PRINCÍPIOS E ANÁLISES DA COMPUTAÇÃO FORENSE

Rafael Paes da COSTA[1]
Raphael GARCIA[2]

RESUMO: Este artigo pretende apresentar os principais princípios que devem ser considerados nas análises dos crimes que envolvem tecnologia da informação. O objetivo é demonstrar as análises que são feitas nos crimes computacionais pelo Perito Criminal em Informática, com a ajuda de softwares e demais ferramentas.

Palavras-chave: Computação Forense. Hacker. Internet. Malwares. Esteganografia. Criptografia.

1 INTRODUÇÃO

Ciência Forense é a aplicação de um conjunto de técnicas científicas para responder a questões relacionadas ao Direito, podendo se aplicar a crimes ou atos civis. O esclarecimento de crimes é a função de destaque da prática forense. Através da análise dos vestígios deixados na cena do crime, os peritos, especialistas nas mais diversas áreas, conseguem chegar a um criminoso. Algumas das áreas científicas que estão relacionadas à Ciência Forense são a Biologia, Computação, Matemática, Química, entre várias outras áreas(SIGNIFICADO.DE, 2013, s.d.; s.p.).

A Computação Forense tem como objetivo auxiliar e determinar toda a dinâmica e materialidade de ilícitos relacionados à área da informática, utilizando de técnicas e métodos científicos, com o foco principal na identificação e análise do processo das evidências digitais e matérias de crime (ELEUTÉRIO e MACHADO, 2011, p. 15).

O artigo 158 do CPP[3] determina que: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não

[1] Discente do 7º termo do curso de Sistemas de Informação das Faculdades Integradas “Antônio Eufrásio de Toledo” de Presidente Prudente. E-mail: rafael-alc@hotmail.com
[2] Docente do curso de Sistemas de Informação das Faculdades Integradas “Antônio Eufrásio de Toledo” de Presidente Prudente e orientador do trabalho.

podendo supri-lo a confissão do acusado", o que leva a necessidade de um profissional qualificado para tal tarefa que produza laudos de interesse à justiça na apuração do delito, conforme artigos 159 e 160 do CPP: "O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior" e "Os peritos elaborarão o laudo pericial, no qual descreverão minunciosamente o que examinarem e responderão aos quesitos formulados", em crimes digitais quem realiza esse trabalho é o Perito Criminal em Informática, porém outros profissionais também podem ter a necessidade de realizar os exames ligados à computação, sendo eles: peritos particulares, auditores de sistemas, profissionais de TI[4], juízes, advogados, delegados, promotores e demais profissionais da área de direito, dos quais devem conhecer como evidências e provas digitais devem ser devidamente coletadas, apresentadas e apuradas (ELEUTÉRIO e MACHADO, 2011, p. 16-17).

2 DOS CRIMES COM USO DE EQUIPAMENTOS COMPUTACIONAIS

Nestes crimes, o computador é utilizado como ferramenta de auxílio aos criminosos, entre eles os principais: sonegação fiscal, tráfico de entorpecentes, falsificação de documentos, compra de votos em eleições e outros. Nestes casos o computador está dentro do termo "modus operandi[5]" do crime. Sendo assim, são feitos os exames forenses nos equipamentos utilizados, levando os laudos produzidos para serem analisados por um juiz em sua elaboração da sentença. Como um exemplo, temos: Em um assalto a banco, onde os computadores são utilizados para armazenar informações, como mapas das agências, horários, funcionários e entre outros. O computador é tratado como peça auxiliar no crime por guardar tais informações. Já nos crime de roubo de informações e dados valiosos, por meio de malwares[6] e phishing[7]. Como exemplos: um hacker utiliza um malware para obter dados de uma conta bancária e desviar dinheiro a partir de um acesso a um Internet Banking. Assim o computador se torna fundamental no decorrer do

[3] Código de Processo Penal (Lei 11.690, de 09 de Junho de 2008).
[4] Tecnologia de Informação.
[5] "Modo de operação."
[6] O nome Malware vem do inglês Malicious Software.
[7] Tipo de fraude eletrônica que consiste basicamente em enganar usuários de computadores com o objetivo de "roubar" informações sensíveis, como senhas de bancos e de cartões de crédito.

crime, ou seja, se não existisse, tal crime não poderia ser praticado desta forma, onde é válido também para a prática de pedofilia pela internet. O artigo 241-A do Estatuto da Criança e do Adolescente diz: “Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.”, o que torna o computador e o acesso à internet essencial para a pratica do crime, pois sem o mesmo, tal conduta seria impossível (ELEUTÉRIO e MACHADO, 2011, p. 18-19).

2.1 Crimes famosos já cometidos com uso da computação

Desde o início da “Era da Internet” muitos criminoso começaram a utilizar a computação para a prática de crimes, seja para simples invasões em sites na busca de informações valiosas, busca de informações para benefício próprio como roubo de cartões de crédito, pedofilia e até mesmo por simples “brincadeira”.

Veremos agora casos paradigmáticos de crimes computacionais.

2.1.1 Invasão ao Pentágono na procura por UFOs

Em 2002, o Pentágono admitiu que o escocês Gary McKinnon de 44 anos, invadiu e danificou 53 computadores do comando das Forças Armadas do Exército, Força Aérea e até mesmo da Nasa, tornando inoperante o distrito militar de Washington e causando prejuízos de US$ 1 milhão (DEZ HACKERS, s.d.; s.p.). Ainda conforme o site Terra (s.d; s.p.) Tudo isto na busca por provas de que UFOs[8] realmente existem juntamente com seres extraterrestres. Conhecido como “Solo” no mundo hacker, McKinnon além de não provar tal existência, acabou indicado em sete crimes nos Estados Unidos e preso na Grã-Bretanha. Ele nunca negou as acusações de invasão, garantindo apenas que sua intenção não era a espionagem.

2.1.2 Controle das linhas telefônicas para ganhar sorteio de Porsche

Em 1990 um jovem chamado Kevin Poulsen interceptou todas as linhas telefônicas da estação de rádio KIIS – FM, vencendo assim um concurso realizado pela emissora. O prêmio era um Porsche para o 102º ouvinte que telefonasse. Kevin garantiu seu carro, mas passou 51 meses na prisão e hoje ele é diretor do site Security Focus e editor da Wired (OS MAIORES HACKERS, s.d.; s.p.).

2.1.3 Invasão ao The New York Times

Ficando conhecido como “Grey Hat Hacker”, o Hacker do chapéu cinza, o norte-americano Adrian Lamo, em 2003, invadiu o sistema do jornal The New York Times apenas para incluir a si mesmo na lista de colaboradores. Também conhecido por quebrar uma série de sistema de alta segurança de rede de computadores como os da Microsoft, Yahoo!, MCI WorldCom e empresas de telefonia como SBC, Ameritech e Cingular (DEZ HACKERS, s.d.; s.p.).

[8] Do inglês “Unidentified Flying Object”, Objeto Voador Não Identificado.

2.1.4 Invasão a sistemas para roubo de cartões de crédito

Graças às suas habilidades de hacker, Albert Gonzalez, teve uma vida de riqueza e luxo. Com a ajuda de um programa criado por um amigo, ele invadiu sistemas de lojas e se apoderou de algo como 130 milhões de números de cartões de crédito e dados de clientes entre 2005 e 2007. Os dados eram vendidos na internet. Gonzalez fazia compras fraudulentas e vendia os produtos na web, tal esquema é considerado a maior fraude da história. Tudo isto no mesmo tempo em que era informante do Serviço Secreto dos Estados Unidos onde seu trabalho era justamente combater hackers (OS MAIORES HACKERS, s.d.; s.p.).

2.1.5 Invasão à conta do Twitter de Barack Obama

Com apenas 23 anos, o francês François Cousteix não pensou pequeno em se tornar célebre. Ele hackeou a conta do Twitter do homem mais poderoso do mundo, o presidente dos Estados Unidos, Barack Obama. Com a ajuda de um programa que faz um ataque de força bruta, testando várias senhas de login até ser aceita, Cousteix conseguiu tal acesso não somente de Obama, mas também da estrela pop Britney Spears e dos serviços como Fox News (DEZ HACKERS, s.d.; s.p.).

2.1.6 Garoto de 15 anos invade Departamento de Defesa dos Estados unidos e NASA

Sendo o primeiro adolescente a ser preso por crimes digitais nos Estados Unidos em 1999, Jonathan James aos 15 anos de idade invadiu computadores do Departamento de Defesa dos Estados Unidos e da NASA. James suicidou-se em maio de 2008, onde junto com o corpo foi encontrado uma carta justificando que ele não acreditava mais no sistema judiciário. Isso porque ele estava sendo investigado pelo Serviço Secreto dos Estados Unidos por ter ligação a um grande roubo de dados de clientes de várias lojas virtuais norte-americanas em 2007, algo que ele negava (OS MAIORES HACKERS, s.d.; s.p.).

2.1.7 Lei Carolina Dieckmann

A lei 12.737 de 2012, chamada lei “Carolina Dieckmann” que entre outras coisas, torna crime a invasão de aparelhos eletrônicos para a obtenção de dados particulares entrou em vigor em 2013 (LEI ‘CAROLINA DIECKMANN’, s.d.; s.p.).

Ao todo, 36 imagens da atriz nas quais ela aparecia nua, foram publicadas em maio de 2012. Ela recebeu ameaças de extorsão para que pagasse R$10 mil para não ter as fotos publicadas. Após dar queixa, a Polícia descartou a hipótese de as imagens terem sido copiadas de uma máquina fotográfica que havia sido levada para conserto quando constataram que a caixa de e-mail da atriz havia sido violada por hackers (G1, s.d.; s.p.).

Se houver comercialização ou divulgação das informações obtidas, a pena pode ser elevada de um a dois terços. Caso tal crime seja cometido contra o presidente da República, do Supremo Tribunal Federal, Governadores, Prefeitos e entre outros, a pena será aumentada de um terço à metade. Também passa a ser crime interromper serviço telemático ou de informática de utilidade pública, como também dados de cartões de crédito passam a equivaler aos dados do documento particular para atribuir punição à falsificação de identidade (G1, s.d.; s.p.).

3 DAS PRINCIPAIS ANÁLISES FORENSES EM INFORMÁTICA

Levando em consideração o crescimento do uso de dispositivos computacionais portáteis, espera-se que novos exames forenses sejam criados em um futuro próximo. De tal forma acredita-se que a demanda se expandirá nos próximos anos, devido aos computadores serem ótimos instrumentos no auxílio da investigação e essenciais na solução de diversos tipos de delitos. Entre os principais exames forenses de informática estão:

3.1 Análise e procedimentos em locais de crimes de informática

São utilizados os processos de mapeamento, correta identificação e preservação do equipamentos utilizados que estão no local e em alguns casos é

necessário ser feito um exame forense no local do crime, a fim de permitir um exame melhor e mais elaborado no laboratório de análise forense dos equipamentos apreendidos no local (ELEUTÉRIO e MACHADO, 2011, p. 20).

3.2 Análise em dispositivos de armazenamento

Consiste em analisar sistemas e programas instalados em discos rígidos, CDs, DVDs, Blu-Rays, pen drives e outros dispositivos de armazenamento. Os exames são seguidos de quatro fases (preservação, extração, análise e formalização) e também são realizadas técnicas para recuperação de arquivos, quebra de senhas e virtualização[9] (ELEUTÉRIO e MACHADO, 2011, p. 20).

3.4 Análise em aparelhos de telefone celular

É feita a extração dos dados armazenados na memória desses aparelhos como: lista de contatos, ligações, fotos, mensagens e etc. De acordo com a necessidade apresentada por cada caso (ELEUTÉRIO e MACHADO, 2011, p. 20).

3.5 Análise em sites da internet

Consiste na verificação e investigação tanto de cópias de conteúdos existentes na Internet, também em sites e servidores remotos, como no rastreamento por um domínio de um site através do seu endereço IP[10] (ELEUTÉRIO e MACHADO, 2011, p. 20).

3.6 Análise em mensagens eletrônicas (e-mails)

Analisar dados das mensagens eletrônicas a fim de identificar hora, data, endereço IP e em certos casos informações confidenciais e valiosas, tanto da mensagem como do remetente (ELEUTÉRIO e MACHADO, 2011, p. 21).

---

[9] Virtualização é um procedimento técnico que consiste basicamente em emular uma máquina virtual dentro de uma máquina real.

[10] O endereço IP, de forma genérica, é a identificação de um dispositivo em uma rede local ou pública.

4 ANÁLISES EM LOCAIS DE CRIMES RELACIONADOS À INFORMÁTICA

Agora veremos os principais procedimentos que devem ser tomados por peritos de informática em locais de crime e buscas e apreensões.

4.1 Conceito e definição

Um local de crime relacionado à informática é um local de crime convencional acrescido de equipamentos computacionais que tem relação com o delito investigado. Já mandado de busca e apreensão é uma ordem expedida pela autoridade judiciária para que seja realizada uma diligência, a fim de buscar e apreender pessoas ou objetos de interesse à justiça.

4.2 Atuações dos peritos nos locais de crimes

Ao participar da equipe de cumprimento do mandado de busca e apreensão, o perito é responsável por orientar a equipe quanto à seleção, preservação e coleta dos equipamentos computacionais. A sua primeira função é realizar o reconhecimento do local, identificando os equipamentos existentes, seguido providências para a preservação dos dados digitais, que são:

Impedir que pessoas estranhas à equipe utilizem os equipamentos de informática existentes sem a anuência/supervisão do perito e não ligar equipamentos computacionais que estejam desligados.

Dependendo do tipo da situação encontrada, pode-se recomendar, interromper as conexões de rede existentes e retirar a fonte de energia[11] desligando-os, exceto quando da possibilidade de flagrante delito[12]. No entanto tais ações somente devem ser realizadas quando o perito tiver certeza de que isso não ocasionará em perdas de evidências (ELEUTÉRIO e MACHADO, 2011, p. 26-27).

Quando computadores estiverem ligados, pode ser necessário copiar os dados da memória RAM (Random Access Memory) antes de desligá-los. A

[11] Retirar os cabos de alimentação das tomadas, baterias, pilhas e entre outras medidas.

[12] Quando durante o cumprimento de mandados de busca e apreensão, pode ser necessário verificar a existência de transmissão e/ou posse de dados ilegais, como pornografia infanto-juvenil. Nesses casos, o perito deve registar fatos por meio de fotos, anotações, vídeos e o que for possível para melhor documentar tal prática criminosa.

memória RAM é volátil, e seus dados são perdidos quando o computador é desligado. Assim, se o perito suspeitar que evidências estejam contidas nesse tipo de memória, ferramentas próprias devem ser utilizadas para realizar tal cópia. A ferramenta Computer Online Forensic Evidence Extractor (COFEE), desenvolvida pela Microsoft, faz o dump (cópia integral) dos dados voláteis contidos na memória RAM do computador a partir do uso de um pen drive, por exemplo (ELEUTÉRIO e MACHADO, 2011, p. 27).

Entrevistar as pessoas que residem e/ou trabalham no local sobre o uso desses equipamentos e juntar tais informações com o conhecimento prévio das investigações são medidas importantes para melhor selecionar o que deverá ser apreendido. Não é recomendado utilizar equipamentos computacionais do local para verificar se estes contêm as informações relevantes ao cumprimento da busca. Em computadores, por exemplo, tal prática pode apagar/alterar dados armazenados mesmo que os usuários não apaguem nenhum arquivo por vontade própria. Apenas profissionais treinados são capazes de realizar verificações nos dispositivos computacionais de forma a não alterar seus conteúdos. Tal verificação faz uso de softwares e equipamentos forenses.

Sistemas operacionais forenses, quando gravados em um CD/DVD, são capazes de inicializar os computadores (boot[13]), disponibilizando acesso somente leitura (ready-only) para que os discos rígidos possam ser inspecionados. Como exemplos desse tipo de sistema operacional, destacam-se o Knoppix e o Helix.

Hardwares forenses são equipamentos criados especificamente para a realização de cópias de diversos tipos de mídias, sempre garantindo que o conteúdo da mídia a ser copiada não seja alterado. Alguns equipamentos como o Logicube Forensic Talon, permitem que buscas por palavras-chaves sejam realizadas no conteúdo dessas mídias, podendo também funcionar como leitores de discos rígidos com bloqueio de escrita habilitado.

Se caso o perito não estiver preparado para utilizar tais procedimentos forenses, o melhor a fazer é coletar tais equipamentos para serem examinados

[13] O termo inglês boot significa inicializar um computador.

posteriormente em laboratório. Assim como no cumprimento de mandados e busca, tais apreensões deverão ser realizadas somente se existirem suspeitas de que esses dispositivos contenham evidências necessárias à investigação. Após realizar tais providências, devem ser coletados os equipamentos computacionais que possam conter as evidências desejadas, realizando o acondicionamento de forma correta e cuidadosa (ELEUTÉRIO e MACHADO, 2011, p. 28).

4.3 Identificações de dispositivos

A seguir serão apresentados os equipamentos computacionais mais comuns encontrados em locais de crime e em buscas e apreensões envolvendo dispositivos dessa natureza. Conhecer visualmente os equipamentos é fundamental para que o perito possa identificá-los e tomar as providências de preservação necessárias.

4.3.1 Computadores pessoais

PCs (Personal Computers), são a maioria dos equipamentos computacionais encontrados em locais de crime e/ou busca relacionados à informática. Um PC típico geralmente é composto, minimamente, de gabinete, monitor, teclado e mouse. Em alguns casos também podem ser encontrados caixas de som, webcam, impressora, scanner e estabilizador de energia. Dentro dos gabinetes estão os principais elementos do computador, como placa-mãe, processador, memórias RAM, fonte de alimentação de energia, placas de expansão (som, rede e vídeo), drives de CD, DVD e disquetes e principalmente discos rígidos. Os gabinetes mais comuns são do tipo torre ou minitorre e podem ser facilmente abertos com o uso de uma chave de fenda e/ou chave Philips. Para isso, primeiramente devem ser desconectados todos os cabos. Uma vez aberto, todos os componentes internos devem ser identificados. Na maioria dos casos, somente os componentes que armazenam informações de usuários são relevantes. Dentro do gabinete, esse componente é o disco rígido. Geralmente os gabinetes têm apenas um, mas também é possível encontrar com dois ou três discos rígidos (ELEUTÉRIO e MACHADO, 2011, p. 30).

4.3.2 Notebooks

Notebooks também são computadores pessoais, mas sua principal característica é que são construídos para serem menores, mais leves e, consequentemente, portáteis. Dentro de um notebook também existem componentes semelhantes aos encontrados nos PCs, como disco rígido, drives de CD, DVD, pentes de memória, monitor, componentes de som, webcam, mouse e teclado, todos integrados em um único produto. Ao contrário dos PCs, as placas de expansão dos notebooks são diferentes e têm a interface de conexão do tipo PCMCIA (Personal Computer Memory Card International Association) ou PC Card. Tais placas em geral também não armazenam informações dos usuários, pois comumente são placas de conexão de rede, modems e outros (ELEUTÉRIO e MACHADO, 2011, p. 32).

4.3.3 Servidores

Os servidores são computadores mais robustos, com maior capacidade de processamento, fisicamente maiores e frequentemente ficam ligados 24 horas por dia e podem apresentar gavetas externas contendo discos rígidos.

4.3.4 Telefones celulares

Aparelhos de telefone celular são dispositivos portáteis que estão se tornando cada vez mais utilizados pelas pessoas. Hoje em dia, os celulares estão incorporando várias funções e muitos já podem ser considerados mini computadores.

4.3.5 Elementos de rede

Muitos computadores têm conexão com a Internet, que geralmente é realizada por meio de dispositivos intermediários utilizados entre o computador e a linha telefônica ou cabo de TV. Alguns também utilizam a tecnologia de transmissão sem fio para conexão. Os principais entre eles são: Access Points, Hubs, Switches, Modems e Roteadores.

5 CUIDADOS TOMADOS E EXAMES FORENSES REALIZADOS NOS DISPOSITIVOS DE ARMAZENAMENTO

Agora serão apresentados as fases de procedimentos e cuidados realizados em exames forenses envolvendo dispositivos de armazenamento computacional. Os materiais mais comuns nesses tipos de exames são: discos rígidos, CDs e DVDs, pen drives, cartões de memória, Blu-rays e entre outros.

5.1 Cuidados com os dispositivos

Os dispositivos de armazenamento computacional são sensíveis e devem ser manuseados com cuidado, principalmente em se tratando de uma possível prova de crime. As principais características das mídias de interesse à Computação Forense, são: fragilidade, facilidade de cópia, sensibilidade ao tempo de vida e sensibilidade ao tempo de uso.

5.1.2 Fragilidade

Normalmente os dispositivos de armazenamento são sensíveis e merecem cuidado especial. Os discos rígidos, por exemplo, têm cabeçotes de leitura que podem girar a dez mil rotações por minuto e não podem encostar na superfície de cada um dos cilindros internos durante o processo de gravação e leitura de dados. Principalmente quando ligados, não devem sofrer vibrações mecânicas, a fim de evitar possíveis perdas de dados ocasionadas por atrito entre os cabeçotes de leitura/gravação e a superfície interna que contém os dados do disco rígido. No caso dos discos ópticos, como os CDs, DVDs e Blu-Rays, por exemplo, especial atenção deve ser atribuída à superfície das mídias. Deve-se sempre evitar arranhões e sujeiras na superfície, a fim de prevenir as leituras incorretas de dados. Precauções sempre devem ser tomadas no contato de mídias digitais com poeira, umidade e calor excessivo, pois são elementos que não combinam com dispositivos computacionais que contêm circuitos eletrônicos.

5.1.3 Facilidade de Cópia

Dispositivos computacionais trabalham com dados digitais binários, ou seja, as informações são representadas apenas por zeros e uns em uma estrutura conhecida como bits[14]. Utilizando mecanismos de correção de erros[15] (ou de paridade), os dados podem ser copiados de um dispositivo para outro sem risco de perda de informações, seja por meio da Internet, seja por uma rede local, seja entre dois discos rígidos de um mesmo computador, por exemplo. Utilizando essas técnicas, é possível fazer cópias fiéis do material digital original para outras mídias, a fim de que os exames forenses sejam realizados nas cópias, preservando, assim, o

[14] Menor unidade de dado manipulada por computador. Pode conter o valor de 0 ou 1.
[15] Mecanismos de correção de erros ou de paridade são técnicas amplamente conhecidas na computação e se baseiam na utilização de determinados bits para garantir que um conjunto de dados não teve seu conteúdo alterado.

material original. Além disso, essa abordagem diminui o tempo de uso do material original após a apreensão, minimizando, assim, defeitos provocados pela utilização natural desses dispositivos.

5.1.4 Tempo de vida

As informações digitais armazenadas nos dispositivos computacionais podem ser perdidas ao longo do tempo, pela quebra dos dispositivos mecânicos, pela desmagnetização ou pelo término da vida útil dos materiais utilizados na fabricação. Por isso, é tão comum no meio computacional a realização de cópias de segurança (backup) dos mais variados dados, pois eles podem ser perdidos a qualquer momento, devido à sua fragilidade. Portanto os exames forenses devem ser feitos o mais rápido possível a partir do momento do recebimento do material apreendido para minimizar a perda de dados ocasionados pelo excesso de tempo de vida do dispositivo.

5.1.5 Tempo de uso

Quando um computador é utilizado para a realização de um crime, seja como meio, seja como ferramenta, dados são armazenados nos dispositivos de armazenamento a ele conectados. A partir de então, tais dados podem ser apagados pelo usuário. Sabendo-se que as chances de recuperação dessas informações diminuem à medida que os dispositivos são utilizados, o tempo torna-se um fator crucial em investigações envolvendo vestígios digitais. Assim, a apreensão dos dispositivos computacionais deve ser feita o mais rápido possível para evitar uma possível perda de evidências armazenadas nesses equipamentos.

5.2 Fases dos exames

5.2.1 Preservação

Consiste em garantir que as informações armazenadas no material questionado sejam jamais alteradas. Assim como em um local de crime convencional, as evidências e provas ali existentes devem ser preservadas. Na

informática não é diferente: os dados contidos nos dispositivos não podem sofrer nenhuma alteração.

Cuidados especiais devem ser tomados nessa fase, pois até uma operação simples pode alterar os dados armazenados em mídia digital. Por exemplo, ao ligar um computador com um sistema operacional típico da família Microsoft Windows instalado no disco rígido, os dados contidos são alterados[16], mesmo que o usuário não execute nenhuma operação. No caso de mídias ópticas, deve-se atribuir atenção especial às mídias regraváveis, como os CD-RW e DVD-RW, pois elas podem ter os dados apagados se manuseados sem o devido cuidado, resultando perda de informações e alteração de prova. Em dispositivos portáteis, como pen drives e cartões de memória, precauções também devem ser tomadas, uma vez que a simples conexão de um desses equipamentos na porta USB de computador com sistema operacional da família Windows pode gerar gravação de dados no dispositivo. Assim como no caso dos discos rígidos, equipamentos e softwares específicos devem ser utilizados para garantir a correta preservação dos dados.

Devido à fragilidade e sensibilidade das mídias de armazenamento computacional, os exames forenses devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original. Assim, deve-se realizar a duplicação do equipamento original com uma das seguintes técnicas computacionais: espelhamento[17] ou imagem[18]. Para isso, devem ser utilizados equipamentos e softwares forenses específicos. Após o fim da fase de preservação, o dispositivo de armazenamento computacional deverá ser lacrado e guardado em local apropriado; não será mais necessária a sua utilização para a realização dos exames e posterior elaboração do laudo (ELEUTÉRIO e MACHADO, 2011, p. 55).

5.2.2 Extração

[16] Ao ligar um computador utilizando um sistema operacional Windows, arquivos temporários são criados e outros têm seu conteúdo alterado. As datas de último acesso também sofrem modificações, por exemplo.

[17] Técnica que consiste na cópia exata e fiel dos dados (bit a bit) contidos em um dispositivo de armazenamento computacional para outro. Logo, sempre é necessário que exista um dispositivo a ser copiado e um para receber a cópia, onde a capacidade de armazenamento deve ser igual ou superior ao original.

[18] Tirar uma imagem de um dispositivo, semelhante ao espelhamento, mas ao em vez de copiar bit a bit de um dispositivo para outro, eles são copiados para arquivos.

A fase de extração de dados consiste basicamente na recuperação de todas as informações contidas na cópia dos dados provenientes da fase de preservação anteriormente realizada. Todos os procedimentos serão realizados nas cópias (espelho ou imagem) dos originais.

Os dispositivos de armazenamento de dados digitais podem guardar muito mais informações do que as visíveis pelos usuários comuns. Insto ocorre basicamente devido ao tipo de organização dos dados dentro desses dispositivos. Ao apagar um arquivo de um computador, o sistema operacional não sobrescreve todo o conteúdo ocupado por esse arquivo no disco rígido com zeros e/ou uns. Ele apenas tem um controle de quais partes do disco rígido estão livres e quais estão ocupadas. Assim, na realidade, ao apagar um arquivo, o sistema operacional apenas altera o status desse espaço de ocupado para livre (disponível). Com isso, os dados referentes aos arquivos apagados continuam armazenados no disco rígido e podem ser recuperados por meio de técnicas específicas. Entretanto, esses dados podem ser sobrescritos a qualquer momento pelo sistema operacional, uma vez que esse espaço está disponível para utilização. Logo conclui-se que, quanto mais recentemente um arquivo foi apagado, maiores são as chances de recuperá-lo, uma vez que será menor a probabilidade de sobrescrita do espaço utilizado no disco rígido por algum novo arquivo a ser gravado ou por alguma ação realizada pelo próprio sistema operacional (ELEUTÉRIO e MACHADO, 2011, p. 62).

Na prática, a recuperação de arquivos é baseada na procura de assinaturas[19] (também chamadas de cabeçalhos) de arquivos conhecidas em toda a área livre (disponível) do disco. Quando uma assinatura é encontrada, realiza-se uma busca pelo conteúdo do arquivo, recuperando a informação original (antes de ser apagada) de forma integral ou parcial (quando o conteúdo completo não estiver mais disponível, ou seja, parte foi sobrescrita por outro arquivo). Por percorrer todos os bits do dispositivo, esse procedimento permite que se recuperem arquivos mesmo que eles não tenham sido salvos pelo usuário. Assim, até uma página de Internet acessada uma única vez pode ser recuperada de um disco rígido, uma vez que pode ter sido armazenada de forma temporária pelo navegador da Internet (ELEUTÉRIO e MACHADO, 2011, p. 64).

[19] Todos os arquivos com formato conhecido, tais como JPEG, AVI, DOC, XLS, BMP, PDF, entre outros, possuem uma assinatura em seu início que os identificam.

5.2.3 Análise

A análise de dados é a fase que consiste no exame das informações extraídas na fase anterior, a fim de identificar evidências digitais presentes no material examinado, que tenham relação com o delito investigado. Em alguns casos, um disco rígido com capacidade de 80 GB, que é considerado um disco pequeno nos padrões de hoje, pode conter mais de um milhão de arquivos, incluindo os já recuperados. Analisar o conteúdo de todos os arquivos, olhando-os um por um, pode levar muito tempo e tornar o exame inviável. Com o objetivo de auxiliar o perito nessa tarefa, alguns procedimento e técnicas podem ser utilizados para tornar esse processo mais eficiente.

Known File Filter, ou simplesmente KFF, é uma lista com os resumos unidirecionais de arquivos conhecidos e pode ser utilizado para filtrar o conteúdo de um dispositivo a ser examinado. Dessa forma, é possível diminuir, por exemplo, o número de arquivos a serem examinados em um disco rígido que tem um sistema operacional e programas diversos instalados. O KFF também pode ser utilizado para, ao invés de descartar, indicar arquivos filtrados que são de interesse à investigação. Essa abordagem é muito utilizada quando se pretende verificar a existência de um mesmo arquivo em várias mídias computacionais. Além disso, pesquisar o conteúdo de um dispositivo de armazenamento computacional por palavras-chave pode ser uma maneira muito eficaz de localizar arquivos de interesse. Uma vez realizada a indexação dos dados, diversas pesquisas podem ser feitas de forma rápida, pois, como o conteúdo do disco foi percorrido e estruturado, não será necessário procurar novamente em todo o conteúdo do disco toda vez que uma nova palavra for pesquisada (ELEUTÉRIO e MACHADO, 2011, p. 67).

Percorrer os dados dos dispositivos de armazenamento computacional por meio da estrutura de pastas e arquivos é uma técnica interessante para localizar vestígios de interesse à investigação, pois geralmente os usuários utilizam determinadas pastas para armazenar seus arquivos pessoais, por exemplo, as pastas Meus Documentos e Desktop, em sistemas operacionais da família Windows. Identificar e analisar os arquivos presentes nessas pastas, incluindo os recuperados, geralmente é de suma importância. No caso de análise de discos rígidos contendo sistemas operacionais, o uso de programas que emulem uma máquina virtual pode

ser muito interessante para entender as operações efetuadas pelos usuários dos computadores a serem examinados. Com a virtualização, é possível inicializar o sistema operacional desses discos rígidos em uma máquina virtual, auxiliando o perito a visualizar e utilizar o sistema operacional contido no dispositivo questionado, como se ele estivesse sido ligado normalmente. Um dos programas mais utilizados nessa operação é o VMWare.

5.2.4 Formalização

Formalização é a fase final dos exames forenses, que consiste na elaboração do laudo pelo perito, apontando o resultado e apresentando as evidências digitais encontradas nos materiais examinados. No aludo devem constar os principais procedimentos realizados, incluindo as técnicas utilizadas para preservar, extrair e analisar o conteúdo das mídias digitais. Em muitas vezes, as evidências digitais encontradas nos dispositivos examinados são copiadas e apresentadas por meio de conteúdo digital, na forma de anexos ao laudo. O perito deve sempre se atentar que o laudo é um documento técnico-científico, que deve descrever com objetividade e clareza os métodos e exames realizados como um todo. Assim, laudos geralmente têm uma estrutura própria, bem definida, formada geralmente pelas seguintes seções: Preâmbulo[20], Histórico[21], Material[22], Objetivo, Considerações técnicas/periciais, Exames e Respostas aos quesitos/conclusões (ELEUTÉRIO e MACHADO, 2011, p. 70).

6 PRINCIPAIS FERRAMENTAS E TÉCNICAS

Para agilizar o processo dos exames e análises realizados nos dispositivos, arquivos e demais possíveis itens relacionados aos crimes, algumas ferramentas e técnicas são utilizadas, para assim, tornar a investigação mais eficiente e eficaz.

[20] Identificação do laudo.
[21] Fatos anteriores e de interesse ao laudo.
[22] Descrição detalhada do material examinado no aludo.

6.1 Forensic Toolkit 3.0

O Forensic Toolkit® (FTK ®) é reconhecido em todo o mundo como um conjunto de ferramentas de tecnologia de computador de investigação forense. Conhecido por sua interface intuitiva, análise de e-mail, exibições de dados personalizáveis e estabilidade, FTK ampliou seu quadro de expansão, com uma gama de funcionalidades que, normalmente, apenas as organizações com dezenas de milhares de dólares podem pagar (NOVO FORENSIC TOOLKIT, 2009, s.p.).

Com a ferramenta é fácil criar imagens, analisar o registro, conduzir uma investigação, decodificar os arquivos, recuperar senhas de arquivos criptografados, identificar esteganografia e construir um relatório. Também é possível recuperar senhas a partir de 100 assinaturas, aproveitar CPUs ociosas em toda a rede para decriptar[23] arquivos e executar robustos ataques de dicionário, e ele ainda possui uma biblioteca com 45 milhões de hashes[24]. A ferramenta enumera todos os processos em execução, incluindo os escondidos por rootkits[25], e exibe as DLLs associadas, soquetes de rede, a partir de máquinas Windows 32-bit. Ela concede a busca sequencial de memória, permitindo que você identifique hits na memória e automaticamente os mapeie de volta para um determinado processo (IMASTERS e VARGAS, 2009, s.p.).

6.2 EnCase

O EnCase é um sistema integrado de análise forense baseado no ambiente Windows. Ele é muito utilizado por oficiais da lei e profissionais da segurança de computadores em todo o mundo. O processo utilizado pelo EnCase começa com a criação das imagens dos discos (disquetes, Zips, Jaz, CD-ROMs e discos rígidos) relacionados ao caso investigado. Depois da criação das imagens, chamadas de EnCase Evidence Files, pode-se adicioná-las a um único caso (case file) e conduzir a análise em todas elas simultaneamente. O ambiente Windows não

[23] Traduzir ou decifrar mensagens ou códigos criptografados.
[24] Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados de hash, códigos hash, somas hash, chechsums ou simplesmente hashes.
[25] Rootkit é um tipo de software, muitas das vezes malicioso, projetado para esconder a existência de certos processos ou programas de métodos normais de detecção e permitir contínuo acesso privilegiado a um computador.

é considerado apropriado por muitos profissionais da área para a prática forense, uma vez que ele rotineiramente altera os dados e escreve no disco rígido sempre que é acessado. Mas, o EnCase não opera na mídia original ou discos espelhados, ele monta os Evidence Files como discos virtuais protegidos contra escritas. Então, o EnCase (não o sistema operacional) reconstrói o sistema de arquivos contido em cada Evidence File, permitindo ao investigador visualizar, ordenar e analisar os dados, através de uma interface gráfica (HOLPERIN e LEOBONS, s.d., s.p.).

6.3 Criptografia

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança para a proteção contra os riscos associados ao uso da Internet (CARTILHA CERT.BR, s.d., s.p.).

Exemplo:

Alfabeto original	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Alfabeto criptografia	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
Texto original	EXEMPLO CRIPTOGRAFIA
Texto criptografado	TBTDHSG EKODZGUKQYOQ

6.4 Esteganografia

Esteganografia é uma palavra que vem do grego e significa “escrita oculta”. Trata-se do estudo de técnicas que permitam esconder informações dentro de outros arquivos, sejam imagens, músicas, vídeos ou mesmo textos. É possível, por exemplo, esconder mensagens dentro de imagens sem que os usuários, ou qualquer outra pessoa que intercepte essa figura, sequer desconfie que existe alguma coisa escrita ali. A esteganografia pode ter utilidade em várias situações. Em um mundo como a internet – em que nada se cria, tudo se copia – essa técnica de esconder informações em outros arquivos pode ser utilizada para inserir

mecanismos de verificação de direitos autorais em imagens, por exemplo. Infelizmente nem tudo são flores. As mesmas técnicas utilizadas para garantir a proteção de informações importantes pode também servir para prejudicar outras pessoas. É muito comum a distribuição de vírus e outros malwares por meio de imagens e arquivos de áudio e vídeo (O QUE É ESTEGANOGRAFIA? s.d., s.p.).

7 CONCLUSÃO

A computação forense tem como principal objetivo, apresentar as principais análises, seguidas de princípios, realizadas em exames forenses. Desde investigações em locais de crime, busca e apreensão, armazenamento em dispositivos e conteúdos impróprios presentes na internet. Diante de análises e dos estudos realizados, foram demonstrados, exemplos de crimes realizados com auxílio da computação, análises forense, tanto em locais de crime como em dispositivos de armazenamento, procedimentos que devem ser seguidos nas análises, atuação do perito, cuidados tomados com os objetos e ferramentas que auxiliam na busca por provas.

Por fim, com a ajuda da tecnologia da informação, hoje em dia, podemos solucionar e agilizar o processo de investigação em muitos crimes, não somente nos ligados à computação, como em outros tipos. Portanto, com esta nova ciência, a computação forense, podemos expandir nossas técnicas, soluções e métodos, para com eles desvendar criminosos e fazer justiça.

8 REFERÊNCIAS

CRIPTOGRAFIA. Disponível em: < http://cartilha.cert.br/criptografia/ > Acesso em 22 de Abril de 2014.

DEZ HACKERS FAMOSOS E SEUS FEITOS. Disponível em: < http://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-01.htm > Acesso em 18 de Abril de 2014.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. São Paulo: Novatec, 2011.

ENCASE. Disponível em: < http://www.gta.ufrj.br/grad/07_1/forense/encase.html > Acesso em 22 de Abril de 2014.

LEI 'CAROLINA DIECKMANN', QUE PUNE INVASÃO DE PCS, ENTRA EM VIGOR. Disponível em: < http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html > Acesso em 19 de Abril de 2014.

SIGNIFICADO.DE, DEFINIÇÃO DE FORENSE. Disponível em: < http://br.significado.de/forense > Acesso em 19 de Maio de 2014.

NOVO FORENSIC TOOLKIT 3.0. Disponível em: < http://imasters.com.br/artigo/14668/gerencia-de-ti/novo-forensic-toolkit-30/ > Acesso em 22 de Abril de 2014.

O QUE É COMPUTAÇÃO FORENSE? Disponível em: < http://tiqx.blogspot.com.br/2012/03/o-que-e-computacao-forense.html > Acesso em 16 de Abril de 2014.

O QUE É ESTEGANOGRAFIA? Disponível em: < http://www.tecmundo.com.br/video/3763-o-que-e-esteganografia-.htm > Acesso em 07 de Maio de 2014.

OS MAIORES HACKERS DA HISTORIA. Disponível em: < http://www.techtudo.com.br/rankings/noticia/2011/06/top-10-os-maiores-hackers-da-historia.html > Acesso em 18 de Abril de 2014.