FORENSE COMPUTACIONAL

SOLUÇÕES EDUCACIONAIS INTEGRADAS

Análise relacionada à pornografia infanto-juvenil

Thaís Bison

OBJETIVOS DE APRENDIZAGEM

- Identificar os itens que podem ser periciados e suas peculiaridades.
- Descrever as metodologias e as ferramentas para realizar os exames na internet.
- Explicar a análise dos vestígios.

Introdução

Em tempos de acesso fácil à internet, o público infantil, mais vulnerável, tem navegado na internet, não raro, sem qualquer supervisão. O crescimento no número de crimes virtuais relacionados à pornografia infanto-juvenil chama a atenção de peritos criminais. Com a popularização da internet e dos novos meios de comunicação, como *smartphones* e *notebooks*, abusadores se aproveitam da possibilidade de anonimato durante os primeiros contatos para alcançar um número maior de vítimas simultaneamente, sem a necessidade de exposição pessoal.

Neste capítulo, você vai estudar os vestígios de pornografia infanto-juvenil, identificando itens que podem ser periciados, além dos métodos e recursos necessários para realizar esse tipo de exame, especialmente nos casos em que os criminosos utilizam a internet como meio de exploração.

Itens para perícia

O aumento de crimes virtuais de pornografia infantil tem exigido atenção redobrada dos peritos criminais, além de investimentos em tecnologia forense. Para atuar em investigações contra essa prática criminosa, os peritos contam com *softwares* e *hardwares* de inteligência forense, que permitem:

- coletar, analisar e identificar criminosos em pouco tempo e na cena do crime;
- analisar mídias, como computadores, HDs, *pen-drives*, cartões de memória e celulares;
- analisar diversos tipos de arquivos, como imagens, vídeos, documentos;
- detectar nudez e pornografia infantil em arquivos armazenados em diversas mídias;
- gerar relatórios das análises periciais.

O indivíduo que utiliza sistemas computacionais com o intuito de realizar crimes de pornografia infanto-juvenil produz vestígios de naturezas lógica ou física, deixando evidências que podem ser identificadas para resolver um fato ou crime. Essas pessoas usam diversos meios para ocultar arquivos que contenham materiais pornográficos associados a crianças e adolescentes, a exemplo de arquivos de mídia, como HDs, *pen-drives*, CDs, cartões de memória, memória de celulares. Essas análises estão entre os exames periciais mais comuns. Devemos tratá-los com o máximo de cuidado, porque são fonte valiosa de provas. Ter clareza sobre o que se quer apurar e provar é o principal ponto para identificar corretamente os vestígios.

À medida que os itens são identificados na cena do crime, algumas providências podem ser tomadas para garantir o isolamento dos vestígios, evitando ataques à integridade das evidências. No isolamento físico, a regra é isolar a maior área possível dentro do contexto do crime. Isso porque o isolamento insuficiente pode levar à perda ou à contaminação de vestígios importantes, já que estão fora do perímetro de isolamento e sujeitos à manipulação indevida. Confira a seguir alguns pontos que devem ser observados.

- Região imediata: com maior concentração de vestígios da ocorrência do fato.
- Região mediata: periferia da região imediata.

- Preservação idônea: situação em que os vestígios são mantidos inalterados desde que ocorre o fato até que os profissionais registrem os vestígios.
- Preservação inidônea: quando há comprometimento dos vestígios, seja por remoção, inserção ou combinação de ambas, o que gera a substituição da evidência.
- Área interna: tem pelo menos uma proteção superior contra chuva, sol e outros elementos naturais.
- Área externa: situa-se fora das instalações e tem influência dos elementos naturais.
- Área virtual: não está vinculada diretamente aos contextos físico e lógico.

No caso de *notebooks* e *desktops*, na maioria das vezes, as informações mais relevantes a serem isoladas estão em alguma mídia secundária de armazenamento, como HD, *pen drive*, HD externo, etc. Isso faz com que apenas esses dispositivos de armazenamento necessitem ser isolados para posterior coleta. Em alguns casos, a máquina inteira deverá ser identificada e isolada, como as que utilizam arranjos de disco RAID. Do ponto de vista físico, encontramos vários HDs e, do ponto de vista lógico, temos um único disco.

Se encontrarmos esses equipamentos desligados, não devemos ligá-los, pois a inicialização do sistema operacional provoca alterações em determinadas regiões da mídia de armazenamento secundária. Além disso, alguns programas podem efetuar atividades não desejadas, o que pode comprometer a integridade dos vestígios. Tendo a necessidade de análise desse tipo de mídia *in loco*, devemos ter cuidado com a proteção contra escrita. Pode-se fazer a inicialização por outro sistema operacional armazenado em outra mídia. Dessa forma, não produzirá alterações na mídia questionada. Caso encontremos essse equipamentos ligados, deve-se proceder a uma análise de viabilidade de registro da evidência em situações de flagrância. A coleta do conteúdo da memória primária, geralmente volátil, deve ser ponderada, pois podemos encontrar arquivos compartilhados, programas de compartilhamento abertos, janelas de *sites* abertas, sessões de navegação em andamento, conversas em *softwares* de comunicação, etc. Além disso, se os equipamentos estiverem alimentados eletricamente por baterias, elas devem ser removidas e não mais inseridas, desligando abruptamente o equipamento. Caso sejam abastecidos diretamente pela rede elétrica via cabos, estes devem ser retirados.

Fique atento

Dispositivos de entrada e saída, via de regra, não devem ser coletados, mas, em casos específicos, sua identificação e isolamento são fundamentais para a elucidação do caso, como uma impressora responsável pela impressão de imagens de pornografia infanto-juvenil ou um escâner utilizado na captura de imagens de menores.

Mídias avulsas, como mídias ópticas, *pen drives*, HDs externos, cartões de memória, etc., podem ser encontradas conectadas aos computadores ou dentro de seus equipamentos originais, como filmadoras ou máquinas fotográficas. Apesar de se tratar de uma filmadora ou de uma máquina fotográfica, a memória ali contida se comporta como qualquer outra memória, sendo possível armazenar outros tipos de arquivos.

É de suma importância separar as mídias não sensíveis à escrita (como CD e DVD) das que são sensíveis à escrita, pois aquelas podem ser manuseadas sem grandes riscos de que o conteúdo seja alterado. Isso porque sua natureza somente de leitura já é o bloqueio natural contra modificações, enquanto as mídias sensíveis à escrita precisam ser protegidas física ou logicamente, evitando transformações indesejadas.

Os discos rígidos internos aos computadores podem ser inicialmente analisados *in loco* ou recolhidos para análise em laboratório. Para a análise direta no computador, sem a retirada, é recomendável usar outra mídia, como *pen drive* e disco de *boot*, para inicializar outro sistema operacional sem modificar as mídias sob análise. Se, na fase de identificação, algum dispositivo for identificado como importante, e a evidência lógica puder ser extraída sem necessidade da coleta física, cópias poderão ser feitas no local.

Equipamentos conectados em rede, por sua vez, devem ser desconectados desligando-se como padrão ou tirando-se o cabo da rede. Durante a análise de redes de internet, caso haja suspeitas de pornografia infanto-juvenil, é necessário solicitar dados ao provedor de internet que está disponibilizando a rede periciada. Isso pode ser feito diretamente na empresa ou por intermédio de um mandado de busca e apreensão. Esses dados coletados, como IP da rede, dados do cliente (nome e endereço, por exemplo), serão de grande importância para o reconhecimento do criminoso que está por trás da ação. Diante do endereço IP informado pela empresa fornecedora do serviço, é possível identificar o responsável consultando as bases de dados públicas.

> Com os dados em mãos, o responsável pela investigação poderá identificar, analisar e coletar as evidências corretamente. Com base nisso, poderá garantir que "a informação obtida é a representação dos dados originais extraídos da aplicação de internet e que os passos para a preservação da evidência foram seguidos e o conteúdo não sofreu alteração" (BARRETO; BRASIL, 2016, p. 30).

Os provedores armazenam os registros de conexão pelo prazo de um ano, e as aplicações de internet, por seis meses. Todavia, contados sessenta dias do pedido cautelar, deve haver uma representação judicial aos provedores embasando-o. Por isso, tão logo tome conhecimento da prática do crime:

> [...] o delegado de polícia deverá expedir ofício direcionado ao provedor de conexão ou de aplicação de internet, indicando formas de localização do suposto ilícito, como perfil do usuário, conta de *e-mail*, URL e outros dados uteis que individualizem os fatos e apontem os indícios referentes à autoria (BARRETO; BRASIL, 2016, p. 30).

A mudança da computação tradicional para a computação em nuvem fez com que informações relacionadas possam estar separadas geograficamente. Assim, é possível acessar esses arquivos de qualquer dispositivo computacional em qualquer local. Um dos principais vestígios que podemos coletar durante a investigação de um crime de pornografia infanto-juvenil, portanto, é o endereço IP, que deve estar acompanhado de data, hora exata da conexão ou comunicação e fuso horário do sistema. Após a localização do provedor de acesso responsável pelo IP, o órgão competente deverá requerer ao juiz um pedido de quebra de sigilo de dados telemáticos para que seu provedor de acesso revele as informações do usuário vinculado, numa determinada data e num determinado horário.

Além disso, podemos encontrar muitas evidências de crime de pornografia infanto-juvenil em *e-mails*. Para análises desse tipo, precisamos considerar a origem e a autoria. É preciso não apenas preservar o conteúdo da mensagem, como também identificar remetente e destinatário pelo cabeçalho do *e-mail* e descobrir o endereço IP, a data, a hora da transmissão e o fuso horário. Caso a mensagem tenha anexos, devemos ter cuidado, pois, para examiná-los, é necessário baixar o arquivo, o que pode levar a uma infecção no nosso próprio computador. Como alternativa, é possível abrir em uma máquina virtual.

Ao analisarmos *sites*, a primeira ação a ser feita é a cópia de todo o conteúdo, que é possível com acesso *off-line*, copiando e preservando informações, evitando a perda de vestígios caso o *site* seja retirado do ar. Quando o *site* periciado está *on-line*, a cópia do seu conteúdo pode ser realizada por meio de aplicativos (específicos para esse fim) ou de um utilitário gratuito, o HTTrack. Caso não esteja mais disponível na internet, podemos usar alguns

serviços que realizam cópias de conteúdos já existentes. Outra opção é o serviço de cache do próprio buscador Google: ao fazer uma pesquisa por assunto, o buscador exibirá um pequeno triângulo ao lado de cada resultado; quando clicamos nele, temos acesso ao *site* que está armazenado em cache. Depois de preservar a prova, o passo seguinte é a identificação do servidor que hospeda a página. Há ferramentas de busca na internet que fazem o serviço, sendo antes necessário verificar se a página é nacional ou estrangeira. O resultado dessa pesquisa fornecerá informações importantes, como o nome do responsável pelo domínio e o provedor.

Um tipo de comunicação tem sido frequentemente usado por adultos para atrair e seduzir crianças ou para trocar fotos, vídeos e conteúdo de pornografia infanto-juvenil: as salas de bate-papo. Elas obrigatoriamente passam por um servidor de provedor, que pode manter *logs* das conversas em seus domínios. De posse do nome ou apelido do investigado e da data/horário em que ocorreu a conversa, os órgãos competentes deverão requerer judicialmente a quebra do sigilo de dados telemáticos, para que o provedor forneça o endereço IP utilizado pelo investigado, a data e a hora.

Nos telefones móveis, *smartphones* e *tablets*, o cuidado deve ser o mesmo adotado em computadores pessoais e *notebooks*: isolamento, coleta, preservação. Muitos são os tipos de vestígios encontrados nesses aparelhos, como vestígios físicos de interesse em investigação ou que requeiram cuidados especiais na manipulação, como impressões digitais e amostras de DNA, que acabam criando um vínculo inquestionável entre o usuário do equipamento e o conteúdo. Em aparelhos bloqueados por senhas geometricas, uma exposição cuidadosa da tela do aparelho pode revelar o padrão de desbloqueio, uma vez que ele é repetido diversas vezes em movimento contínuo de arraste sobre a tela. O exame deve ser realizado imediatamente, pois o atrito entre a tela do aparelho e os contatos durante a apreensão pode destruir o vestígio.

A coleta de dados voláteis em aparelhos portáteis deve ser feita da mesma forma que em computadores. Se no momento da apreensão o equipamento portátil estiver ligado, pode haver informações voláteis importantes na memória, chaves da parte de sessões criptografadas ou, até mesmo, a senha de desbloqueio do aparelho. Em equipamentos que estão conectados a um computador durante a apreensão, interromper uma atualização de *software* ou *backup* pode corromper o sistema de arquivos. Além disso, um processo de sincronização pode estar em andamento, podendo causar a sobreposição de dados nos dispositivos móveis.

Na extração de dados em celulares e *tablets*, quando é analisado o cartão de memória, devem ser seguidos os mesmos procedimentos de exame de mídias de armazenamento computacional clássica. As mídias são duplicadas com bloqueadores de escrita, e os exames são feitos na cópia com as ferramentas forenses apropriadas. Os cartões de memória em dispositivos móveis servem para armazenar grandes quantidades de arquivos de mídia, como fotos, vídeos e áudio. Os cartões SIM já requerem a utilização de ferramentas forenses específicas, porque é um cartão inteligente, protegido por criptografia. A extração de dados da memória interna dos aparelhos portáteis pode ser feita de forma manual, lógica, física e avançada.

Aplicativos de mensagens instantâneas, como WhatsApp, Telegram e Messenger também devem ser analisados. A troca de mensagens contendo material de pornografia infanto-juvenil também é crime. Por mais que o criminoso apague essas mensagens, é possível recuperar o conteúdo nos *backups* que o aplicativo faz. Redes sociais, como Facebook, TikTok, Twitter, entre outros, também não podem passar em branco durante uma perícia. Por serem redes mundialmente usadas e de fácil acesso em vários dispositivos digitais (*notebooks*, *tablets*, *smartphones*), os usuários que cometem algum crime relacionado à pornografia infanto-juvenil as utilizam como parte do seu modo de operação, para planejar e executar os crimes. Além disso, elas facilitam o anonimato. Pela análise dessas redes sociais, podemos descobrir de onde é o criminoso, com quem ele conversou, imagens que revelam o crime, entre outras informações.

Informações inseridas nas rede sociais podem ser apagadas pelo usuário a qualquer momento, mas é possível recuperá-las por meio de ferramentas forenses específicas ou do histórico de armazenamento da própria rede social. Conteúdos do Facebook e do Twitter, como fotos, mensagens, vídeos e *links*, podem ser facilmente copiados para um dispositivo de armazenamento com as mesmas técnicas usadas numa análise de página da *web*. Primeiro, deve-se fazer a cópia de todo o conteúdo para preservar as informações. Se a rede social estiver *on-line*, o conteúdo deve ser copiado por meio de aplicativos específicos para este fim. Caso a rede social não esteja mais disponível na internet, podemos usar serviços que realizam cópias de conteúdos já existentes. Após a preservação da prova, deve-se indetificar o servidor que hospeda a página para obter informações importantes, como o nome do responsável pelo domínio e o provedor em que o *site* está hospedado. O Facebook e o Twitter, por exemplo, dispõem de um recurso para baixar uma cópia dos dados.

Algumas redes sociais e serviços de troca de mensagem, como WhatsApp, utilizam a criptografia de ponta a ponta, recurso de segurança que protege os dados durante uma troca de mensagens, de forma que o conteúdo só possa ser acessado pelos dois extremos da comunicação: o remetente e o destinatário. Isso significa que pessoas sem autorização, como peritos sem um mandato judicial, não vão conseguir acesso aos dados, o que é um desafio para as investigações, porque quebrar essa criptografia sem ter acesso ao equipamento ainda não é possível. A identificação do usuário do Facebook pode ocorrer de duas maneiras: pelo ID do usuário e pelo nome do próprio usuário que aparece depois do domínio. No Twitter, a identificação é caracterizada pelo nome do usuário, logo após o domínio, na barra de endereços do navegador. Essa ferramenta também tem uma identificação numérica composta de uma quantidade variável, e é possível encontrá-la em *sites* que oferecem esses serviços.

Outros vestígios podem ser encontrados nas redes sociais, como linha do tempo, publicações, compartilhamentos, fotos, vídeos, localização, informações pessoais, interesses, publicações de amigos e grupos. O Facebook, por exemplo, registra todas as atividades por meio de marcas temporais, dados de extrema importância no ponto de vista forense, pois permitem que os investigadores se certifiquem de quando o evento realmente ocorreu. Além disso, o Facebook permite identificar se uma postagem na página originou-se de um computador por meio de um navegador ou por um dispositivo móvel como celular.

A identificação de arquivos de pornografia infanto-juvenil necessita continuamente de avanços, porque, normalmente, arquivos desse tipo estão armazenado em dispositivos com milhões de outros arquivos. Usar técnicas computacionais e ferramentas automatizadas que auxiliem na identificação desse tipo de conteúdo é fundamental para o sucesso das análises. Nesses casos, os exames podem ser realizados no local do crime, com busca e apreensão, ou em laboratório. Nos exames em locais de crime, podemos encontrar diversos dispositivos de armazenamento com dados no formato digital, como celulares, *tablets*, câmeras, filmadoras, computadores, etc. Durante a busca, deve-se ter atenção às novas tecnologias, para que todos os materiais que possam ter relação com o fato investigado sejam considerados e, havendo indícios de crimes, deve-se garantir a preservação dos dados contidos nesses dispositivos.

Fique atento

Manter, em qualquer dispositivo, fotos e vídeos com cenas de sexo explícito ou pornográficas envolvendo crianças e adolescentes é o mesmo que armazená-las e constitui a posse de pornografia infanto-juvenil. Se algum amigo, parente, conhecido ou desconhecido enviar a você materiais dessa natureza para demonstrar sua indignação ou com o objetivo ajudar a identificar e localizar os criminosos, apague imediatamente e avise-o de que essa conduta também configura uma forma de violência sexual: o crime de divulgação de pornografia infanto-juvenil. Se você armazena, também pratica crime e pode ser responsabilizado por isso.

Legislação

Os meios de violência sexual contra crianças e adolescentes têm crescido muito nas últimas décadas, sobretudo devido ao fácil acesso à internet, à modernização dos meios de comunicação e à variedade de equipamentos e mecanismos para captura de imagens e vídeos, como *smartphones*, câmeras e filmadoras digitais.

Os crimes relacionados ao abuso e à exploração sexual de crianças e adolescentes estão previstos nos arts. 240 a 241-E do Estatuto da Criança e do Adolescente (ECA), Lei nº 8.069, de 13 de julho de 1990. O art. 240 (BRASIL, 2019) inclui nesses crimes produzir, reproduzir, dirigir, fotografar, filmar ou registrar cenas de sexo explícito ou pornográficas envolvendo crianças e adolescentes com o objetivo de satisfazer o próprio agressor ou para comercialização. A pena é de quatro a oito anos de prisão e multa. Essa punição também se aplica a quem agencia, facilita, recruta, coage ou intermedeia a participação de menores em cenas de sexo explícito ou pornográfica, bem como quem com eles contracena.

O art. 241 do ECA (BRASIL, 2019) prevê que é crime a venda de pornografia infanto-juvenil, incluindo a comercialização e exposição à venda de fotografias, vídeos ou outros registros que contenham cenas de sexo explícito ou pornográficas envolvendo criança ou adolescente. A pena é de quatro a oito anos prisão e multa. O mesmo artigo prevê a divulgação de pornografia infanto-juvenil, praticada por quem oferecer, trocar, transmitir, distribuir, publicar ou divulgar imagens, vídeos ou outro registro contendo cena de sexo explícito ou pornográficas envolvendo menores por qualquer meio, inclusive por meio de sistema de informática ou telemático. A pena é de três a seis anos de prisão e multa, que será igualmente imposta àquele que garante os meios ou serviços para que se proceda ao armazenamento desse conteúdo e/ou assegura o acesso a ele pela internet. Também ocorre a violência sexual

contra menores quando há posse de pornografia infanto-juvenil, que se materializa no adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 2019, art. 241-B). A pena varia de um a quatro anos de prisão e multa.

Além disso, é crime, segundo o ECA (BRASIL, 2019, p. 115, art. 241-D), o aliciamento de crianças, que consiste em "[...] aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso". As punições para este crime são de um a três anos de prisão e a multa, que também são aplicadas a quem facilita ou induz o acesso da criança a material pornográfico objetivando com ela praticar ato libidinoso. Um exemplo ocorre na situação em que o adulto mostra a pornografia para a criança com a intenção de despertar nela o interesse sexual e, depois, praticarem atos libidinosos. Também caracteriza esse crime praticar o aliciamento com o intuito de induzir a criança a se exibir de forma pornográfica ou sexualmente explícita (BRASIL, 2019, art. 241-D, § 1o, II). É o caso, por exemplo, do criminoso que pede à criança que se exiba nua, seminua ou em poses eróticas diante de uma *webcam* ou pessoalmente.

Saiba mais

O aliciamento de crianças consubstancia-se na conduta conhecida pela expressão em inglês *child grooming*, isto é, assédio sexual pela internet, que se desenvolve por contatos assíduos e regulares e pode envolver a lisonja, a simpatia, a oferta de presentes, dinheiro, supostos trabalhos de modelo, chantagem e intimidação.

Por fim, constitui uma forma de violência sexual a submissão de criança ou adolescente à prostituição ou à exploração sexual, com pena de 4 a 10 anos de prisão, multa e perda de bens e valores empregados na prática criminosa em benefício do Fundo dos Direitos da Criança e do Adolescente do respectivo Estado ou Distrito Federal em que foi praticado o crime, ressalvado o direito de terceiro de boa-fé (BRASIL, 2019, art. 244-A). Essas mesmas penas são aplicadas em relação ao proprietário, gerente ou responsável pelo estabelecimento em que se constate a submissão de criança ou adolescente às práticas de prostituição ou à exploração sexual. Um efeito obrigatório da condenação é a cassação da licença de localização e funcionamento do estabelecimento acima referido (BRASIL, 2019, art. 244-A, §§ 1º e 2º).

Saiba mais

A produção de pornografia infanto-juvenil simulada também está classificada como crime de exploração sexual de crianças e adolescentes. Trata-se da montagem, isto é, da conduta de "[...] simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual" (BRASIL, 2019, p. 114, art. 241-C). A pena é de um a três anos de prisão e multa.

Metodologias e ferramentas para exames na internet

Criminosos sexuais normalmente tentam conquistar a confiança dos menores, tornando-se seus "amigos virtuais". Utilizam *chats* e redes sociais para se aproximarem de suas vítimas, principalmente pela facilidade de acesso dos *smartphones*. Inúmeras crianças com pouca idade já têm acesso a esses aparelhos e utilizam diversos aplicativos de comunicação instantânea, como WhatsApp, Skype, Telegram, Facebook, Likee, TikTok, entre outros. Confira a seguir possíveis ferramentas e métodos para encontrar esses criminosos dependendo do meio examinado.

- Endereços IP: é um dos principais vestígios que podemos encontrar. Deve estar acompanhado de data, hora exata da conexão e fuso horário do sistema. Para identificar qual provedor nacional é responsável por determinado endereço IP, podemos usar ferramentas *on-line* de consulta a registros. O site *What is my IP*, por exemplo, fornece informações sobre um endereço IP localizado no exterior.
- *E-mails*: é preciso preservar o conteúdo da mensagem e identificar remetente e destinatário, sendo o objetivo final descobrir o endereço IP, a data, a hora e o fuso horário da transmissão. Os cabeçalhos das mensagens têm muitas informações, como várias linhas começando com a palavra *received*, que marca por quantos servidores a mensagem passou antes de chegar ao destinatário.
- Páginas *web*: o objetivo é verificar o conteúdo e determinar os responsáveis pela publicação. Deve-se realizar a cópia de todo o conteúdo do *site*, para ter acesso *off-line* e preservar as evidências caso ele saia do ar. Na análise *on-line*, a cópia do conteúdo pode ser feita por aplicativos como WGET e HT-Track, que permitem baixar todo o

site ou partes dele. Para identificar o servidor que hospeda a página, há ferramentas de busca na internet, como o TLD. A pesquisa retornará o nome dos responsáveis pelo domínio e o provedor em que a página está hospedada.

- Comunicação instantânea: passa por servidores de provedor que disponibilizam as salas de *chat* e podem manter *logs* de conversas em seu domínio. Sabendo o nome ou o apelido usado pelo suspeito, a data e o horário que ocorreram as conversas, deverá ser requerida judicialmente a quebra do sigilo de dados telemáticos, para que o provedor forneça o endereço IP utilizado pelo suspeito, a data e o horário.
- *Deep web*: são necessárias técnicas e procedimentos na tentativa de identificar origem, destino e conteúdo do tráfego de dados, como extração de metadados de fotos e vídeos publicados na *deep web*, captura de características do navegador usado, resolução, idioma, fontes instaladas, etc.
- Redes sociais: informações inseridas nas redes sociais são sensíveis e podem ser apagadas pelo usuário a qualquer momento. No entanto, é possível recuperá-las com ferramentas forenses específicas ou com o histórico de armazenamento da rede social.

Análise de vestígios

A análise desse tipo de material segue uma metodologia de trabalho para o manejo das evidências digitais dividida em quatro etapas: identificação, preservação, análise e apresentação dos resultados. Em todas as etapas, os procedimentos devem ser padronizados. Utilizam-se técnicas e ferramentas, atentando-se a dar respostas aos pontos solicitados em juízo.

Busca ao vivo

Depois que todas as evidências foram processadas com algum *software* forense, cada um dos elementos obtidos pelo *software* é comparado com os objetos da pesquisa. Tem a vantagem de ser muito simples, mas a desvantagem de ser muito lenta e sujeita a erros, como a modificação das provas durante o manuseio.

Filtro de imagem

Permite selecionar um subconjunto dos elementos analisados aplicando alguns critérios, sendo uma maneira de limitar o tempo da pesquisa ao vivo. Usando um *software* forense, pode-se optar por exportar apenas arquivos de imagem para pesquisar esse subconjunto de evidências. É uma técnica mais rápida que a anterior, pois descarta os arquivos que não devem ser verificados, mas também está sujeita a erros.

Filtro de metadados

Metadados são dados que servem para descrever a estrutura do conjunto de um dado principal, como data de criação, tamanho, etc., evidenciando a utilidade das informações dos dados. Por exemplo, os dados EXIF contêm informações sobre como uma fotografia foi tirada, incluindo a câmera (marca, modelo, etc.). Usando os metadados das imagens pesquisadas, os filtros podem ser refinados. Sabendo o tamanho, a data de modificação ou os dados EXIF das imagens pesquisadas, o *software* forense pode ser configurado para filtrar as imagens que correspondem a esses valores com as imagens pesquisadas.

Os metadados podem ser verificados, além de em imagens e fotos, em arquivos de extensões variadas, como editores de texto (doc, pdf, ppt, etc.). Quando um arquivo é copiado, carregado ou baixado em qualquer lugar, seus metadados o acompanham. A visualização não ocorre pela execução do arquivo propriamente dito, mas pode ocorrer por vários caminhos, que apresentarão diversos níveis de acesso a informações gravadas nos arquivos. A análise dos metadados dos arquivos funciona como valioso recurso de coleta de dados, traduzindo-se como verdadeira impressão digital daquele arquivo, possibilitando individualizar sua criação, modificação, origem, marcação geográfica, entre outros.

Filtro de tom de pele

Algumas ferramentas forenses incluem um analisador de tom de pele entre suas funções. Essas ferramentas têm a capacidade de identificar de forma rápida e eficaz os arquivos de interesse com base na porcentagem do tom de pele contido nele. Para isso, utilizam tecnologia de análise de imagens baseadas em pixels. Feita essa análise, é gerada uma galeria organizada por conteúdo de tons de pele. Isso torna possível acelerar a busca por vestígios

de pornografia infantil. A vantagem dessa técnica é a automação de parte do reconhecimento de fotos.

Hashes de arquivo

As funções *hash* são algoritmos que conseguem criar começando de uma entrada (um arquivo, por exemplo) e uma saída alfanumérica de comprimento fixo, que representa um resumo de todas as informações dadas. A partir dos dados de entrada, cria-se uma *string* que só pode ser recriada com os mesmos dados.

Com a utilização dos *hash* podemos identificar e remover arquivos conhecidos, o que permite excluir arquivos não relevantes para a investigação e aplicativos conhecidos e de sistemas operacionais. O analista pode usar bancos de dados *hashes* validados ou bases de dados próprias geradas a partir da criação de uma lista de *hashes* criptográficos de aplicativos e sistemas operacionais verificados. As vantagens dessa técnica são a redução de tempo para procurar e a possibilidade de ter bancos de dados consistentes. A principal desvantagem é que pequenas modificações em um arquivo (um bit) geram diferentes valores de *hash*. Essa técnica não será mais útil se a imagem pesquisada tiver sofrido qualquer modificação de forma ou tamanho.

Nomes dos arquivos

O compartilhamento de arquivos de pornografia infanto-juvenil pela internet é o grande motivador para o uso dessa técnica. Inúmeros arquivos dessa natureza são trocados com o uso de programas do tipo P2P. Para encontrar arquivos nesses programas, utilizam-se expressões e palavras-chave típicas relacionadas à pornografia infanto-juvenil. Essa técnica tem a vantagem de ser muito rápida, já que não envolve operações demoradas de leitura de disco.

Fique atento

É importante abordar quais são os critérios para classificar um conteúdo como ilegal ou não. A seleção de arquivos no exame de informática tem apenas o intuito de reduzir o volume de dados para facilitar a compreensão do laudo. Considerando uma grande quantidade de arquivos, é possível destacar imagens e vídeos nitidamente contendo crianças, bem como descartar material que apenas contém claramente adultos. Entretanto, haverá cenas em que é inviável

determinar se os indivíduos são adolescentes ou jovens adultos. Nos exames periciais, esses arquivos duvidosos podem eventualmente ser adicionados ao laudo com ressalvas, por não se tratar de conteúdo claramente infanto-juvenil. Nesses casos, resta somente a tentativa de localizar os indivíduos retratados para verificar a idade deles à época da realização das fotografias ou vídeos. Finalmente, podem ser necessárias técnicas adequadas de amostragem para contabilizar as imagens de nudez ou sexo envolvendo crianças ou adolescentes num conjunto demasiadamente grande de arquivos de pornografia. Durante toda a análise, deve-se garantir a privacidade do menor envolvido.

Referências

BARRETO, A. G.; BRASIL, B. S. *Manual de investigação cibernética*: à luz do marco civil da internet. São Paulo: Brasport, 2016.

BRASIL. *Estatuto da Criança e do Adolescente*: Lei Federal n. 8.069, de 13 de julho de 1990. Brasília, DF: Ministério da Mulher, da Família e dos Direitos Humanos, 2019. Disponível em: https://www.gov.br/mdh/pt-br/centrais-de-conteudo/crianca-e-adolescente/estatuto-da-crianca-e-do-adolescente-versao-2019.pdf. Acesso em: 26 ago. 2021.

Leituras recomendadas

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. *Internet segura para seus filhos*. São Paulo: CERT.br, [2021]. Disponível em: https://internetsegura.br/pdf/guia-internet-segura-pais.pdf. Acesso em: 26 ago. 2021.

EXPLORAÇÃO sexual infantil afeta todos nós: vídeo 2. [*S. l.*: *s. n.*], 2014. Publicado pelo canal GVT: Banda Larga, TV por Assinatura e Telefonia Fixa. Disponível em: https://www.youtube.com/watch?v=84VGPqx7x2w&feature=youtu.be. Acesso em: 26 ago. 2021.

NILLES, G.; SILVA, G. *Perícias informáticas para casos de pornografia infantil*. [*S. l.*: s.*n.*], 2016. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.F66E836D&lang=pt-br&site=eds-live&scope=site. Acesso em: 15 jul. 2021.

PACHECO, A.; CABRAL, C. A efetivação da proteção integral a partir do campo psicossocial: considerações sobre a violência doméstica contra a criança. *In*: CHILDHOOD BRASIL. *Violência sexual contra crianças e adolescentes*: novos olhares sobre diferentes formas de violações. São Paulo: Childhood Brasil, 2013. p. 145-176. Disponível em: http://crianca.mppr.mp.br/pagina-1869.html. Acesso em: 26 ago. 2021.

POLASTRO, M. de C.; ELEUTÉRIO, P. M. da S. Exames relacionados à pornografia infato-juvenil. *In*: VELHO, J. A. (org.). *Tratado de computação forense*. Campinas: Millennium, 2016. p. 245-287.

SANTOS, B. R. *Guia de referência*: construindo uma cultura de prevenção à violência sexual. São Paulo: Childhood Brasil, 2009.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS