forense.

- Na primeira opção, deve-se conectar a mídia em análise a um laptop com ferramentas forenses, com bloqueio de escrita via hardware ou software. Os arquivos podem então ser acessados por meio de algum visualizador, como o FTK® Imager.
- Na segunda opção, utiliza-se uma mídia externa de inicialização com sistema operacional forense que monte as mídias do dispositivo periciado no modo somente leitura. A ordem de inicialização do sistema deve ser configurada na BIOS de modo a impedir a inicialização da mídia instalada no equipamento.

- Caso seja pertinente, utilizar bases de hashes para busca de arquivos suspeitos.
- Sendo constatado algum tipo de criptografia nas mídias examinadas, deve-se tentar obter no local as senhas ou chaves criptográficas de acesso. Nesta situação, caso a senha seja conhecida, pode ser necessária a inicialização do sistema operacional da máquina em questão (por exemplo, em um computador Windows com TPM e BitLocker ativado, o acesso às partições depende da senha do usuário). Com o equipamento ligado, seguir as recomendações do capítulo "4.3.1 Exame em computador ligado".

4.4. Extração (coleta) de dados

- A extração de dados pode-se dar de forma parcial ou nas mídias inteiras, podendo ou não ser apreendida a mídia original:

  - sendo a extração parcial, podem ser coletados: arquivos selecionados, bases de dados exportadas, relatórios sobre o estado do computador (gerados por ferramentas de análise live), uma partição lógica de um volume originalmente criptografado, etc;
  - caso seja feita a extração de mídias inteiras, deve-se verificar a existência de partições criptografadas. Caso existam, deve-se tentar obter no local as senhas ou chaves criptográficas de acesso. Nesta situação, caso a senha seja conhecida, pode ser necessária a inicialização do sistema operacional da máquina em questão (por exemplo, em um computador Windows com TPM e BitLocker ativado, o acesso às partições depende da senha do usuário) e utilização de ferramentas forenses portáveis para a extração (como o FTK® Imager).

- O hash dos arquivos extraídos deve constar no documento produzido pelo perito.

4.5. Cadeia de Custódia de Dados e Materiais

- Os hashes de todos os dados extraídos ou copiados devem constar em termo de apreensão.
- Deve-se acondicionar e lacrar todos os materiais apreendidos, incluindo as mídias usadas como destino de dados. Os respectivos lacres e descrição sucinta do material e sua origem devem constar em termo de apreensão.
- Recomenda-se a utilização de embalagem antiestática para acondicionamento de materiais com circuitos eletrônicos expostos, como SSDs NVMe e HDs.

4.6. Elaboração do Laudo

Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames, além de citar todos os lacres, hashes e responsáveis pelos exames ou extrações.
Tópicos a serem observados durante o processamento do material a ser examinado:

- detalhar os procedimentos realizados no local, em especial aqueles que possam ter gerado alterações nos dados (durante o exame com computador ligado, por exemplo);
- recomenda-se especificar os softwares utilizados durante os exames para permitir a compreensão dos procedimentos adotados ou para futuras verificações dos resultados;
- descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses;
- na existência de anexo eletrônico, os arquivos devem ser submetidos a uma função de hash para fins de garantia de integridade, e o hash desta lista de hashes deve estar presente no laudo.

4.7. Geração de anexo eletrônico

- Caso haja grande volume de dados, é aconselhável o envio de ferramenta de indexação de palavras-chave junto ao anexo eletrônico (como exemplo: IPED).
- A integridade dos dados contidos no anexo eletrônico deve ser garantida por meio de utilização de uma função de hash criptograficamente segura.
- Não se recomenda a gravação de programas de cálculo de hash no anexo eletrônico gerado, exceto quando objeto dos exames.

5. PONTOS CRÍTICOS

- O ambiente computacional deve ser examinado apenas por peritos criminais com conhecimento específico para esse propósito.
- Caso as condições necessárias para realização dos exames no local não sejam suficientes (como a falta de ferramentas adequadas), o melhor a fazer é coletar os equipamentos para serem examinados posteriormente em laboratório.
- Atentar-se para a possível necessidade de vincular os usuários dos equipamentos às suas respectivas contas.
- No caso de utilização de mídias externas de inicialização, atentar-se para a ordem de inicialização na BIOS do equipamento periciado. ·
- Deve-se ficar atento à existência de mídias de armazenamento camufladas (como pendrives em formato de chaveiros, enfeites, etc.) ou fisicamente ocultas (como SSDs presentes embaixo de dissipadores, placas de vídeo, ou na face inferior da placa-mãe).
- O perito deve observar a existência de partições criptografadas ou se algum software criptográfico se encontra instalado ou em execução.
- Senhas, nomes de usuários ou detalhes do funcionamento de sistemas podem ser necessários em um exame futuro. Essas informações podem ser encontradas em anotações próximas aos computadores ou ser solicitadas às pessoas presentes no local, mesmo que sejam os próprios suspeitos da investigação. Essas informações devem constar no termo de apreensão e ser enviadas junto ao equipamento de informática ao qual se referem.
- Checar se os equipamentos de interesse possuem alguma mídia removível neles inseridas (mídias óticas, cartão de memória, etc.).

6. ESTRUTURA BÁSICA DO LAUDO

- Preâmbulo
- Histórico (opcional)
- Material
- Objetivo
- Exame
- Conclusão/Resposta aos Quesitos
- Considerações Técnico-Periciais (opcional)
- Anexos (opcional)

7. REFERÊNCIAS

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**
Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941.
DITEC/DPF. Instrução Técnica no 003/2010 e respectivos manuais. Brasília, 2010.
DITEC/DPF. Instrução Técnica no 018/2013 e respectivo manual. Brasília, 2013.
DITEC/DPF. Manual de Exames Periciais em Informática. Brasília, 2013.
ELEUTÉRIO, Pedro Monteiro da Silva, MACHADO, Márcio Pereira. **Desvendando a computação forense.** São Paulo: Novatec Editora, 2010.
Relatório final: câmaras técnicas de cadeia de custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019 (Portaria Senasp/MJSP n. 282, de 21 de maio de 2021) / Ministério da Justiça e Segurança Pública, Secretaria Nacional de Segurança Pública. – Brasília: O Ministério, 2023. ISBN digital 978-65-87762-56-2.
SHIMABUKO, Ângelo. **Introdução à Perícia em Informática.** Brasília, 2009.

8. GLOSSÁRIO

ALGORITMO DE HASH: gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações em uma pequena sequência de bits (hash). Esse hash se altera se um único bit da entrada for alterado, acrescentado ou retirado.

BITLOCKER: é uma funcionalidade dos sistemas operacionais Microsoft© Windows© utilizada para criptografia de volumes de mídias de armazenamento.

BLOQUEADOR DE ESCRITA: equipamento ou software que previne a escrita de dados em uma mídia de armazenamento computacional e, assim, garante que os dados não sejam alterados durante os procedimentos periciais.

DUMP DE MEMÓRIA: extração dos dados armazenados em memória volátil do equipamento.

FTK® IMAGER: é uma ferramenta forense de propriedade da Exterro, Inc. que permite a captura da memória e aquisição e visualização de dados em unidades de armazenamento.

IPED (Indexador e Processador de Evidências Digitais): É um software de código aberto, originalmente e ainda desenvolvido pela Polícia Federal, que pode ser utilizado para processar e analisar evidências digitais.

LOCAL DE INFORMÁTICA: é um local onde se encontram vestígios em ambientes computacionais, que demandam profissional de perícia especializado para seu reconhecimento, isolamento, fixação, coleta, acondicionamento e processamento.

LOCALIZADOR DE EVIDÊNCIAS DIGITAIS (LED) e NUDETECTIVE: são ferramentas desenvolvidas dentro da Polícia Federal com o objetivo de facilitar a localização e classificação, de maneira rápida e eficaz, de evidências relacionadas à abuso sexual infantojuvenil em operações de busca e apreensão de equipamentos de informática.

M.2: especificação para placas de expansão de computador montadas internamente e conectores associados. M.2 substitui o padrão mSATA, que usa o layout e os conectores físicos da placa PCI Express Mini Card.

MÍDIA EXTERNA DE INICIALIZAÇÃO: mídia externa (como pendrive ou HD externo) contendo versão de um sistema operacional carregável em memória RAM, ou seja, sem necessidade de instalação, contendo ferramentas forenses.

TPM (Trusted Platform Module): é um módulo usado por serviços de criptografia, para criar e armazenar chaves criptográficas com segurança e para confirmar se o sistema operacional e o firmware do dispositivo não foram adulterados.

VOLATILITY: ferramenta desenvolvida pela Volatility Foundation que permite extração e análise do estado da memória RAM de equipamentos computacionais.

9. ANEXOS

- Não consta.

EXAME PERICIAL DE LOCAL DE INTERNET

POP N° 5.04 - INFORMÁTICA FORENSE

EXAME PERICIAL DE LOCAL DE INTERNET

FINALIDADE

Orientar o profissional de perícia da área de informática a realizar exame pericial de local de internet.

PÚBLICO ALVO

Peritos Criminais afetos à atividade deste POP.

1. ABREVIATURAS E SIGLAS

ARC: Authenticated Received Chain
CGNAT: Carrier Grade Network Address Translation
DNS: Domain Name Server
IP: Internet Protocol
SPF: Sender Policy Framework
TOR: The Onion Router
VPN: Virtual Private Network

2. RESULTADOS ESPERADOS

- Padronização dos exames periciais de local de Internet.

3. MATERIAIS E EQUIPAMENTOS

- Equipamento computacional equipado com softwares forenses.
- Conexão dedicada de Internet desvinculada da rede corporativa da instituição pública (sem informações cadastrais que indiquem a natureza pericial), ou alternativamente, utilização de serviço de navegação anônima (por exemplo, TOR ou VPN).

4. PROCEDIMENTOS

4.1. Ações Preliminares

Esta etapa tem como objetivo determinar a viabilidade de realização do exame. Para tanto, os Peritos Criminais devem:

- Informar-se previamente a respeito do tipo de delito investigado e das peculiaridades do local a ser examinado.
- Caso o exame exija navegação anônima, garantir que seu endereço IP não está vinculado a um órgão pericial ou policial.
- Garantir que haja autorização legal para acesso aos dados periciados.
- Caso haja material encaminhado para exame (como mídias contendo dados de Internet):

    - conferir se a descrição dos materiais e identificadores (em especial o número de lacre) constantes em documentação associada está de acordo com os objetos recebidos. Havendo inconsistência, adotar os procedimentos definidos pelas normas locais;
    - deslacrar e realizar nova conferência com a sua descrição na documentação associada;
    - identificar e individualizar todo o material.

4.2. Exame

- O exame de local de Internet consiste na utilização de técnicas e ferramentas para coletar vestígios deixados pela prática de infração penal com a utilização da Internet.
- Pode-se classificar o exame de local de Internet em quatro tipos básicos: exames de IPs e nomes de domínio, exames de mensagens de correio eletrônico, exames de sítios de Internet e exames de dados em nuvem.

4.2.1. Exame de IPs e nomes de domínio

- Existem situações em que são necessárias as análises de determinado endereço IP ou nome de domínio, tais como na análise de endereços IP presentes em cabeçalhos de correio eletrônico (e-mail) ou registros de eventos (logs) de acesso em servidores de rede.
- O endereço IP ou nome de domínio, sendo examinado, pode ser submetido à consulta de:

- dados cadastrais de registro em sites especializados (por exemplo, whois);
- rastreamento de rota de tráfego (por exemplo, traceroute);
- DNS reverso, visando identificar o domínio qualificado para a respectiva faixa de endereços (por exemplo, nslookup);
- informações gerais da origem, como sua localização geográfica.

- Para determinar o equipamento que utilizava o endereço IP na data e hora de interesse, a autoridade requisitante do exame deve oficiar ao provedor de conexão responsável pela faixa de IP. Em se tratando de IP versão 4 e da utilização de IPs compartilhados entre múltiplos usuários (CGNAT), faz-se necessário também o provedor de conexão fornecer qual era o usuário da porta lógica específica no momento do fato investigado.

4.2.2. Exame de mensagens de correio eletrônico

- Este exame visa a determinar a real origem de uma mensagem de correio eletrônico. Para tanto, é necessário estar de posse do cabeçalho completo da mensagem. Vale ressaltar que não há garantia de integridade dos dados de um cabeçalho de mensagem de correio eletrônico (e-mail), considerando que alguns campos podem ser facilmente forjados.
- Os campos "Received" contêm informações de rastreamento geradas pelos servidores de correio eletrônico (e-mail) pelos quais a mensagem passou. A ordem na qual os campos "Received" aparecem é inversa à ordem na qual a mensagem trafegou.
- Os campos "Received" devem ser verificados quanto à:

  - consistência dos horários de envio e recebimento;
  - consistência entre o endereço IP e o domínio indicados;
  - ordem dos campos no cabeçalho.

- Apesar de incomum, recomenda-se verificar se o servidor de correio eletrônico permite o envio de mensagens por usuários não identificados ("open relay" – "spoofing").
- Atentar ainda para os seguintes campos:

  - "X-Sender-IP" ou "X-Originating-IP": em alguns casos é preenchido pelo servidor de webmail no envio, indicando o endereço IP do remetente;
  - "DKIM-Signature" ou "DomainKey-Signature": mecanismos de

autenticação que podem ser utilizados para verificar a integridade de uma mensagem;
  - cabeçalhos relacionados ao protocolo Sender Policy Framework (SPF): mecanismos que garantem que um servidor de envios de e-mail é autorizado a enviar e-mail de um determinado domínio;
  - cabeçalhos relativos a outros protocolos de autenticação e segurança de e-mails, como Authenticated Received Chain (ARC).

4.2.3. Exame de sítios de internet

Este exame consiste em preservar o conteúdo de um sítio na Internet. A depender do caso, pode ser necessária a utilização de uma rede distinta da rede corporativa da Instituição, de modo a se evitar a identificação do acesso como proveniente de um órgão pericial.

- Se o sítio da Internet não estiver acessível, recomenda-se:
  - realizar tentativas de acesso em dias posteriores;
  - consultar sítios especializados em registrar o histórico da Internet, citando no laudo tal procedimento.
- O conteúdo de interesse deve ser salvo, preferencialmente, no formato digital original.
- Não sendo possível, utilizar qualquer outra maneira capaz de preservar os dados (por exemplo, captura de tela, fotografia, impressão, etc.). É importante registrar a data e hora dos exames e o endereço IP utilizado para acessar o sítio.

4.2.4. Exames de dados em nuvem

- Há duas possibilidades de exame de dados em nuvem:
  - quando houver quebra de dados determinada judicialmente, e os dados foram fornecidos pelo provedor de nuvem;
  - quando se possui as credenciais ou tokens de acesso do usuário, e pretende-se capturar estes dados diretamente da nuvem.
- Sempre que possível, deve-se dar preferência à quebra de dados determinada judicialmente, com o provedor fornecendo os dados.
- Para captura de dados diretamente da nuvem, caso esteja disponível, recomenda-se realizar uma cópia completa dos dados do usuário através de

recurso fornecido pelo provedor (como Google Takeout), em detrimento da captura individual de cada artefato. Quando indisponível, é possível utilizar-se de ferramentas forenses de extração de dados em nuvem, atentando-se ao risco de provedores detectarem tal tipo de extração e realizarem o bloqueio da conta ou do token de acesso obtido.

4.3. Elaboração do Laudo

- Esta etapa envolve a descrição dos exames efetuados e a apresentação, de forma clara e sucinta, dos procedimentos e métodos utilizados, esclarecendo os temas relevantes para a compreensão dos exames. Tópicos a serem observados:

    - Descrever os exames de forma proporcional à sua complexidade, evitando-se assim descrições extensas e complexas para laudos simples, e vice-versa.
    - Caso haja material (como mídias contendo dados de Internet), recomenda-se a inclusão de suas fotos.
    - Recomenda-se especificar os softwares utilizados durante os exames para permitir a compreensão dos procedimentos adotados ou para futuras verificações dos resultados.
    - Descrever as técnicas periciais propriamente ditas, e não os detalhes da utilização dos aplicativos forenses.
    - Detalhar as datas e horários dos exames realizados, evidenciando no laudo que o exame se refere a dados examinados da maneira como se encontravam naquele momento.
    - Na existência de anexo eletrônico ao laudo, os arquivos devem ser submetidos a uma função de hash, e o hash desta lista de hashes deve estar presente no laudo, juntamente com a explicação de seu propósito para a garantia de integridade.

4.4. Geração de anexo eletrônico

- Caso haja grande volume de dados, é aconselhável o envio de ferramenta de indexação de palavras-chave junto ao anexo eletrônico (IPED, por exemplo).
- A integridade dos dados contidos no anexo eletrônico deve ser garantida por meio de utilização de uma função de hash criptograficamente segura.
- Não se recomenda a gravação de programas de cálculo de hash no anexo eletrônico gerado, exceto quando objeto dos exames.

5. PONTOS CRÍTICOS

- Priorizar este tipo de perícia, dada a volatilidade dos dados.
- Os dados cadastrais apresentados pelos sites especializados (por exemplo, whois) podem ser falsos. Sendo assim, recomenda-se que esses dados sejam conferidos e confrontados com outras fontes de informação sobre o alvo.
- É recomendável, durante os exames, que se oculte a origem da navegação. Um acesso a um sítio suspeito através de um computador funcional, por exemplo, pode ser detectado, alertando o criminoso, que poderá retirar o material do ar antes de sua preservação.
- Caso sejam utilizadas ferramentas forenses de extração de dados em nuvem, atentar-se ao risco de provedores detectarem tal tipo de extração e realizarem o bloqueio da conta ou do token de acesso obtido.
- Atentar-se ao fato do uso de CGNAT por provedores de conexão para o compartilhamento de um único endereço IP versão 4 com múltiplos usuários, tornando necessário o conhecimento da porta lógica para identificação da origem da conexão.

6. ESTRUTURA BÁSICA DO LAUDO

- Preâmbulo
- Histórico (opcional)
- Material
- Objetivo
- Exame
- Conclusão/Resposta aos Quesitos
- Considerações Técnico-Periciais (opcional)
- Anexos (opcional)

7. REFERÊNCIAS

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**

Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**

Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941.

DITEC/DPF. **Instrução Técnica no 003/2010 e respectivos manuais.** Brasília, 2010.
DITEC/DPF. **Manual de Exames Periciais em Informática.** Brasília, 2013.
ELEUTÉRIO, Pedro Monteiro da Silva, MACHADO, Márcio Pereira. **Desvendando a computação forense.** São Paulo: Novatec Editora, 2010.
Relatório final: câmaras técnicas de cadeia de custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019 (Portaria Senasp/MJSP n. 282, de 21 de maio de 2021) / Ministério da Justiça e Segurança Pública, Secretaria Nacional de Segurança Pública. – Brasília: O Ministério, 2023. ISBN digital 978-65-87762-56-2.
SHIMABUKO, Ângelo. **Introdução à Perícia em Informática.** Brasília, 2009.

8. GLOSSÁRIO

ALGORITMO/FUNÇÃO DE HASH: gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações em uma pequena sequência de bits (hash). Esse hash se altera se um único bit da entrada for alterado, acrescentado ou retirado.

CGNAT (Carrier Grade Network Address Translation): é uma abordagem ao design de rede IP versão 4 em que os pontos finais, em particular as redes residenciais, estão configurados com endereços de rede privada que são traduzidos para endereços IP versão 4 públicos por dispositivos incorporados na rede do provedor de rede, permitindo o compartilhamento de um pequeno número de endereços públicos entre muitos usuários finais.

IPED (Indexador e Processador de Evidências Digitais): É um software de código aberto, originalmente e ainda desenvolvido pela Polícia Federal, que pode ser utilizado para processar e analisar evidências digitais.

9. ANEXOS

- Não consta.

APREENSÃO DE DISPOSITIVOS COMPUTACIONAIS MÓVEIS

POP N° 5.05 - INFORMÁTICA FORENSE

APREENSÃO DE DISPOSITIVOS COMPUTACIONAIS MÓVEIS

FINALIDADE

Orientar o profissional de perícia criminal a realizar apreensão de dispositivos computacionais móveis.

PÚBLICO ALVO

Peritos Criminais afetos à atividade deste POP.

1. ABREVIATURAS E SIGLAS

AFU = After First Unlock (ver glossário para detalhes)
eSIM = Embedded Subscriber Identity Module (ver glossário para detalhes)
ICCID = Integrated Circuit Card Identifier
SIM = Subscriber Identity Module

2. RESULTADOS ESPERADOS

- Padronização dos procedimentos para apreensão de dispositivos computacionais móveis.

3. MATERIAIS E EQUIPAMENTOS

- Câmera fotográfica
- Faraday bags e/ou papel alumínio
- Baterias externas portáteis (caso pertinente)
- Embalagens e lacres ou embalagens autolacrantes
- Etiquetas autoadesivas
- Papel toalha
- EPIs (luvas de látex e outras dependendo das peculiaridades esperadas)

4. PROCEDIMENTOS

4.1. Ações Preparatórias

- Garantir que baterias externas portáteis estejam carregadas, caso haja previsão de apreensão de dispositivos ligados em modo AFU.
- Caso pertinente, deixar de prontidão uma equipe pericial para extração de dados dos dispositivos computacionais móveis que estejam em modo AFU ou com desbloqueio por smartlock.

4.2. Ações Preliminares

- Reconhecer os dispositivos computacionais móveis presentes no ambiente, e selecionar os que são de possível interesse.
- Providenciar o isolamento do local para evitar que pessoas estranhas à equipe de perícia criminal tenham acesso físico aos dispositivos.
- Realizar um levantamento do local de apreensão (fixação), fotografando-o, se necessário.
- Atentar-se que os dispositivos podem conter vestígios físicos que podem ser de interesse ou exigir cuidados de manipulação, tais como impressões digitais, resíduos orgânicos (cabelo, pele, sangue, etc.) ou outros materiais contaminantes.

4.3. Apreensão

- Solicitar ao proprietário ou pessoas relacionadas a apresentação de todos os dispositivos computacionais móveis – a entrega de um dispositivo não exclui a possibilidade de existirem outros também em uso.
- Não permitir que o proprietário manipule os equipamentos.
- Deve ser colocada uma etiqueta tampando câmeras frontais, pois elas podem tirar fotos automáticas durante tentativas de desbloqueio ou realizar tentativas de desbloqueio por identificação facial de modo inadvertido. Não devem ser colocadas quaisquer outras etiquetas na parte frontal do aparelho (tela).
- Solicitar e anotar no termo de apreensão as senhas de desbloqueio.
    - Solicitar também as senhas adicionais utilizadas em segundo espaço, espaços paralelos, “cofres” de arquivos, diferentes usuários ou similares, caso existentes.

  - Sempre deve-se verificar nas configurações do dispositivo se há bloqueio por senha, pois aparelhos podem aparentar estar sem senha configurada em razão de configurações de smartlock e o bloqueio ser ativado quando a situação prevista no smartlock deixar de existir (geofence, conexão a uma rede Wi-Fi ou dispositivos Bluetooth específicos, etc.).
  - Caso o dispositivo esteja ligado, verificar se a senha está correta.
  - Todas as senhas devem também ser anotadas em etiquetas afixadas no verso do aparelho.

- Caso seja possível, os dispositivos apreendidos ligados devem ser colocados em modo avião. Verificar se todas as conexões foram efetivamente desabilitadas (Wi-Fi, Bluetooth, rede de telefonia móvel, etc.).

  - Alguns modelos e marcas só permitem a ativação do modo avião com o uso de senha ou se o aparelho estiver desbloqueado.
  - Registrar no termo de apreensão se foi possível ou não, colocar o dispositivo em modo avião.

- Caso o aparelho esteja desbloqueado, desabilitar todos os seus alarmes, pois em alguns modelos o dispositivo é ligado automaticamente no horário programado.
- Sempre remover os cartões SIM dos aparelhos, independente se foi possível colocar em modo avião. Ao realizar tal procedimento, identificar em qual slot do suporte os cartões se encontravam e descrever no termo de apreensão o slot, a operadora e o ICCID, caso visível.

  - Afixar os cartões SIM com etiqueta adesiva no verso do próprio aparelho, evitando o contato da cola da fita com os contatos do cartão.

- Em situações em que não haja interesse ou possibilidade de extração de dados em modo AFU, o dispositivo deve ser desligado, se possível.

  - Se a bateria for removível, deve ser retirada do aparelho e acondicionada na mesma embalagem;
  - Caso seja necessário o uso de senha para desligar o dispositivo e a senha seja desconhecida, devem ser tomadas as mesmas precauções com relação ao bloqueio de conexões utilizadas na apreensão de aparelhos em modo AFU. Caso viável, outras técnicas para desligamento do

aparelho podem ser utilizadas.

- Devem ser relacionados todos os cartões de memória, descrevendo suas capacidades e marcas no termo de apreensão.
    - Os cartões de memória devem sempre ficar dentro do aparelho e serem removidos apenas para anotações. Após o procedimento de identificação, devem ser reinseridos no dispositivo.
- No caso de apreensão do aparelho ligado para extração de dados em modo AFU ou quando não foi possível desligar o aparelho, devem ser tomadas medidas para evitar sua conexão com a Internet.
    - Remover os cartões SIM não é suficiente para garantir que os aparelhos fiquem sem conectividade, pois ainda é possível que se conectem em redes Wi-Fi próximas ou públicas, além da existência de eSIMs, que são cartões SIM virtuais que não podem ser removidos fisicamente.
    - Os dispositivos devem ser acondicionados em Faraday bags ou, na sua falta, embrulhados em papel-alumínio com ao menos três camadas cobrindo completamente o equipamento.
    - Caso a situação seja de extração de dados em modo AFU, o dispositivo deve ser mantido com carga na bateria e, se necessário, deve ser utilizada uma bateria portátil externa. A bateria portátil deve ser embalada na Faraday bag ou papel alumínio junto com o aparelho.
    - É possível que as Faraday bags sejam utilizadas para acondicionar múltiplos aparelhos já embalados e lacrados individualmente, otimizando a utilização desse recurso. No caso de uso de papel alumínio, cada dispositivo deve ser embrulhado individualmente e, após isso, lacrado.
- Todos os dispositivos devem ser embalados e lacrados individualmente, se possível, no local de coleta e o número do lacre deve constar no termo de apreensão.

4.4. Condições especiais relacionadas ao estado do dispositivo

- Caso o dispositivo esteja com danos físicos significativos que impeçam sua operação, existe o risco de ainda estar ligado e com possível conexão à rede de dados. Nessa situação devem ser tomadas as mesmas precauções com relação ao bloqueio de conexões utilizadas na apreensão de aparelhos em modo AFU.

  - Caso haja suspeita de danos à bateria e ela não possa ser removida, há risco de explosão e/ou incêndio, devendo-se tomar os cuidados adequados durante todas as fases da custódia do material.

- Se o aparelho for encontrado molhado, devem ser tomadas medidas para secá-lo externamente ainda no local de coleta e essa condição deve ser citada no termo de apreensão. Recomenda-se, também, afixar uma etiqueta na embalagem, indicando o estado do aparelho.

  - Na chegada do material à base policial/pericial, o aparelho deve ser removido da embalagem para secagem. Caso haja disponível laboratório e equipe especializada para desmontagem do aparelho, devem ser realizados procedimentos para secagem e limpeza interna. Caso contrário, o aparelho deve ser mantido em ambiente arejado e sem exposição direta ao sol para secagem natural. Para acelerar o processo é possível a utilização de pacotes de sílica gel (não utilizar outras técnicas "caseiras" para tal, pois podem trazer danos ao aparelho).
  - Caso a umidade seja decorrente de sangue ou outras contaminações biológicas (mesmo que secas), deve haver indicação de tal situação no termo de apreensão e afixada etiqueta na embalagem indicando contaminação biológica.

5. PONTOS CRÍTICOS

- Deve-se buscar elencar os usuários de cada aparelho no termo de apreensão, caso essa informação seja conhecida.
- Sempre que possível, deve-se tentar obter senhas ainda no local de coleta.
- Os dispositivos devem ser manipulados o mínimo necessário para permitir a execução dos procedimentos descritos neste POP.
- Caso o aparelho seja encontrado em situações ou condições especiais (como necessidade de extração em modo AFU, contaminação por agentes biológicos, danos físicos significativos, etc.), tal fato deve ser destacado no termo de apreensão e na embalagem do equipamento, e realizada a devida comunicação a quem for processar o material.

6. ESTRUTURA BÁSICA DO LAUDO

- Não se aplica.

7. REFERÊNCIAS

ABNT NBR ISO/IEC 27037:2013. Tecnologia da informação — Técnicas de segurança — **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.**

Código de Processo Penal, Decreto-Lei Nº 3.689, de 3 de outubro de 1941.

Relatório final: câmaras técnicas de cadeia de custódia: discussão, diagnóstico e recomendações pós Lei n. 13.964/2019 (Portaria Senasp/MJSP n. 282, de 21 de maio de 2021) / Ministério da Justiça e Segurança Pública, Secretaria Nacional de Segurança Pública. – Brasília: O Ministério, 2023. ISBN digital 978-65-87762-56-2.

8. GLOSSÁRIO

AFU (After First Unlock): estado de um dispositivo que foi desbloqueado ao menos uma vez após ser ligado, possibilitando, em alguns casos, a extração dos dados do dispositivo utilizando ferramentas avançadas, sem o conhecimento da senha.

CARTÃO SIM: cartão inteligente utilizado para identificar, controlar e armazenar dados de telefones celulares. Ele pode armazenar dados como informações do assinante, agenda, preferências, serviços contratados, SMS, dentre outras.

DISPOSITIVO COMPUTACIONAL MÓVEL: dispositivos eletrônicos como aparelhos de telefonia celular, smartphones e tablets (não incluem notebooks).

COFRE DE ARQUIVO: local de armazenamento de arquivos em dispositivos computacionais móveis, protegidos por senha específica e normalmente criptografados.

eSIM (Embedded SIM): uma forma de cartão SIM virtual que é embarcado diretamente no dispositivo, sem necessidade de cartão físico.

ESPAÇO PARALELO: local alternativo de instalação de aplicativos e armazenamento de arquivos separado do ambiente principal do usuário, podendo ser protegido por senha específica e/ou criptografado.

FARADAY BAG: embalagem utilizada para bloquear campos eletromagnéticos, evitando a transmissão ou recepção de sinais de radiofrequência.

GEOFENCE: técnica utilizada por equipamentos que possuem sistema de posicionamento geográfico para estabelecer um perímetro seguro, como a residência do usuário, por exemplo.

MODO AVIÃO: função existente em dispositivos computacionais móveis que desabilita o acesso à rede celular da operadora de telefonia e, dependendo do equipamento, outras conexões sem fio, como Wi-Fi e Bluetooth.

SEGUNDO ESPAÇO: similar ao espaço paralelo, mas permite o uso de senha específica na tela de desbloqueio do aparelho para acesso direto à área de trabalho independente da principal.

SMARTLOCK: opção para desabilitar temporariamente a necessidade de senha em situações pré-determinadas definidas pelo proprietário do aparelho, como uma determinada posição geográfica (georreferência) ou uma conexão a uma determinada rede Wi-Fi ou Bluetooth.

9. ANEXOS

- Não se aplica.

DSUSP

SECRETARIA
NACIONAL DE
SEGURANÇA PÚBLICA

MINISTÉRIO DA
JUSTIÇA E
SEGURANÇA PÚBLICA

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO