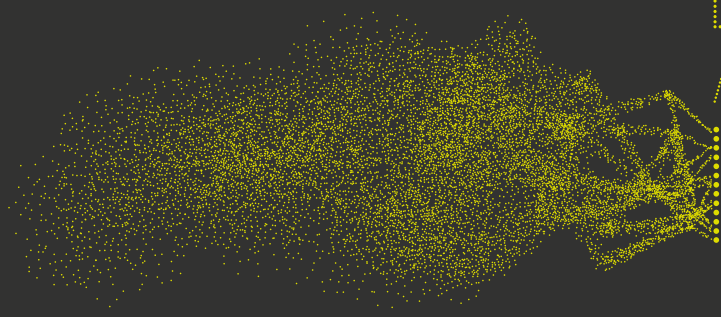
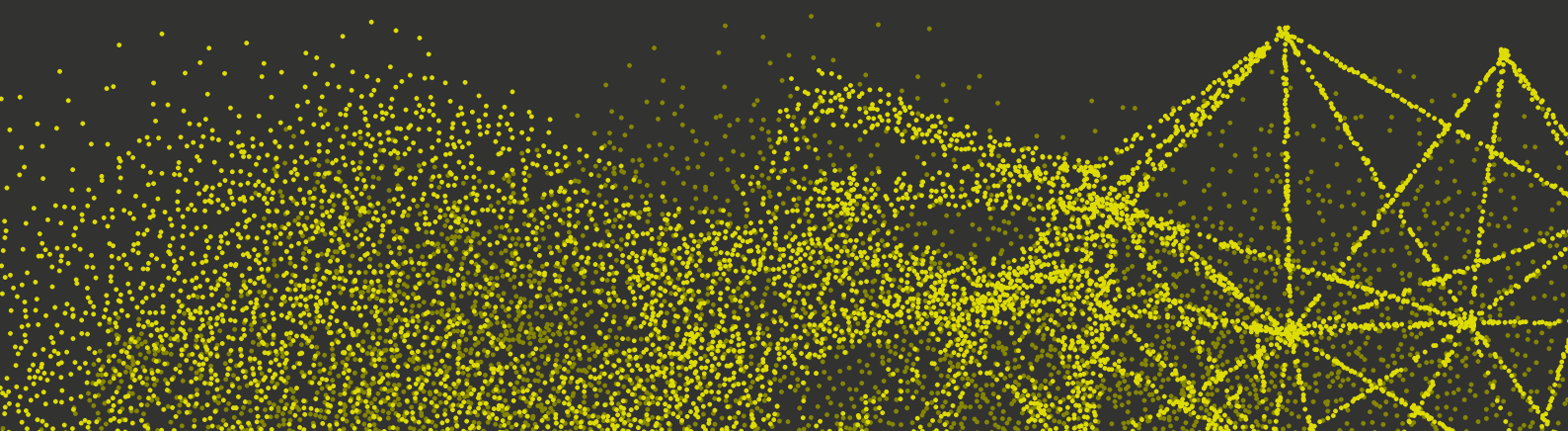
MINISTÉRIO PÚBLICO FEDERAL

MANUAL DE PROCEDIMENTOS DE CÓPIAS FORENSES DE MÍDIAS DE ARMAZENAMENTO DIGITAL





MANUAL DE PROCEDIMENTOS DE CÓPIAS FORENSES DE MÍDIAS DE ARMAZENAMENTO DIGITAL

MINISTÉRIO PÚBLICO FEDERAL

Raquel Elias Ferreira Dodge
Procuradora-Geral da República

Luciano Mariz Maia
Vice-Procurador-Geral da República

Humberto Jacques de Medeiros
Vice-Procurador-Geral Eleitoral

Julieta Elizabeth Fajardo Cavalcanti de Albuquerque
Ouvidora-Geral do MPF

Oswaldo José Barbosa Silva
Corregedor-Geral do MPF

Alexandre Camanho de Assis
Secretário-Geral

Cláudia Roque
Secretária-Geral Adjunta

Pablo Coutinho Barreto
Secretário de Perícia, Pesquisa e Análise

Vitor Souza Cunha
Secretário de Perícia, Pesquisa e Análise Adjunto

Ministério Público Federal
Secretaria de Perícia, Pesquisa e Análise

MANUAL DE PROCEDIMENTOS DE CÓPIAS FORENSES DE MÍDIAS DE ARMAZENAMENTO DIGITAL

Brasília - DF
MPF
2018

Disponível em:

<http://intranet.mpf.mp.br/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios-1>

Dados Internacionais de Catalogação na Publicação (CIP)

B823m

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

Manual de procedimentos de cópias forenses de mídias de armazenamento digital / Ministério Público Federal, Secretaria de Perícia, Pesquisa e Análise. – Brasília : MPF, 2018.

21 p.

Disponível também em: <http://intranet.mpf.mp.br/areas-tematicas/gabinete-pgr/pericia-pesquisa-e-analise/publicacoes-e-manuais/relatorios-1>.

1. Mídia digital. 2. Prova pericial. 3. Perícia. 4. Preservação de documentos digitais. 4. Ministério Público Federal – manual. I. Brasil. Ministério Público Federal. Secretaria de Perícia, Pesquisa e Análise. II. Título.

CDD 302.23

Elaborado por Juliana de Araújo Freitas Leão – CRB1/2596

Organização

Centro Nacional de Perícia - Assessoria Nacional de Perícias em TIC

Coordenação

Marcelo Caiado e Mauro Sobrinho

Redação

Altenis Valecio Lima e Lima, Antônio Willian Sousa, Bruno Brito de Oliveira, Guimel Medeiros Almeida, Marcelo Beltrão Caiado, Marcelo Santiago Guedes, Marcos Thompson Viegas Lerário e Tiago Calmon de Jesus

Planejamento visual, revisão e diagramação

Secretaria de Comunicação Social

Normalização Bibliográfica

Coordenadoria de Biblioteca e Pesquisa (Cobip)

Procuradoria-Geral da República

SAF Sul, Quadra 4, Conjunto C

70050-900 - Brasília - DF

Telefone (61) 3105-5100

www.mpf.mp.br

SUMÁRIO

APRESENTAÇÃO

Este manual tem como objetivo descrever, no âmbito do Ministério Público Federal, as atividades relacionadas à realização de cópias forenses de mídias de armazenamento digital.

Descreve, com maior nível de detalhe, as diretrizes e procedimentos gerais, relativos à duplicação forense de mídias, sem, entretanto, esgotar cada tema. Detalhes técnicos devem ser procurados nos manuais dos produtos e em repositórios de conhecimento existentes no MPF Colabora.

A leitura deste manual é recomendada a todos os peritos, peritos eventuais e servidores de Tecnologia da Informação e Comunicação atuantes no suporte de perícias de TIC, que terão neste documento um referencial para a realização de duplicação forense de mídias de armazenamento de forma padronizada e sistematizada, ajudando-os na busca incessante do aprimoramento das atividades periciais.

LISTA DE SIGLAS E ABREVIATURAS

BIOS = Basic Input/Output System

CD = Compact Disc

DCO = Device Configuration Overlay

DVD = Digital Versatile Disk

HPA = Host Protected Area

MD5 = Message Digest 5

PCMCIA = Personal Computer Memory Card International Association

PFL = Portable Forensic Lab

RAID = Redundant Array of Independent Disks

SHA = Secure Hash Algorithm

SSH = Secure Shell

USB = Universal Serial Bus

INTRODUÇÃO

Os exames em mídias de armazenamento digital devem, sempre que possível, ser efetuados sobre cópias integrais dos dados a serem examinados. O objetivo primordial é a preservação da mídia original, cujo manuseio pode, eventualmente, comprometer a integridade dos dados.

A obtenção, o manuseio e o armazenamento de evidências são informações importantes para a perícia e o processo investigatório. O registro sistematicamente documentado de onde, quando e como estavam as evidências é crucial e pode, inclusive, complementar e auxiliar o perito na elucidação dos cenários objetos de questionamento. Portanto, a Cadeia de Custódia é um documento que precisa ser produzido com o mesmo cuidado e atenção da própria cópia forense.

Nesse sentido, todo e qualquer procedimento de cópias forenses deverá, obrigatoriamente, possuir as informações de quem o realizou, quando (data e horário), como foi realizado (software e hardware utilizados) e de quem o material foi recebido e para quem foi entregue (custodiante), além da descrição completa da mídia copiada. O formulário padrão de cadeia de custódia, a ser utilizado em todo o MPF, está disponível para download em: <https://goo.gl/H27DMd>.

A duplicação de mídias, também conhecida como "espelhamento", é o nome dado ao processo de cópia integral dos dados contidos em uma mídia de armazenamento digital para outra.

Existem dois tipos de espelhamento:

a) espelhamento de mídia para mídia ou "cópia física" – feito diretamente para a mídia de armazenamento que será utilizada para o exame;

b) espelhamento de mídia para arquivo de imagem – feito para um arquivo que conterá todos os dados da mídia original.

Devido à maior flexibilidade para se analisar diversas mídias simultaneamente, à maior facilidade para se manter a integridade dos dados e à facilidade no gerenciamento de armazenamento de arquivos, recomenda-se o tipo de espelhamento "mídia para arquivo de imagem".

No caso de espelhamento de mídia para mídia, recomenda-se a utilização de mídia destino com tamanho igual ou superior ao da mídia de origem e a prévia realização do procedimento de wipe no disco rígido que receberá a cópia. Tal procedimento consiste no apagamento forçado das áreas de memória, inclusive sobrescrevendo todo o disco com informações ininteligíveis (utilizando, por exemplo, a ferramenta DBAN), garantindo, assim, que possíveis informações preexistentes sejam efetivamente eliminadas e não se confundam com as informações da mídia sendo copiada.

CAPÍTULO I – CATEGORIAS DE MÍDIAS DE ARMAZENAMENTO

NA AVALIAÇÃO DA NECESSIDADE DE ESPELHAMENTO, AS MÍDIAS DE ARMAZENAMENTO PODEM SER CLASSIFICADAS EM TRÊS CATEGORIAS:

A com interface de acesso direto aos dados e sem proteção contra gravação (ex.: discos rígidos, pendrives, alguns tipos de cartões de memória, alguns tipos de máquinas fotográficas): dispositivos nesta categoria somente devem ser acessados para a realização do espelhamento. Para alguns desses dispositivos, é possível prover proteção contra gravação por meio de ferramentas como bloqueadores de escrita, permitindo que sejam classificados na próxima categoria;

B com interface de acesso direto aos dados e com proteção contra gravação (ex.: CDs, DVDs, disquetes, alguns tipos de cartões de memória): para dispositivos nessa categoria o espelhamento é opcional, ou seja, eles podem ser acessados diretamente, desde que sejam tomados os cuidados adequados para que a proteção contra gravação esteja sempre ativa. Apesar desse tipo de acesso direto ser possível, ainda assim é recomendável a utilização do espelhamento, com vistas à diminuição dos riscos à integridade dos dados;

C sem interface de acesso direto aos dados (ex.: telefones celulares de modelos antigos): para tais dispositivos, o espelhamento é impossível. Os trabalhos periciais devem ser conduzidos diretamente por meio do manuseio do dispositivo, mas tomando-se precauções para minimizar as alterações de dados.

CAPÍTULO II – CÁLCULO DE HASH

1 As mídias de armazenamento computacional periciadas devem ser submetidas a duas funções unidirecionais de resumo (hash) visando a futuras verificações de integridade dos dados:

   A primeiro deve-se produzir um único valor calculado sobre o conteúdo integral da mídia, utilizando preferencialmente o algoritmo SHA-256. Tal procedimento tem por finalidade possibilitar a verificação de integridade preliminar da mídia e afastar a possibilidade de argumentação de colisões. Obs.: alguns equipamentos duplicadores não apresentam o recurso de cálculo de hash único para a mídia inteira; nesse caso, devem ser calculados os hashes parciais dos fragmentos do arquivo-imagem;

   B em seguida, deve-se produzir um valor calculado sobre cada um dos arquivos identificados na mídia pela ferramenta pericial empregada. Deve ser utilizado o algoritmo SHA-1 ou MD5, por serem os mais suportados pelas ferramentas periciais e por serem os mais utilizados nos conjuntos de hashes de arquivos conhecidos. Tal procedimento tem por finalidade possibilitar a verificação detalhada do conteúdo da mídia e garantir a integridade parcial em caso de falha no cálculo do hash integral da mídia.

2 Para mídias óticas (como CDs e DVDs) não deve ser feito o primeiro 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.

3 Mídias que, por conta de suas características, tenham sido preliminarmente identificadas pelo perito como irrelevantes para os exames – como CDs ou DVDs comerciais de música ou vídeo – não precisam ser submetidas aos procedimentos de cálculo de hash acima descritos.

4 Caso a mídia original apresente erros de leitura, o arquivo de log listando os setores defeituosos também deverá ser incluído na mídia anexa ao documento científico.

5 Nos casos em que, após a conclusão dos exames, não houver geração de mídia anexa, deve ser incluído no corpo do documento científico o hash único de toda a mídia examinada, quando houver.

CAPÍTULO III – DISCOS RÍGIDOS

1 Existem três formas para a realização do procedimento de espelhamento, utilizando:

A equipamento de duplicação;

B computador;

C interface externa (USB, Firewire, Ethernet).

2 O espelhamento com equipamento de duplicação é o método preferencial para a realização de exames em discos rígidos, pois não depende da confiabilidade de dispositivos bloqueadores de escrita e reduz o risco de falhas no disco. Excepcionalmente, quando houver alguma restrição de natureza operacional ou técnica, é possível utilizar um meio para bloquear a escrita, viabilizando inclusive o exame direto.

3 Alguns discos rígidos possuem áreas protegidas chamadas HPA – Host Protected Area e DCO – Device Configuration Overlay, que requerem comandos ATA especiais para serem acessadas. Quando habilitadas, essas áreas podem ser usadas para armazenamento de dados. Em um espelhamento normal, sem a desativação do HPA e/ou DCO, os dados residentes nessas áreas não são copiados. Assim, deve-se realizar os procedimentos para que tais áreas também sejam copiadas durante o processo de duplicação.

4 Deve-se tomar muito cuidado na definição dos discos de origem e destino durante os procedimentos de espelhamento, pois uma troca dos discos sobrescreverá os dados da mídia original. Esse procedimento deve ser bem controlado, principalmente se for designado para auxiliares.

5 Outra recomendação é a verificação da ordem de inicialização (ordem de boot) do computador. É imprescindível que essa ordem seja verificada antes do processo de espelhamento, para se garantir que o disco rígido questionado não esteja configurado para inicializar o equipamento. A inicialização inadvertida do computador a partir da mídia questionada poderia trazer grandes prejuízos para a integridade dos dados a serem examinados. Existem várias alternativas para a realização de espelhamento de discos rígidos, conforme descrito a seguir.

1 ESPELHAMENTO UTILIZANDO EQUIPAMENTO DE DUPLICAÇÃO

1 Além da facilidade de uso e bom desempenho, uma grande vantagem de utilizar um equipamento de duplicação é a garantia, quando corretamente utilizado, de que a mídia questionada não será alterada.

2 Como a utilização desse tipo de equipamento pressupõe o acesso direto à mídia original, pode ser utilizado nos casos em que seja possível retirar o disco rígido do equipamento original e conectá-lo ao equipamento de duplicação.

3 O equipamento ImageMaster Solo III, disponível na Sppea/PGR, realiza os dois tipos de espelhamento ("mídia para mídia" ou "mídia para arquivo-imagem"), possui suporte à desativação de DCO e HPA, mas não suporta o algoritmo de hash SHA-256. Esse equipamento, juntamente com o kit Tableau Hardware Blocker, possui interface para praticamente todos os tipos de discos rígidos.

2 ESPELHAMENTO UTILIZANDO COMPUTADOR

1 O espelhamento utilizando um computador apresenta maior flexibilidade na escolha de interfaces e software. É especialmente útil para casos de discos rígidos que não foram reconhecidos pelos equipamentos de duplicação ou quando é necessário um procedimento especial, como tolerância a erros ou recuperação de setores defeituosos.

2 De forma análoga ao espelhamento com equipamento de duplicação, esse tipo de procedimento pode ser utilizado nos casos em que seja possível retirar o disco rígido do equipamento original e conectá-lo ao computador que fará a cópia.

3 O grande problema de utilizar um computador comum para espelhamento é o risco de alterar acidentalmente os dados da mídia questionada. Por isso, a recomendação é a utilização de hardwares bloqueadores de escrita ou, na inexistência deste e em situações bastante limitadas, a utilização de bloqueio de escrita por software. Recomenda-se a utilização do sistema operacional Linux, preferencialmente uma distribuição para uso forense que já traga instaladas as principais ferramentas.

4 Para todos os casos, deve ser verificado se a solução de espelhamento adotada possui suporte à desativação de DCO e HPA, de modo a serem utilizados procedimentos que permitam a cópia dos dados presentes nessas áreas, se existentes.

5 Os itens a seguir descrevem as ferramentas de software que podem ser utilizadas para o espelhamento utilizando computador.

2.1 LINUX

1. A distribuição escolhida não deve montar partições automaticamente, para evitar possíveis alterações no disco a ser examinado.

2. A recomendação de distribuição Linux recomendada é o Caine, que é a distribuição homologada pela Anptic/Sppea.

3. Uma outra sugestão de distribuição Linux é o Helix, que é um CD de boot Linux criado especificamente para o trabalho pericial. Além de ferramentas Linux para espelhamento e análise, ele possui também programas de resposta a incidentes para Windows.

4. Outras opções a serem consideradas são a distribuição Raptor (utilizada para o espelhamento de alguns modelos de computadores da empresa Apple) e a DEFT Linux.

5. Em casos de mídias que apresentem erros de leitura, recomenda-se o uso da ferramenta GNU ddrescue com as opções "-d –r Y /dev/sdX image.dd image.log" (em que "Y" é o número de tentativas de leitura dos blocos defeituosos).

6. Para verificar se as áreas de DCO ou HPA do disco estão ativadas, podem ser utilizados os seguintes comandos:

    A. HPA: hdparm –N /dev/sdX; e

    B. DCO: hdparm –dco-identify /dev/sdX.

2.2 FTK IMAGER

1. Software de espelhamento gratuito da empresa AccessData. Roda sobre Windows, por isso só deve ser usado para espelhamento de mídias que estejam protegidas contra gravação. O FTK Imager também é útil para visualização de arquivos.

2.3 ENCASE ACQUISITION

1. O Encase, quando executado em uma máquina sem o dongle, entra em modo de aquisição. Como roda em Windows, só deve ser usado para espelhamento de dispositivos protegidos contra gravação. O espelhamento também pode ser realizado com o dongle plugado.

2.4 ENCASE LINEN

1 Software de espelhamento do Encase para Linux. Gera imagens no formato do Encase. Recomenda-se o uso do LinEn em versão maior ou igual a 6.0, pois essa versão é capaz de armazenar o número de série do disco rígido espelhado no arquivo-imagem. O Helix contém o LinEn, sendo que a versão 1.9 do Helix contém o LinEn 6.0.

3 ESPELHAMENTO POR INTERFACE EXTERNA

1 Nos casos em que não é possível ou conveniente retirar a mídia original do equipamento onde está instalada, pode-se realizar o espelhamento por meio de interfaces externas, como USB, Firewire, PCMCIA ou Ethernet. Esse tipo de procedimento também é útil quando a configuração de hardware da máquina original impede o espelhamento por outros meios, como em servidores com discos conectados a controladoras RAID.

2 No caso de se deparar com uma estrutura em RAID (exceto RAID 1), pode ser necessária a cópia dos arquivos no local, e deverão ser observadas as técnicas expostas neste documento, aproveitando-se assim a mesma estrutura física/lógica em que o RAID foi montado e está ativo. Isso é importante, pois pode haver algum fator que depois impossibilite replicar o ambiente de onde a evidência foi retirada.

3 Como nesses casos o hardware original será utilizado para fazer a cópia, é de extrema importância verificar a ordem de boot dos dispositivos no BIOS, de modo a garantir que o sistema operacional original não seja inicializado.

3.1 ETHERNET

1 Nesta modalidade são utilizadas as interfaces Ethernet do equipamento original e do computador que receberá a imagem, conectadas por meio de uma rede ou de um cabo crossover.

2 A maneira mais simples de realizar esse espelhamento é utilizando o aplicativo netcat, uma ferramenta de linha de comando disponível tanto no Linux quanto no Windows, voltada para a transferência de dados sobre uma rede IP. Recomenda-se utilizar o CD de boot do Helix na máquina de origem.

3 Caso a rede utilizada para a cópia não seja segura, deve-se utilizar um serviço SSH.

3.2 USB/FIREWIRE

1 Caso se disponha de um disco rígido externo com interface USB ou Firewire, pode-se realizar o espelhamento inicializando-se a máquina de origem com o CD do Helix empregando os mesmos comandos mencionados na seção “Espelhamento utilizando computador”, em que o disco rígido externo receberá a imagem gerada a partir do disco original.

CAPÍTULO IV – DISPOSITIVOS DE MEMÓRIA FLASH

1 Alguns exemplos de memória flash são os USB flash drives (pendrives), cartões de memória (Secure Digital, Memory Stick etc.) e a memória interna de alguns dispositivos, como das máquinas fotográficas e de alguns modelos de notebooks.

2 Assim como os discos rígidos, tais dispositivos também sofrem alterações em seu conteúdo ao serem conectados a um computador com sistema operacional Windows. Embora alguns dispositivos possuam uma espécie de “chave” para ligar ou desligar o acesso para escrita, não é recomendável confiar nesse tipo de recurso. Pelas mesmas razões que os discos rígidos, recomenda-se realizar o exame sobre a cópia ou arquivo-imagem gerado a partir do original.

3 Os métodos para espelhamento desse tipo de dispositivo são os mesmos descritos na seção “Espelhamento utilizando computador”. Alternativamente, se for utilizado um bloqueador de escrita, recomenda-se a desativação da função autorun para o exame de dispositivos de memória flash, com a finalidade de proteger a estação pericial da execução de software estranho ou malicioso.

CAPÍTULO V – MÍDIAS ÓTICAS (CD/DVD/BLU-RAY)

1 Embora seja relativamente seguro o exame direto desse tipo de mídia, é necessário considerar o risco de dano ao material causado pela manipulação. Sendo assim, é recomendável que sejam gerados arquivos-imagem dos discos óticos por meio de software adequado, como o FTK Imager.

2 Além disso, discos com múltiplas sessões podem conter dados de sessões anteriores que não sejam diretamente acessíveis, devendo ser feita a verificação da existência de múltiplas sessões por meio de software como o FTK Imager ou o ISOBuster.

3 Como medida de segurança, recomenda-se a desativação da função autorun para o exame de CDs, DVDs e Blu-ray. Cuidados adicionais devem ser tomados ao lidar com mídias óticas rachadas ou de algum modo desbalanceadas (por exemplo, com etiquetas não uniformes), pois esses discos podem estilhaçar-se dentro do drive.

4 Recomenda-se que a mídia ótica seja visualizada antes da sua utilização, em busca de sujeiras ou arranhões. Caso existam, a leitura dos dados poderá ser prejudicada.

5 Caso esteja apenas suja, geralmente com manchas de gordura ou poeira, basta uma simples lavagem em água corrente e sabão neutro. Após uma breve lavagem, secar a mídia de forma lenta e minuciosa, utilizando para isso um pano seco e macio. A mídia deve estar completamente seca antes de ser inserida no drive para leitura.

6 Caso a mídia ótica esteja arranhada de forma não muito profunda, é possível realizar um procedimento de recuperação. Esse procedimento retira uma fina camada da superfície com a utilização de uma pasta abrasiva própria e um equipamento especial para rotacionar o disco.

CAPÍTULO VI – FITAS MAGNÉTICAS

1 Fitas magnéticas geralmente possuem trava de proteção contra gravação. Dessa forma, ao contrário dos discos rígidos, é possível acessar o conteúdo de uma fita DAT sem alterá-lo, mesmo no sistema operacional Windows.

2 Como existem muitos formatos e programas diferentes de backup para fitas, é recomendável utilizar no processo de recuperação o mesmo programa que gravou os dados. Também vale lembrar que em uma busca e apreensão deve-se tentar arrecadar tanto o leitor de fitas quanto o servidor que possui o programa de backup instalado. É aconselhável fazer alguns testes com o programa antes de utilizar a fita a ser examinada.

3 Nos casos em que não for possível a arrecadação tanto do leitor das fitas quanto do servidor que possui o programa de backup, deve-se tentar a extração dos dados no local da busca e apreensão. Em geral, para isso faz-se necessária a colaboração de um funcionário do local. Os dados devem ser copiados para uma mídia eletrônica (disco rígido externo, por exemplo) e essa mídia então deve ser formalmente apreendida.

4 O espelhamento pode ser dispensado se a trava de proteção for utilizada e se os procedimentos forem testados antes de serem aplicados. Caso a restauração do backup não seja viável, deve-se tentar realizar o espelhamento da fita.

CAPÍTULO VII – ACESSO AOS DADOS UTILIZANDO BLOQUEADORES DE ESCRITA

1 BLOQUEADOR DE ESCRITA VIA SOFTWARE

1 O acesso aos dados de uma mídia utilizando bloqueio de escrita via software é um procedimento não recomendado e que deve ser utilizado apenas se não houver outras opções que permitam maior garantia de integridade dos dados a serem examinados. Ao utilizar bloqueio de escrita via software, deve-se ter o cuidado de não se reiniciar o computador com o dispositivo examinado conectado, pois, durante a inicialização, o bloqueio não fica ativo.

2 O acesso aos dados por bloqueador de escrita via software pode ser feito de duas formas:

A com o uso do FastBlock SE do Encase: essa é a maneira mais segura e recomendável;

B com a modificação de uma chave de registro do Windows: essa opção não é recomendável, considerando-se os grandes riscos para a integridade dos dados. Deve ser utilizada apenas em último caso. Para bloquear a escrita em todos os dispositivos USB, no caso do Windows XP Service Pack 2 ou posterior, modificar a seguinte chave de registro: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]”WriteProtect” = dword:00000001

2 TABLEAU COMO BLOQUEADOR DE ESCRITA

1 O equipamento Tableau pode ser utilizado como bloqueador de escrita para discos rígidos. Quando utilizado dessa forma, o disco examinado deve ser colocado conectado ao Tableau. A ligação com o computador pericial é feita usualmente por meio da interface USB.

CAPÍTULO VIII – SOFTWARES FORENSES

1 Para cada etapa da análise forense – preservação, extração dos dados, análise e apresentação – existe determinado software apropriado, que deverá ser utilizado conforme o caso e exclusivamente por pessoal qualificado, tais como: Guidance EnCase, AccessData Forensic Toolkit (FTK), X-Ways Forensics, The Sleuth Kit (TSK), UFED 4PC, entre diversos outros. A Polícia Federal brasileira também dispõe de alguns aplicativos como: Indexador e Processador de Evidências Digitais (Iped) e NuDetective (para investigações de pornografia infantojuvenil).

GLOSSÁRIO

BIOS – Sistema gravado em memória não volátil na placa-mãe de computadores, responsável por inicializar e testar seus componentes de hardware e por carregar o programa (bootloader) que irá inicializar o sistema operacional.

DCO – Área escondida em alguns discos rígidos geralmente não acessível pela BIOS, sistema operacional ou pelo usuário.

Firewire – Padrão de interface serial de entrada e saída de dados de alta velocidade.

Hash – Na área de Computação Forense, refere-se ao resultado de funções unidirecionais de resumo criptográficas, ou seja, funções que mapeiam conjuntos de dados de tamanho arbitrário em um conjunto de dados de tamanho fixo, sendo probabilisticamente improvável que mensagens de entrada diferentes resultem em um mesmo valor de hash. É utilizado para garantir a integridade e/ou autenticidade de conteúdos digitais.

HPA – Assim como o DCO, é uma área escondida em alguns discos rígidos, acessível apenas via software ou firmware que seja "HPA aware". Normalmente, sistemas operacionais e usuários, usando comandos padrão da controladora do disco, não têm acesso a essa área.

RAID – Tecnologia de armazenamento de dados que combina dois ou mais discos para oferecer maior tolerância a falhas e/ou desempenho.

SSH – Protocolo criptográfico para implementar comunicação segura de dados via rede.

Wipe – Procedimento pericial para apagar dados presentes em mídias de armazenamento computacionais.

MPF

Ministério Público Federal