FACULDADE DE TECNOLOGIA DE SÃO PAULO

RAFAEL NADER DE ALMEIDA

Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais

São Paulo
2011

FACULDADE DE TECNOLOGIA DE SÃO PAULO

RAFAEL NADER DE ALMEIDA

Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais

Monografia submetida como exigência parcial para a obtenção do Grau de Tecnólogo em Processamento de Dados.
Orientador: Prof. Rodrigo Zuolo Carvalho.

São Paulo
2011

Dedicatória

Dedico este trabalho de conclusão da graduação aos meus pais, namorada, irmãos, familiares e amigos que de muitas formas me incentivaram e ajudaram para que fosse possível a concretização deste trabalho.

Agradecimentos

Agradeço especialmente e carinhosamente os meus pais Maria Aparecida Moreira Nader e Humberto de Almeida, pelo amor incondicional, pela confiança depositada, pelo respeito e por terem feito o possível e o impossível para me oferecerem a oportunidade de estudar.

À minha namorada Amanda Teixeira Rodrigues, pelo amor, pela amizade, por estar comigo nos momentos de angústia e felicidade, pela motivação e por ser exemplo de dedicação aos estudos.

Aos meus irmãos e familiares pelo incentivo, por compreenderem a importância dessa conquista e aceitar a minha ausência quando necessário.

Aos meus amigos pela torcida positiva, pela amizade e por ajudar a tornar a vida muito mais divertida.

Ao meu orientador, o Professor Rodrigo Zuolo Carvalho pelo empenho, paciência e credibilidade, obrigado por tudo.

Resumo

A facilidade e a velocidade com que o computador processa, armazena e transmite informações tornou-o um bem de consumo muito apreciado - e por diversas vezes indispensável – em todo o mundo. No Brasil, o ramo de informática cresceu de forma vertiginosa na última década, graças aos avanços econômicos, sociais e de demanda por esses equipamentos.

Com essa disseminação dos computadores e do acesso a internet, os criminosos também passaram a utilizar esses dispositivos em seus delitos, seja utilizando-os como ferramenta de apoio para crimes convencionais, ou como meio para a violação da lei. Para combater tais transgressões, a polícia teve que se aperfeiçoar, fazendo surgir a figura do Perito Computacional, um profissional com conhecimentos tanto em informática, quanto em direito, especialista em analisar vestígios digitais e em produzir provas técnicas fundamentais que servirão de apoio para a decisão de um juiz. Este trabalho de graduação visa descrever a Perícia Forense Computacional, bem como as técnicas empregadas na extração e análise dos dados de mídias de armazenamento digital e os aspectos jurídicos envolvidos na atuação do perito.

Abstract

The ease and speed with which the computer processes, stores and transmits the information became a commodity much appreciated - and needed several times - throughout the world. In Brazil, the computer industry has grown over the last decade, thanks to economic and social advances and demand for such equipment.

With the spread of computers and access the Internet, criminals have also begun to use these devices in their crimes, either using them as a tool to support conventional crime or as a means for breaking the law. To combat such offenses, the police had to be improved, leading to the figure of the Computer Specialist, a professional with expertise in both computer science, as in law, expert in analyzing digital footprints and to produce technicals evidences that will support the judge decision. This graduate work aims to describe the Computer Forensics as well as the techniques employed in the extraction and analysis of data from digital storage media and the legal aspects involved in the performance of the specialist.

Sumário

Capítulo 1 - Conceitos Gerais

1.1 - Introdução

Durante o período Mesolítico da Pré História, a aproximadamente dez mil anos atrás, a humanidade conseguiu dar importantes passos rumo à sua evolução e sobrevivência. Foi nessa fase que o homem dominou o fogo, domesticou animais e desenvolveu a agricultura, o que exigiu o conhecimento do tempo, das estações do ano e das fases da lua, além de formas de controlar seu rebanho, surgindo assim a necessidade de contar. A partir de então, não parou mais, quantificando desde alimentos para o consumo da tribo, até partículas subatômicas para pesquisas espaciais.

O ser humano percebeu que a capacidade de efetuar cálculos sempre esteve ligada com o seu desenvolvimento, ou seja, cada vez que ele conseguia resolver operações matemáticas mais complexas e com maior rapidez, maiores eram os avanços científicos que alcançava. Baseado nessa percepção, diversos instrumentos de contagem foram criados, como o ábaco, as Réguas de Cálculo de John Napier, a Pascalina de Blaise Pascal que depois foi aperfeiçoada por Gottfried von Leibnitz e muitos outros, incluindo o computador. Inclusive o termo Computar, segundo o dicionário Michaelis, é originário do latim e significa calcular, contar; portanto, computador seria então o mecanismo ou máquina que auxilia nessa tarefa.

Em 1946, surge nos EUA com cerca de 30 toneladas; 18000 válvulas; ocupando, aproximadamente, uma área de 180 m2; e com capacidade de realizar 5000 somas por segundo, o primeiro computador digital eletrônico automático do mundo, chamado ENIAC (Electrical Numerical Integrator and Computer). Ele foi concebido através de uma parceria entre o exército norte americano e a Universidade da Pensilvânia, com o intuito de realizar cálculos balísticos e continha a arquitetura básica de um computador empregada até hoje, com memória principal, memória auxiliar, unidade central de processamento e dispositivos de entrada e saída de dados.

Em 1947, a invenção do transistor - em substituição às válvulas - trouxe maior velocidade às máquinas e provocou uma revolução na eletrônica dos aparelhos da época. Houve um tempo de constantes aprimoramentos e desenvolvimento tecnológico, tanto que em 1965, Gordon Earle Moore – futuro cofundador e presidente da Intel – conjeturou que a quantidade de transistores que podiam ser impressos numa pastilha (futuro processador de um computador)

dobraria a cada ano mantendo o seu custo. Tal previsão de evolução acabou se concretizando até os dias atuais, porém no intervalo maior de 18 meses. Mesmo assim, foi um prognóstico ousado e demonstra o quanto a computação evoluiu desde então.

Atualmente, a facilidade e a velocidade com que o computador processa, armazena e transmite informações por toda a sua rede, tornou-o um bem de consumo muito desejado – e por diversas vezes indispensável – em muitos lares de todo o mundo. Segundo a pesquisa Mercado Brasileiro de Tecnologia de Informação (TI) e Uso nas Empresas, feita pela Fundação Getúlio Vargas, há cerca de 2,5 bilhões de computadores no planeta em 2011. No Brasil, as vendas desses equipamentos aumentaram 20% no último ano, o que contribuiu para que chegássemos ao número de 85 milhões, o que significa que quatro de cada nove brasileiros têm um computador para uso residencial ou corporativo. De acordo com o coordenador da pesquisa e professor da FGV, Fernando Meirelles, a tendência é que essa expansão continue nos próximos anos devido à redução do custo dos aparelhos, à elevação do poder aquisitivo e ao crescimento da percepção das pessoas sobre a utilidade do computador[1].

Governos e empresas notaram esse avanço e passaram a oferecer diversos serviços aos cidadãos, como emissão de documentos, transações bancárias, vendas de produtos, entre outros, gerando assim uma enorme quantidade de dados sigilosos. Os criminosos, atraídos pelo grande volume de informações pessoais circulando pelas redes do mundo inteiro, começaram a se especializar e até recrutar pessoas com conhecimentos na área de computação. A melhor maneira para combater tais ataques, sem dúvida, é a prevenção, não só utilizando equipamentos de alta tecnologia e sistemas seguros, como também instruindo as pessoas que os utilizam. Entretanto, quando ela se torna ineficaz ou inexistente, deve-se recorrer à Perícia Forense Computacional para que haja uma investigação e os criminosos punidos. Esta prática é feita por um profissional habilitado, com conhecimentos tanto em informática, quanto em direito, especialista em analisar vestígios digitais e em produzir provas técnicas que servirão de apoio para a decisão de um juiz.

Mesmo com toda a importância da Perícia Forense Computacional, livros, documentos e textos científicos são escassos, superficiais ou, até mesmo, incompletos, abordando apenas uma das vertentes dessa área. Este trabalho acadêmico ambiciona preencher esta lacuna, fornecendo conhecimentos relevantes sobre todas as áreas relacionadas à investigação digital, sobre a atuação do perito, as técnicas de coleta e exame dos dados e os aspectos jurídicos presentes.

[1] http://agenciabrasil.ebc.com.br/noticia/2011-04-19/pesquisa-mostra-que-brasil-tem-85-milhoes-de-computadores-em-uso

1.1.1. Objetivos

O objetivo deste trabalho de conclusão de curso é conceituar Perícia Forense Computacional; descrever os processos executados durante a investigação; traçar os tipos de crimes cometidos utilizando equipamentos computacionais; exibir as técnicas envolvidas na coleta e no exame de vestígios digitais; relatar as principais dificuldades que podem surgir na fase de análise dos dados como quantidade de arquivos, existência de senhas, criptografia e esteganografia; e citar os principais aspectos jurídicos envolvidos durante a perícia. Também se pretende discutir os métodos usados na preservação de evidências para garantir a integridade do material questionado, porém este texto não intende abordar os procedimentos para a elaboração de um laudo pericial.

Ou seja, esta monografia aspira apresentar um novo enfoque da Perícia Computacional, ao mostrar como é a atuação do perito, ao estudar a coleta e exame dos dados pelos aplicativos forenses e ao analisar os aspectos jurídicos presentes.

1.1.2. Justificativa

Mesmo com toda a importância da Perícia Forense Computacional atualmente, livros, documentos e textos científicos são escassos, superficiais ou, até mesmo, incompletos, abordando apenas uma das vertentes dessa área. Este trabalho acadêmico ambiciona preencher esta lacuna, fornecendo conhecimentos relevantes sobre todas as áreas relacionadas à investigação digital, como a atuação do perito, as técnicas de coleta e exame dos dados e os aspectos jurídicos presentes.

1.1.3. Metodologia

Primeiramente, foi feito um levantamento bibliográfico em busca de obras de qualidade e produzidas por profissionais conceituados na área, não só na parte teórica, como também na prática, como por exemplo, peritos computacionais com anos de experiência. Após a escolha

e estudo da literatura, foram feitas diversas buscas em sites da Internet por informações complementares para que o enfoque deste trabalho pudesse ser atingido.

1.1.4 Apresentação do trabalho

O capítulo 1 deste texto aborda os conceitos gerais e a definição sobre Perícia Forense Computacional e os tipos de crimes cometidos utilizando dispositivos computacionais.

Os procedimentos executados durante a investigação, como a busca e o comportamento do perito em locais de crime de informática e os aspectos das apreensões de equipamentos computacionais, são detalhados no capítulo 2.

O capítulo 3 é o cerne deste trabalho de graduação, pois descreve as características sobre o armazenamento digital, as etapas de um exame forense computacional, as técnicas utilizadas para coleta e análise dos dados e os métodos praticados para a preservação de evidências.

No capítulo 4 são apresentados os maiores desafios que podem surgir durante a análise dos dados, como a quantidade de arquivos, senhas, criptografia e esteganografia.

O capítulo 5 é o responsável por discorrer a respeito dos principais aspectos jurídicos presentes durante a investigação com relação à Perícia Forense Computacional.

1.2 - Definição de Perícia Forense Computacional

A inovação tecnológica traz uma série de benefícios para as pessoas e a comunidade em geral. Todavia, com as vantagens, surge também a possibilidade de realização de novas práticas ilegais e criminosas. Para punir os agentes de tais atos, é necessário que haja uma investigação por parte das autoridades competentes, a qual se inicia sempre com a apuração e análise dos vestígios deixados, conforme determina o Código de Processo Penal Brasileiro (CPP) em seu artigo 158: “Quando a infração deixar vestígios, será indispensável o exame de corpo de

delito, direto ou indireto, não podendo supri-lo a confissão do acusado.” Segundo o dicionário Michaelis da Língua Portuguesa, vestígio é definido como “1 Sinal deixado pela pisada ou passagem, tanto do homem como de qualquer outro animal; pegada, rasto. 2 Indício ou sinal de coisa que sucedeu, de pessoa que passou. 3 Ratos, resquícios, ruínas. Seguir os vestígios de alguém: fazer o que ele fez ou faz; imitá-lo.” No caso da computação, os vestígios de um crime são digitais, uma vez que toda a informação armazenada nesses equipamentos computacionais é composta por bits em uma ordem lógica.

Já em seu artigo 159, o CPP impõe que “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.” Desta forma, Perícia Forense Computacional é a atividade concernente aos exames realizados por profissional especialista, legalmente habilitado, “destinada a determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crimes, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo” (ELEUTÉRIO / MACHADO, 2011, p.16).

1.3 - Tipos de crimes cometidos utilizando dispositivos computacionais

Embora a utilização de computadores para o cometimento de crimes não ser uma atividade tão recente, a legislação brasileira ainda não está totalmente preparada para tipificar todas as modalidades de crimes cibernéticos. Atualmente, há um projeto de lei e o Marco Civil da Internet Brasileira tramitando na Câmara dos Deputados e no Senado Federal, porém não há previsão para que sejam apreciados, votados e entrarem em vigor. Tais textos regulamentam, por exemplo, o crime de criação e transmissão de vírus e o tempo mínimo que um provedor de internet deve guardar os registros de acesso de seus usuários. Esses aspectos jurídicos serão abordados mais detalhadamente no capítulo *Principais aspectos jurídicos presentes na Perícia Forense Computacional.*

Diante dessas dificuldades, delegados e promotores vem utilizando a estratégia de enquadrar os atos ilícitos em crimes já existentes no Código Penal brasileiro e assim evitar a impunidade dos delinquentes. Portanto, é de suma importância diferenciar se o computador é utilizado apenas como ferramenta de auxilio à pratica de delitos convencionais ou se é usado como meio para a realização do crime.

1.3.1 Equipamento computacional utilizado como ferramenta de apoio aos crimes convencionais

Estima-se que 90% dos exames forenses realizados na área de informática são para investigações desse tipo de crime, onde o computador é apenas uma ferramenta de auxílio aos criminosos na prática de delitos conhecidos, como falsificação de documentos, violação de direito autoral, sonegação fiscal, tráfico de entorpecentes, etc.

Podemos fazer uma analogia com um veículo que é utilizado na fuga de bandidos de um roubo a banco. Nessas situações, tanto o computador, quanto o carro estão relacionados ao *modus operandi* do crime, ou seja, à maneira que a atividade ilegal é executada. Assim, em muitos casos, exames forenses nesses objetos são uma excelente prova técnica e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença.

1.3.2 Equipamento computacional utilizado como meio para a realização do crime

Nessa modalidade, o computador exerce o papel central para a realização do delito, ou seja, a infração não seria cometida se tal dispositivo não existisse. Alguns exemplos de crimes cibernéticos desse tipo são: roubo de informações sigilosas, ataques a sites, *phishing*, *malwares*, vírus de computador, cavalos de tróia, *worms*, etc.

Apesar de existir alguns crimes cibernéticos já tipificados, como a pornografia através da internet (artigo 241-A do Estatuto da Criança e do Adolescente), ou serem enquadrados como delitos convencionais, como estelionato e furto, o Brasil necessita de uma lei específica para todas as violações que utilizam um computador como meio.

Capítulo 2 - Início da Perícia Forense Computacional

2.1 - Procedimentos executados durante uma investigação

A apuração de um delito, independente se há um computador envolvido, deve seguir as normas estabelecidas pela legislação brasileira, mais precisamente o decreto-lei Nº 3.689, de 3 de outubro de 1941. Nesse texto, conhecido como Código de Processo Penal, está regulamentado a função do Estado de julgar as infrações penais e de aplicar punições a quem as pratica. Porém, antes de tudo, é necessário que haja uma investigação (iniciada após uma denúncia ou suspeita de crime) para esclarecer a materialidade (o que aconteceu), a dinâmica (como) e autoria (quem) dos atos ilícitos. Em geral, os procedimentos executados pela autoridade policial durante a inquirição são: dirigir-se ao local e preservar o estado e a conservação das coisas até a chegada dos peritos criminais; apreender os objetos que tiverem relação com o fato, após liberados pelos peritos; colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; proceder a reconhecimento de pessoas e coisas e a acareações; determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias; e outras condutas que estão fora do escopo deste trabalho. Portanto, no caso de uma investigação envolvendo uma análise de dispositivos computacionais, é possível identificarmos quatro etapas:

Coleta: Nesta etapa, o perito deve isolar a área, identificar equipamentos e coletar, embalar, etiquetar e garantir a integridade das evidências, garantindo assim a cadeia de custódia – mais informações no item 3.5, Métodos praticados para a preservação de evidências.

Exame: Nesta fase, deve-se identificar, extrair, filtrar e documentar os dados relevantes à apuração.

Análise: Nesta etapa os dados transformam-se em informações, ou seja, o perito computacional deve identificar e correlacionar pessoas, locais e eventos, reconstruir as cenas e documentar os fatos;

Resultado: Neste momento deve-se redigir o laudo e anexar as evidências e demais documentos.

2.2 - Locais de crime de informática e busca e apreensões de equipamentos computacionais

É chamado de local de crime o lugar onde uma suposta infração penal ocorreu. Nele, evidências muito úteis à investigação podem ser encontradas e ajudar a determinar o que aconteceu, como aconteceu e quem foi o responsável por tal ato. Por isso, o isolamento e análise da cena, a documentação minuciosa dos vestígios encontrados e sua posterior coleta são tarefas fundamentais para a apuração dos fatos. Um local de crime de informática nada mais é do que um local de crime convencional acrescido de equipamentos computacionais que podem ter relação com o delito investigado, não importando se eles foram utilizados como ferramenta de apoio ou como meio para a realização contravenção. Já o mandado de busca e apreensão é uma ordem expedida pela autoridade judiciária para que seja realizada uma diligência, a fim de procurar e apreender pessoas ou objetos que sejam de interesse à justiça. Ao participar do cumprimento dessa ordem judicial, o perito é o responsável por orientar a equipe quanto à preservação, seleção e reunião dos equipamentos computacionais, além da realização de exames forenses que se façam necessários ainda no local. Em ambos os casos, precauções especiais devem ser tomadas durante a coleta, transporte e armazenamento do material apreendido, uma vez que os vestígios digitais encontrados são muito sensíveis e podem ser facilmente perdidos e/ou destruídos por eletromagnetismo, impacto, calor excessivo, atrito, umidade, entre outros.

As primeiras atitudes de um perito, tanto num local de crime, quanto no cumprimento de mandado de busca e apreensões, devem ser direcionadas para a preservação dos dados digitais, como impedir que pessoas estranhas à equipe utilizem os equipamentos de informática existentes e não ligar equipamentos computacionais que estejam desligados. Tais práticas podem alterar e apagar os dados armazenados, mesmo que os usuários não o façam por vontade própria. Além disso, quando computadores estiverem ligados, pode ser necessário copiar as informações da memória RAM (Random Access Memory) que possuem a característica de serem voláteis, podendo ser perdidas quando o computador é desligado.

Após esses procedimentos, o perito deve realizar o reconhecimento do local, identificando os equipamentos computacionais presentes, incluindo computadores, notebooks, pontos de acesso de rede e outros, e verificar quais deles possam conter informações relevantes para elucidação dos fatos. Tais exames devem ser executados somente por profissionais capacitados na área de informática e de modo que nenhum conteúdo armazenado nos

dispositivos seja alterado, garantindo assim a preservação das evidências digitais e evitando questionamentos e a invalidação da prova. Adicionalmente, entrevistar as pessoas que residem e/ou trabalham no local sobre o uso desses aparelhos é uma medida recomendada para melhor selecionar os objetos a serem confiscados. Ao reter um equipamento, o perito também precisa levar em conta o foco da investigação. Não há uma regra específica sobre o que deve ser apreendido, mas se o mandado é para busca de arquivos, dados ou sistemas contidos em um computador, geralmente são levados para perícia os dispositivos de armazenamento computacional, como por exemplo, discos rígidos, CDs, DVDs, pen drives, cartões de memória etc. Se o tema principal da inquirição for a suspeita de falsificação de documentos, arresta-se também impressoras, scanners e multifuncionais. Todos os equipamentos citados, além de gravadores de mídias óticas, também são confiscados caso haja indícios de contrafação de mídias (pirataria). Já em investigações em que se precise identificar o endereço IP utilizado pelo computador nos últimos tempos, adicionalmente aos dispositivos de armazenamento computacional, apreende-se elementos de rede que possam armazenar históricos de conexão, como modems, Access Points, roteadores e switches. Como podemos perceber, essa é uma etapa muito importante, porque permite a apreensão somente dos equipamentos suspeitos de possuírem indícios referentes e necessários à investigação, evitando perda de tempo e esforço.

Todo o material confiscado deverá ser descrito em auto pela autoridade competente, comumente um delegado. Neste momento, é importante que ela utilize os conhecimentos técnicos do perito para a correta especificação dos objetos com o objetivo de garantir a idoneidade da prova e evitar dúvidas quanto à sua origem ou seu estado inicial. No caso de equipamentos computacionais, é recomendável sempre constar a quantidade, o tipo do dispositivo, a marca, o modelo, o número de série e país de fabricação. Em alguns casos, como discos rígidos e pen drives, também é desejável informar a capacidade de armazenamento.

Conforme já dito anteriormente, os equipamentos computacionais são frágeis e sensíveis ao tempo. Por esse motivo, alguns cuidados devem ser tomados durante seu acondicionamento e transporte, a fim de evitar perdas de evidências digitais. Os discos rígidos precisam evitar choques físicos e, quando possível, embalados com material antiestático. Já as mídias ópticas devem ser guardadas em seus estojos ou capas plásticas para evitar atritos na parte inferior, local onde os dados são gravados. Mas, em geral, todos os dispositivos computacionais, incluindo impressoras, equipamentos de rede, cartões de memória, pen drives, entre outros,

precisam ser mantidos longe da água, do calor, de lugares sujos ou com muito pó e da vibração excessiva.

Após a preservação do material apreendido, ele é encaminhado para a realização dos exames forenses em laboratórios que é o tema do próximo capítulo.

Capítulo 3 - Técnicas envolvidas na coleta e no exame de vestígios digitais

3.1 - Etapas de um exame forense computacional

Após o cumprimento de um mandado de busca e apreensão que tenha resultado na coleta de equipamentos computacionais, conforme descrito no capítulo anterior, deve-se encaminhar o material confiscado para um laboratório de informática capacitado a fim de realizar os exames forenses necessários. Ao receber um dispositivo de armazenamento computacional para análise, independente se for um disco rígido, DVD, pen drive, cartão de memória ou outra mídia, o perito deve seguir uma série de etapas que são descritas a seguir, porém serão melhores detalhadas ao longo desse capítulo.

- Preservação: Diferentemente do que ocorre durante a busca e apreensão de equipamentos, onde há um foco maior na integridade física deles, esta fase tem o objetivo de garantir que as informações armazenadas no material questionado jamais sejam alteradas durante toda a investigação e processo.

- Coleta de dados: Esta etapa baseia-se na execução de um conjunto de procedimentos para recuperar e catalogar todos os dados contidos na mídia investigada, estando eles ocultos ou explícitos. A partir de sua conclusão, será possível realizar buscas rápidas por palavras-chaves no conteúdo dos dispositivos armazenados.

- Análise: A análise dos dados consiste no exame das informações extraídas do material questionado durante a fase anterior, a fim de identificar evidências digitais que tenham relação com o delito investigado.

- Formalização: É a etapa final dos exames forenses e é formada pela elaboração do laudo pelo perito, apontando o resultado e apresentando as evidências digitais encontradas nos materiais examinados.

3.2 - Preservação

Assim como em um local de crime convencional cujas evidências e provas ali existentes devem ser preservadas, os dados contidos no material enviado para exames forenses jamais devem ser alterados. Inclusive, a garantia da cadeia de custódia é uma das principais obrigações do perito. Ele deve assegurar a proteção e idoneidade da prova, a fim de evitar questionamentos quanto à sua origem ou estado inicial, pois qualquer suspeita pode anulá-la e colocar em risco toda a investigação policial.

Precauções especiais devem ser tomadas ao manipular os equipamentos questionados, porque até operações simples podem modificar as evidências armazenadas. Ligar o computador, por exemplo, altera alguns arquivos, datas de último acesso e criam arquivos temporários, mesmo que o usuário não execute nenhuma ação. Até a trivial conexão de um pen drive na porta USB, pode gerar gravação de dados no dispositivo. Em vista disso, toda e qualquer atividade deve ser realizada com a garantia de que as informações armazenadas não sofram alterações. Por isso, os exames forenses devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original. Para conceber tais cópias, os peritos utilizam, principalmente, as técnicas de espelhamento e imagem.

O espelhamento é uma técnica que consiste na cópia exata e fiel dos dados contidos em um dispositivo de armazenamento computacional para outro, ou seja, a duplicação é feita bit a bit. Logo, o disco de destino deverá ter capacidade igual ou superior ao original, porém é preciso ficar atento, pois há no mercado vários discos com o mesmo volume nominal, porém com tamanho real diferente. Deve-se sempre comparar o número de setores de cada disco, cuja informação, denominada LBA, fica na etiqueta do fabricante. *Logic Block Addressing*, é uma organização lógica dos setores, utilizada nos discos rígidos atuais, que faz com que o computador enderece cada setor do disco sequencialmene, ao invés de usar localização física, como cilindro, cabeça e setor.

Caso o dispositivo que receberá a cópia seja maior do que o original, é necessário garantir que todo o espaço remanescente esteja limpo, a fim de não sobrar resquícios de dados que possam ser confundidos durante os exames. Esse processo de limpeza é chamado de *wipe* e consiste em excluir um arquivo ou toda uma partição e gravar bytes na mesma área do disco, desta forma se houver algum software que faça a leitura binária do disco, este verá os dados recém gravados e não os originais. O *wipe* dispõe de vários métodos que executam avançados algoritmos, sendo que cada um tem os seus prós e contras, mas que diferem-se principalmente

pelo nível de segurança e tempo de processamento. Inclusive, o Departamento de Defesa dos Estados Unidos criou a metodologia *DoD* 5220.22 que consiste em sobrescrever os locais endereçáveis do disco primeiro com um caractere, depois com o seu complemento e por fim com um caractere aleatório. Porém, há outras opções que vão desde a sobrescrita de toda a área desejada com um caractere específico (0x00), até métodos que fazem isso sete vezes, alternando as seis primeiras entre 0x00 e 0xff e a última com um caractere randômico. Mas, segundo o documento SP 800-88 publicado pelo NIST (National Institute of Standards and Technology) em 11 de setembro de 2006, “estudos têm mostrado que a maioria das mídias atuais podem ser efetivamente sanitizadas com apenas uma sobrescrita”. Entretanto, assim como o *wipe* pode evitar enganos durante a fase de análise com a limpeza do espaço excedente, ele pode ser usado também pelos criminosos para apagar os vestígios deixados pela atividade criminosa.

Outra recomendação que deve ser seguida ao utilizar a técnica de espelhamento é jamais utilizar como destino discos rígidos com setores defeituosos, caso contrário, o dado original referente àquele setor não será copiado, gerando, assim, uma perda de evidências e uma duplicação incompleta. Além disso, alguns estudos mostram que os trechos defeituosos de um disco tendem a aumentar cada vez mais, comprometendo novas áreas de dados, resultando em mais perda de informações.

A duplicação de discos utilizando a técnica de gerar uma imagem sobre eles possui um processo semelhante ao espelhamento, onde se copia o sistema operacional, programas, drivers, configurações e todo tipo de arquivo, originando assim uma reprodução exata e fiel do disco. Porém, ao invés de copiar bit a bit os dados de um dispositivo para outro, eles são copiados para arquivos de imagem. Essa técnica possui algumas vantagens em relação ao espelhamento, como a possibilidade de copiar o disco inteiro ou apenas uma de suas partições; a possibilidade do dispositivo de destino ser utilizado para receber distintas imagens de dispositivos variados, se houver capacidade suficiente; a maior facilidade em manipular os dados, uma vez que são arquivos que podem ser replicados de maneira simples por qualquer sistema operacional; e a capacidade de compactar os arquivos de imagens, e assim, economizar a utilização do disco de destino.

Tanto no processo de espelhamento, quanto por imagem, a cópia dos dados deve ser efetuada de forma que nenhuma informação contida no material questionado seja alterada. Atualmente, podem ser encontrados no mercado diversos equipamentos e softwares forenses que auxiliam na realização dessa tarefa, como por exemplo, produtos para acesso somente leitura das

informações em discos rígidos e para duplicação, incluindo as duas técnicas citadas neste texto.

Os bloqueadores de escrita em disco rígido são os dispositivos mais comuns e simples de serem utilizados. Conectado entre o material questionado e o computador, esse tipo de equipamento possui a garantia, certificada pelo próprio hardware, de que nenhum dado será gravado, necessitando apenas utilizar o programa específico para a cópia do disco. Já os duplicadores forenses são equipamentos muito mais avançados e, além de efetuarem o bloqueio de escrita, também permitem a realização de cópias para outros discos rígidos, via espelhamento ou imagem. A sua utilização para o processo de duplicação de dados possui as vantagens de suportar múltiplas interfaces de conectores (IDE, SATA), velocidade muito maior na cópia das informações e ausência da necessidade de um computador dedicado. Na falta desses equipamentos, pode-se efetuar a duplicação de discos rígidos com o uso de alguns softwares específicos que não alterem as evidências contidas no material questionado, como por exemplo, os sistemas operacionais forenses Knoppix e Helix que acessam os dados de forma somente leitura e têm o comando *dd* (duplicar disco), utilizado para realizar o espelhamento ou imagem do dispositivo. É importante ressaltar novamente que um computador contendo discos rígidos questionados e desprotegidos contra gravação não deve ser inicializado com sistemas operacionais convencionais, pois, mesmo que o usuário não faça nenhuma operação, alterações serão realizadas nos dados.

Além dos riscos de alteração das informações armazenadas, conforme dito anteriormente, os dados contidos nos equipamentos computacionais podem ser perdidos ao longo do tempo, pelo término da vida útil dos materiais utilizados na fabricação, pela quebra dos dispositivos mecânicos ou pela desmagnetização. Devido a essa fragilidade, tornou-se muito comum no meio computacional a realização de cópias de segurança dos mais variados dados.

Outro fator que deve ser levado em conta é a sensibilidade ao tempo de uso. Quando um computador é utilizado para a realização de um crime, seja como meio, seja como ferramenta, rastros são deixados nos dispositivos de armazenamento e eles podem ser apagados pelo usuário. Além disso, sabe-se que as chances de recuperação dessas informações diminuem à medida que os equipamentos são utilizados (mais informações no item 3.3). Portanto, o tempo torna-se um fator crucial em investigações envolvendo vestígios digitais, devendo os exames forenses ser feitos o mais rápido possível a partir do recebimento do material apreendido e assim minimizar a perda de evidências ocasionadas pelo excesso de tempo de vida ou de tempo de uso do dispositivo.

Após o término da fase de preservação, o dispositivo de armazenamento computacional deverá ser lacrado e guardado em local apropriado até que haja uma autorização por parte da justiça permitindo o seu descarte ou devolução.

3.3 - Coleta de dados

A fase de coleta de dados consiste basicamente na recuperação, reunião e organização de todas as informações contidas na cópia dos dados proveniente do passo anterior, ou seja, todas as ações deverão ser executadas no espelho ou na imagem do disco, mantendo o material original intacto e protegido. Essa etapa é de suma importância para o processo investigatório, pois as análises dos indícios serão realizadas a partir de seu resultado. Uma eventual falha nessa fase, como por exemplo, a negligência em não analisar todas as partes do disco rígido, compromete a produção de provas e pode influenciar na decisão das autoridades judiciais.

Ao examinar o material, é primordial que a extração dos dados seja feita de forma minuciosa e com muita atenção, uma vez que as evidências da realização do delito podem estar nas áreas mais improváveis do disco ou até terem sido removidas. Por isso, o perito não deve se limitar apenas em coletar os chamados “arquivos convencionais”. Os dispositivos de armazenamento, devido ao tipo de organização dos dados, guardam mais informações do que as acessadas pelos usuários comuns. Desse modo, podemos dividir os discos rígidos em camadas, cuja a mais superficial possui os arquivos visíveis aos usuários tradicionais de computador, enquanto que nas camadas mais internas encontramos os arquivos ocultos, criptografados, temporários e apagados, além de fragmentos de arquivos, sistemas computacionais, bancos de dados, registros de impressão, swap de memória, entre outras informações. À medida que se quer conhecer as partes mais profundas, maior será o tempo e a complexidade para a exploração das camadas, necessitando, assim, de técnicas especiais para recuperação e interpretação dos dados.

Para que a extração dos dados seja completa e da melhor maneira possível, é essencial que se conheça o sistema operacional contido no disco e, principalmente, o sistema de arquivos utilizados. Um sistema de arquivo é o conjunto de estruturas lógicas e de rotinas que define o modo como os arquivos são estruturados, nomeados, acessados, utilizados, protegidos e manipulados pelo sistema operacional. Ele armazena os arquivos como seqüência de bytes e os organiza dentro de uma hierarquia de diretórios, gerenciando seus nomes e conteúdos além

de atributos como posse, permissões de acesso, data e hora da última modificação etc. Na verdade, essa percepção de arquivos, diretórios e atributos é uma das representações que os sistemas de computador criam para facilitar o uso por parte dos programas aplicativos e seus usuários. Os sistemas de arquivos, na realidade, alocam espaço a partir de um arranjo linear de blocos de disco de igual tamanho e destinam parte dessa capacidade de armazenamento para seus próprios propósitos.

Mesmo a noção de um arranjo linear de blocos de disco de igual tamanho é uma ilusão, cujo objetivo é tornar a implementação dos sistemas de arquivos mais fácil. Discos físicos têm cabeças e pratos e armazenam informações em domínios magnéticos, além de também reservar um espaço para uso próprio. À proporção que desmontamos camada após camada, as informações tornam-se mais precisas devido a sofrer menos processamento. Entretanto, quanto mais nos aproximamos dos bits brutos, menos significativas as informações se tornam, pois temos cada vez menos conhecimento sobre a sua finalidade.

Conforme dito anteriormente, para que haja uma correta recuperação dos dados contidos no disco, é necessário que se conheça o sistema de arquivos utilizado. Entretanto, existe atualmente uma grande variedade de sistemas como FAT16, FAT32, NTFS, EXT2, EXT3, UFS, JFS, HPFS, Reiser, entre outros, cada qual com a sua maneira de estruturar e organizar os bits. Não é o foco deste trabalho descrever os pormenores existentes em cada um deles, e sim, apresentar um panorama geral dos sistemas de arquivos e suas características mais comuns. Entretanto, hoje já é possível encontrar uma vasta bibliografia técnica sobre eles. Além disso, todo esse conhecimento já foi sistematizado, possibilitando a criação de ferramentas forenses que examinam toda a superfície do disco em busca de bytes significativos, de acordo com o sistema de arquivo subsistente. Essa automatização proporcionou que a extração dos dados tivesse uma redução significativa de tempo e permitiu que o perito se dedicasse mais na etapa de análise e produção de evidências.

Ao apagar um arquivo de um computador, o sistema de arquivo não sobrescreve todo o conteúdo ocupado por ele no disco rígido com zeros e/ou uns, porque isso demandaria muito esforço da cabeça de gravação e, consequentemente, muito tempo. O sistema “apenas” tem um controle de quais partes do disco estão livres e quais estão ocupadas. Assim, na realidade, ao apagar um dado, o sistema de arquivo apenas altera o status desse espaço de utilizado para livre. Com isso, os dados referentes aos arquivos apagados continuam armazenados no disco rígido e podem ser recuperados. Porém, esses bits podem ser sobrescritos a qualquer momento pelo sistema operacional, uma vez que esse espaço está disponível para uso.

Entretanto, a destruição de informações acaba se revelando algo difícil de realizar. Embora discos magnéticos sejam projetados para armazenar informações digitais, a tecnologia subjacente é analógica, isto é, o valor de um bit é uma combinação complexa dos valores guardados no passado. Com circuitos eletrônicos modificados, sinais a partir dos cabeçotes de leitura de disco podem revelar dados mais antigos como modulações no sinal analógico. Outra maneira de analisar os discos é por meio do exame da superfície, onde, utilizando-se de técnicas de microscopia eletrônica, revelam-se padrões magnéticos antigos que persistem em uma trilha de disco. Assim, os dados em um disco magnético podem ser restaurados mesmo depois de serem sobrescritos múltiplas vezes. Porém, a recuperação nos casos citados somente seria possível em circunstâncias especiais, pois os processos para leitura de vestígios de dados anteriores requerem tempo, equipamentos, instalações e procedimentos sofisticados que não são viáveis na prática forense normal. Além disso, a restauração convencional de arquivos excluídos se mostra suficiente para a investigação.

As informações apagadas podem ficar intactas por meses ou até mesmo por anos devido ao projeto de alto desempenho do sistema de arquivos que evita movimentos do cabeçote de disco mantendo os dados relacionados juntos. Isso não apenas reduz a fragmentação do conteúdo de um arquivo individual, como também reduz retardos ao se percorrer diretórios para acessar um arquivo. Um típico sistema de arquivos com essas propriedades divide o espaço de armazenamento em múltiplas zonas. Cada zona contém sua própria tabela/bitmap de alocação dos bytes, blocos de dados de arquivo e blocos de atributo de arquivo. Normalmente, as informações sobre um pequeno arquivo são armazenadas inteiramente dentro de uma zona; novos arquivos são criados preferivelmente na mesma zona do seu diretório pai e novos diretórios são criados nas zonas que possuem poucos diretórios e muito espaço não utilizado. Esse processo de agrupar os arquivos de diferentes usuários ou aplicativos de acordo com as diferentes zonas do sistema de arquivos, mantendo as informações relacionadas dentro da mesma zona, chama-se *clusterização*. Por isso, o tempo de sobrevivência das informações excluídas depende fortemente do volume das atividades de gravação em arquivo dentro da sua zona.

Quando um arquivo é excluído em uma zona de baixa atividade, as informações sobre seus blocos de dados e atributo de arquivo podem escapar da destruição desde que a atividade do sistema de arquivos permaneça dentro de outras zonas. À medida que o disco se enche, a atividade de gravação inevitavelmente migrará para vizinhanças calmas das zonas de baixa atividade, transformando-as em zonas de alta atividade destrutiva. Até esse momento, as informações de arquivo excluído nas zonas de baixa atividade podem sobreviver intactas e em

quantidades volumosas. Por outro lado, quando um arquivo é excluído em uma zona de alta atividade, as informações sobre seus blocos de dados e atributo de arquivo serão sobrescritas de maneira relativamente rápida por novos arquivos. Portanto, conclui-se que quanto mais recentemente um arquivo foi apagado, maiores são as chances de recuperá-lo.

Ao varrer todos os bits de um dispositivo de armazenamento computacional, além de recuperar as informações de arquivos excluídos, também é feita a indexação dos dados contidos nele. Ela consiste em localizar todas as assinaturas de arquivos conhecidas, organizando-as de forma que sejam acessadas e recuperadas rapidamente. Após a execução desse processo, é possível saber quais e quantas são as ocorrências de cada uma das cadeias alfanuméricas. É criada então uma espécie de catálogo contendo cada uma das cadeias encontradas e sua localização, possibilitando a realização de buscas rápidas por palavras-chave no conteúdo dos dispositivos examinados.

Uma vez concluída a coleta e indexação dos dados dos dispositivos de armazenamento computacional, cabe ao perito executar a próxima fase: Análise.

3.4 – Análise dos vestígios encontrados

A análise de dados é a fase que consiste no exame das informações extraídas na etapa anterior, a fim de identificar evidências digitais presentes no material examinado que tenham relação com o delito investigado. Essa relação se estabelece através dos quesitos elaborados pela autoridade solicitante presentes no laudo. Eles devem ser claros e específicos, pois analisar individualmente todo o conteúdo do dispositivo de armazenamento computacional tende a ser inviável, ocupando um tempo muito grande do perito e impactando na eficiência dos exames forenses. É recomendável, sempre que possível, que as autoridades detalhem os tipos de arquivos procurados e utilizem quesitos com nomes de pessoas, empresas e/ou documentos específicos, possibilitando, assim, a procura por meio de palavras-chave. É aconselhável que o solicitante entre em contato com um especialista antes de elaborar os quesitos com o objetivo de se evitar trabalhos desnecessários.

Em alguns casos, um disco rígido com capacidade de 80 GB (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 a um, pode levar

muito tempo e tornar o exame impraticável. Com o objetivo de auxiliar o perito nessa tarefa, procedimentos e técnicas podem ser utilizados para tornar esse processo mais eficiente.

Um desses procedimentos é utilizar um filtro de arquivos conhecidos para eliminar da análise aqueles que não são importantes para a investigação. O Instituto Nacional de Justiça (NIJ) do Departamento de Justiça dos Estados Unidos, em conjunto com o Instituto Nacional de Padrões e Tecnologia mantém um projeto chamado Biblioteca Nacional de Referência de Software com o objetivo de promover o uso eficiente e eficaz da tecnologia em investigações de crimes envolvendo computadores. A biblioteca foi projetada para coletar programas de diversas fontes, criar um perfil para cada um deles e adicioná-lo às informações do Conjunto de Arquivos para Referência (RDS). O RDS pode ser usado pelas polícias, governos, órgãos investigativos e empresas e consiste numa coleção de assinaturas digitais de arquivos conhecidos e rastreáveis até sua origem. Ele, ao permitir que se compare os perfis criados com os arquivos do dispositivo de armazenamento, ajuda a mitigar o esforço envolvido em determinar quais dados são importantes como evidências.

Desta forma, é possível diminuir, por exemplo, o número de arquivos a serem examinados. Se ao conteúdo do disco rígido for aplicado um filtro com base no RDS dos arquivos conhecidos do sistema operacional e dos programas instalados, obter-se-á uma lista de arquivos que podem ser ignorados durante a análise do perito sobre o conteúdo do disco, uma vez são arquivos sem relação com a investigação. Da forma oposta, o RDS também pode ser utilizado para indicar arquivos que são de interesse à investigação. Essa abordagem é muito praticada quando se pretende verificar a existência de um mesmo arquivo em várias mídias computacionais, como por exemplo, para se verificar se houve cópias ilegais de programas protegidos por direitos autorais. Portanto, o uso do RDS torna possível uma análise mais eficiente, desde que se conheça previamente o que se pode descartar ou o que se deve procurar.

Outra técnica que auxilia o perito nessa fase é pesquisar o conteúdo de um dispositivo de armazenamento por palavras-chaves. Uma vez realizada a indexação dos dados, onde todo o conteúdo do disco foi percorrido e estruturado, diversas buscas podem ser efetuadas de forma rápida e eficaz para localizar arquivos e fragmentos de arquivos que interesse à investigação. Também é possível realizar essa busca sem que a indexação seja feita previamente, entretanto, a cada nova pesquisa, o sistema deverá varrer todo o conteúdo do disco novamente, gastando muito tempo dependendo da capacidade e da velocidade de leitura. A pesquisa por palavras-chaves é, portanto, um meio eficiente para encontrar a maioria das evidências digitais

necessárias para elaboração de laudo forense. O único porém é que, se o conteúdo dos arquivos estiver criptografado, a busca não encontrará os valores procurados.

Percorrer os dados dos dispositivos de armazenamento computacional por meio da estrutura de pastas e arquivos é um procedimento eficiente para localizar vestígios de interesse à investigação, pois geralmente os usuários convencionais utilizam determinadas pastas para armazenar seus arquivos pessoais, como por exemplo, *Documentos*, *Fotos* e *Downloads*. 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. Essa emulação é feita sem alterar os dados das cópias realizadas na fase de preservação e é possível através da criação de uma camada de dados intermediária entre a máquina virtual emulada no computador do perito e a cópia do disco rígido que contém o sistema operacional. Com a virtualização, é possível inicializar o sistema operacional desses discos rígidos em uma máquina virtual, auxiliando e permitindo ao perito a visualização e utilização do mesmo, como se ele estivesse sido ligado normalmente. Em alguns casos, é muito trabalhoso executar um sistema específico a partir de outra máquina realizando-se apenas a cópia dos arquivos referentes a ele. Geralmente, muitas configurações são necessárias e podem tomar muito tempo do perito.

Investigações de invasões de computadores e subversão de sistemas requerem um pouco mais de atenção e tempo, pois os exames são feitos, geralmente, depois que o sistema foi comprometido. Nesse caso, embora as conseqüências sirvam como ponto de partida da análise, o perito deverá, se possível, reconstruir todo o cenário e ações executadas pelo invasor até descobrir a origem do ataque e a vulnerabilidade do sistema explorada. Para isso, conforme dito anteriormente, o RDS pode ser usado para comparar os arquivos do sistema comprometido com os arquivos originalmente lançados pelas empresas, a fim de saber se há algum código malicioso tentando se passar por um programa confiável.

Outro procedimento usualmente executado é o estudo das datas e horas dos arquivos. Embora eventos individuais possam ser interessantes quando considerados isoladamente, suas seqüências no tempo fornecem um contexto valioso que pode alterar seus significados. Por exemplo, novos programas são instalados regularmente, mas, se um aplicativo foi introduzido logo após um computador ter sido invadido, essa ação assume um novo sentido. Todos os arquivos e diretórios possuem, independente do sistema de arquivos utilizados, ao menos três atributos de tempo: *mtime*, *atime* e *ctime*, chamados pelos profissionais da área de *MACtimes*.

O atributo *atime* refere-se à última data e hora em que o arquivo ou diretório foi acessado. O atributo *mtime* monitora quando o conteúdo de um arquivo ou diretório é modificado. Já o atributo *ctime* muda quando o conteúdo ou as meta-informações sobre o arquivo mudaram, como por exemplo, o proprietário, o grupo, as permissões etc. Ele também pode ser utilizado como uma aproximação de quando um arquivo foi excluído.

Os *MACtimes* são muito úteis para descobrir o que aconteceu depois de um incidente, porém, eles possuem algumas deficiências. A primeira delas é que eles só informam a última vez em que um arquivo foi modificado e, consequentemente, não fornecem nenhuma maneira de revelar o histórico de atividades dele. Ou seja, um programa malicioso pode ser executado diversas vezes, porém só haverá vestígios de uma única ocorrência. Outra limitação é que os *MACtimes* só mostram o resultado de uma ação, não quem a fez. Além disso, sua coleta e análise precisam ser feitas minuciosamente, porque eles são extremamente efêmeros e sensíveis. Até ações mais simples, como a cópia de arquivos, destroem vestígios redefinindo as datas e horas de acesso ao arquivo.

Para sanar um desses problemas dos *MACtimes*, criou-se um recurso nos sistemas de arquivos conhecido como *journaling*. Com ele, algumas ou todas as atualizações de disco são, primeiro, gravadas um arquivo de registro seqüencial (*journal*) antes de serem gravadas no próprio sistema de arquivos (Robbins, 2001). Ou seja, cada operação não-trivial no sistema de arquivos, como criar ou alterar um arquivo, resulta numa seqüência de atualizações de disco que afeta tanto os dados do arquivo (isto é, o conteúdo), como os metadados dele (por exemplo, a localização do conteúdo e quais arquivos pertecem a um diretório). Quando essa seqüência de atualizações é interrompida devido a uma queda de sistema, os sistemas de arquivos sem suporte a *journaling* podem deixar os metadados dos seus arquivos em um estado inconsistente e o processo de recuperação pode levar várias horas. Já a recuperação com um sistema de arquivo com *journaling* é quase instantânea, podendo ser tão simples como refazer as gravações do sistema de arquivos a partir dos registros contidos. Do ponto de vista forense, o *journal* é uma série de datas/horas do *MACtime* e de outras informações sobre o arquivo que permite observar o acesso repetido a ele. Embora à primeira vista isso pareça trabalho extra, o sistema de arquivos com *journaling* pode aprimorar a análise dos vestígios, além de melhorar significativamente a recuperação do sistema em caso de queda.

Nos sistemas de arquivos atuais, os arquivos e diretórios possuem, entre outros atributos, um nome e um número. O nome é o texto usado pelos programas e usuários a fim de identificar o arquivo. Já o número refere-se a um *inode* do arquivo em uma tabela chamada blocos *inode*, que descrevem todas as suas propriedades de um arquivo, exceto seu nome[1](Essa estrutura se

refere a sistemas de arquivos UNIX, porém a maioria dos outros sistemas possuem as mesmas características). O bloco *inode* tem referências aos blocos de dados que contêm o conteúdo real do arquivo. À medida que o sistema operacional é instalado no disco e que os arquivos são criados, os números de *inode* são atribuídos pelo sistema de arquivos de forma seqüencial. Dessa forma, é possível identificar invasões e códigos maliciosos que se passam por programas confiáveis através da análise o número de *inode* de arquivo.

Terminada a fase de análise dos dados, cabe ao perito realizar a formalização do estudo efetuado através da elaboração do laudo pericial, apontando o resultado e apresentando as evidências digitais encontradas nos materiais examinados. No laudo devem constar os principais procedimentos realizados, incluindo as técnicas utilizadas para preservar, extrair e analisar o conteúdo das mídias digitais.

3.5 - Métodos praticados para a preservação de evidências

Conforme discutido no item 3.2 deste capítulo, é essencial que haja a garantia da integridade do conteúdo de um dispositivo de armazenamento computacional questionado, tanto que se recomenda a duplicação dos dados presentes nele e assim, todos os exames são realizados na cópia efetuada. Porém, esse procedimento por si só não assegura que as informações ficarão intactas até a conclusão do processo. Além disso, em exames forenses, principalmente na área de informática, é comum a necessidade de se encaminhar arquivos anexos juntamente com o laudo para a apreciação do juiz. Quando possível, é permitido realizar a impressão de arquivos que podem ser reproduzidos em papel sem a perda de informações, como textos, planilhas, figuras e relatórios de sistemas. No entanto, quando se trata de uma grande quantidade de dados ou quando o conteúdo dos arquivos não tem um formato apropriado para exibição impressa, como programas executáveis, seqüências de vídeo, sons e bancos de dados, faz-se necessária a utilização de um computador. Uma solução viável é a gravação das evidências digitais encontradas pelo perito em mídias computacionais ópticas, como CDs, DVDs e Blu-Rays, que permite o encaminhamento dos arquivos em seu formato original e sem perda de informações. Essa técnica, além de possibilitar que um grande volume de dados seja anexado ao laudo, facilita a sua manipulação, uma vez que, com o uso de um computador, algumas funcionalidades podem ser utilizadas para tornar o trabalho mais eficaz,

como por exemplo, a procura por palavras-chave e cálculos a partir dos resultados apresentados.

Tanto no caso do dispositivo de armazenamento computacional questionado, quanto na utilização de mídias ópticas para armazenar as evidências digitais, há a preocupação de assegurar que o conteúdo desses materiais não tenha sido alterado nem substituído até a conclusão do inquérito e, consequentemente do processo. Assim, torna-se necessário lançar mão de mecanismos que permitam a verificação da integridade e da legitimidade dos dados gravados, sendo que o principal é o cálculo realizado utilizando funções de autenticação unidirecionais conhecidas como *hash*. Essas funções geram, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo, ou seja, é a transformação de uma grande quantidade de informações (informação original) em uma pequena seqüência de bits (valor hash). O que torna esse tipo de função extremamente utilizada para a verificação de integridade de dados computacionais é o fato que uma simples alteração na informação de entrada do algoritmo gerará uma seqüência de bits (valor hash) completamente diferente. Assim, se o conteúdo de um arquivo é submetido a uma função unidirecional, em seguida ter o seu conteúdo alterado em um único bit e passar novamente pela mesma função, serão obtidas como resultado duas seqüências de bits completamente diferentes. Outra vantagem adquirida com o uso das funções unidirecionais é que a realização do processo inverso é impossível, isto é, não é possível retornar à informação original a partir de um valor hash. Isso faz com que tais funções sejam de grande aplicação em algoritmos de criptografia. No entanto, como o tamanho da seqüência de bits gerada é limitado, muitas vezes não passando de 128 bits, existem colisões, ou seja, valores hash iguais para informações originais diferentes, uma vez que a variedade de informações de entrada é ilimitada. Assim, quanto maior a dificuldade de se encontrar colisões, melhor é o algoritmo. Atualmente, as funções mais utilizadas são: o MD5 (128 bits), o SHA-1 (160 bits), o SHA-256 (256 bits) e o SHA-512 (512 bits).

Na fase de preservação, após a duplicação dos dados do dispositivo de armazenamento computacional original, o perito pode utilizar o hash criptográfico como forma de registrar o conteúdo de cada arquivo presente no disco rígido questionado. Entretanto, o material questionado, seja um disco rígido, um cartão de memória, um disquete ou um pen drive, não armazena somente o conteúdo de seus arquivos. Uma série de estruturas, como a tabela de partição e a tabela de alocação de arquivos, além da área não alocada e disponível para utilização, também é armazenada na própria mídia. Assim, para garantir a integridade e autenticidade do dispositivo de armazenamento, pode-se calcular o valor hash de todo o seu

conteúdo. No entanto, vale ressaltar que, se o conteúdo de um disco rígido questionado, por exemplo, apresentar uma pequena variação, mesmo que seja de um bit, o valor hash do conteúdo de todo o disco será completamente diferente. Por isso, deve haver uma atenção especial para o correto acondicionamento do material questionado, livre do calor excessivo, da alta umidade, do atrito, de campos magnéticos e de vibrações. A fim de se criar mais uma redundância, o perito pode, também, calcular o conteúdo da mídia de forma segmentada, dividindo-a em partes iguais. Assim, além de um valor hash para todo o conteúdo do disco, existiria também um valor hash para cada parte que garantiria a sua integridade individual. Desse modo, se o disco sofresse alterações e algum questionamento fosse feito sobre a integridade da prova, apenas os segmentos alterados poderiam ser descartados, evitando-se, assim, em última instância, que toda a prova fosse invalidada.

Após a realização do cálculo utilizando funções unidirecionais para cada parte do disco, será obtida uma relação das partes contidas no dispositivo de armazenamento e o seu respectivo hash em valor hexadecimal. Essa relação deverá ser registrada em um arquivo de texto, o qual deverá ser gravado numa mídia óptica que será anexada no laudo. Em seguida, calcula-se o valor do hash desse arquivo e coloca-o no corpo do laudo impresso, que também deve conter todo esse procedimento. Uma vez recebido o resultado da perícia com seus respectivos anexos digitais gravados em uma mídia óptica, é necessário conferir se ela não foi substituída ou alterada por outra qualquer. Essa verificação consiste basicamente em calcular novamente os hashes dos arquivos contidos na mídia e compará-los com os códigos de integridade obtidos anteriormente. Caso os valores obtidos se apresentarem iguais àqueles presentes no laudo e na mídia, significa que as informações foram preservadas, garantindo assim o cumprimento da cadeia de custódia.

Capítulo 4 - Principais dificuldades que podem surgir durante a investigação

Durante todo o processo investigatório, desde a etapa de recolhimento dos equipamentos para exames até a fase de análise dos dados encontrados, o perito depara-se com diversos desafios que podem atrapalhar ou impossibilitar a apuração dos fatos. Essas dificuldades, quando impostas explicitamente pelos usuários, são conhecidas comumente na área pelo termo Anti Forense e consistem em métodos de remoção, ocultação ou subversão de evidências com o objetivo de mitigar os resultados de uma análise forense computacional. Podemos citar como exemplo desse tipo de prática, a criptografia, a existência de senhas e o uso do *wipe* e da esteganografia.

Além dessas complicações, existem outras que surgem de acordo com o avanço da tecnologia. Como a área da computação está em constante evolução, o cenário futuro do ponto de vista da Perícia Forense Computacional não é animador, já que as técnicas de coleta e análise de dados não conseguem acompanhar o mesmo ritmo da área. Temos como exemplo desse tipo de dificuldade, o aumento da quantidade de arquivos.

Por último, há os entraves impostos pela falta ou deficiência de legislação que apóiem e sirvam de sustentação para o trabalho das autoridades investigativas, dos peritos e dos juízes. Sem uma regulamentação que tipifique todas as transgressões cometidas no meio virtual e um acordo de colaboração mundial, criminosos ficam impunes e vítimas não têm o seu dano reparado.

Todos esses desafios são explicados a seguir, com exceção do uso da técnica de *wipe*, já explicada no item 3.2 Preservação, e dos aspectos jurídicos envolvidos durante a investigação, que serão discutidos no capítulo 5.

4.1 - Quantidade de arquivos

A capacidade de armazenamento de dados dos dispositivos atuais vem crescendo vertiginosamente. Há poucos anos, era comum a comercialização de disco rígidos com capacidade medida em Megabytes (MB). Hoje, a maioria dos discos vendidos no mercado possui centenas de Gigabytes (GB), porém é fácil encontrar discos com capacidade superior a um Terabyte (TB). Assim, é de se esperar que o número de arquivos contidos nesses

dispositivos aumente de forma proporcional ao volume de armazenamento de informações. Em alguns casos, dispositivos com capacidade inferior a 100 GB podem ter mais de um milhão de arquivos. Manipular e encontrar as evidências desejadas nessa quantidade exorbitante de dados é um desafio e tanto para o perito. A aplicação de filtros como RDS e a procura por palavras-chave ajudam a minimizar este trabalho. Entretanto, é praticamente inviável analisar individualmente todos os arquivos contidos nas mídias de hoje em dia. Dessa forma, para a realização de exames com maior rapidez, é fundamental que se possua conhecimento da investigação, sabendo exatamente o que deverá se procurado. Para isso, os quesitos da solicitação de elaboração do laudo devem ser específicos e claros, evitando-se indagações genéricas. Portanto, é fundamental que a autoridade solicitante tenha um escopo bem delineado sobre o que perguntar ao perito em um exame de Computação Forense.

4.2 - Existência de senhas

Durante a realização de exames na área de informática, é comum se deparar com arquivos e programas protegidos por senha, que podem ocultar possíveis evidências. Assim, é necessário que o perito conheça técnicas para transpor essa barreira. Uma delas é através de ataque de força bruta que consiste em descobrir a senha de um arquivo e/ou sistema por meio de um simples processo de tentativa e erro, em que inúmeras combinações são testadas até que se acerte a senha. Há algumas ferramentas que permitem a criação de um domínio de checagem, definindo o número mínimo e máximo de caracteres e a utilização de letras maiúsculas, minúsculas, números, caracteres especiais e máscaras. O uso desses parâmetros é importante para tentar minimizar o número de combinações a serem testadas. Essa técnica é a mais simples e fácil de utilizar, além de ser muito eficiente quando as senhas são pequenas e utilizam exclusivamente números. Como datas são muito comuns em senhas, a utilização de um ataque contendo somente números de até oito dígitos é um bom ponto de partida para a descoberta. Entretanto, o ataque de força bruta necessita normalmente de um grande esforço computacional e pode levar muito tempo, chegando, em diversos casos, a tornar-se inviável.

Outra maneira de "quebrar" senhas de arquivos é com a utilização de ataques de dicionário. Semelhante ao ataque de força bruta, essa técnica também utiliza o método de tentativa e erro, porém nesse caso o domínio a ser utilizado são palavras ou cadeia de caracteres prontas, daí o nome dicionário. Assim a partir de uma lista de palavras, todas são testadas como possíveis

senhas, sendo possível também utilizar combinações delas. Os dicionários para ataque podem ser construídos baseados em senhas descobertas em casos anteriores ou nos dados encontrados no material questionado. Muitas ferramentas forenses realizam a indexação de dados, resultando uma lista com as palavras encontradas no dispositivo que pode ser usada no dicionário de ataque. Esse procedimento é muito eficiente e caso a senha esteja armazenada no dispositivo examinado, mesmo que seja um armazenamento temporário do próprio sistema operacional, como a memória virtual, terá êxito garantido. Outras boas opções são obter um dicionário específico para cada dispositivo de armazenamento que contém os arquivos/sistemas a serem quebrados ou utilizar dicionários contendo as senhas mais comuns em diversos idiomas.

4.3 - Criptografia

Criptografia, que em grego significa “escrita escondida”, é uma técnica utilizada para escrever em códigos, ou seja, com o uso de algoritmos matemáticos, transforma a informação em sua forma original e legível para um texto incompreensível, procurando garantir a privacidade do dado original. Sua classificação pode ser feita da seguinte maneira: sentido único e dois sentidos. No primeiro caso, não é possível saber quais foram as informações de entrada enviadas para a função de encriptação que produziram o valor obtido, isto é, não há a descriptografia. A função hash, explicada no item 3.5, é um exemplo de criptografia de sentido único, pois através do valor gerado, não é possível reconstituir os dados que o originaram, sendo muito utilizada em validações de senhas, onde se armazena o hash calculado ao invés da senha em texto puro. Em situações como essa, o perito pode se utilizar das *Rainbow Tables*, que são enormes tabelas de hashes pré-compilados para cada combinação existente de caracteres. Isso é possível graças ao resultado de tamanho fixo gerado pela função. Dessa forma, com um valor obtido é possível varrer as tabelas para localizar o texto original. Entretanto, quanto maior o tamanho das senhas e a quantidade de caracteres a se considerar (apenas alfa-numérico ou com caracteres especiais, como !@#), maior será o volume de registros das tabelas, tornando-as muito grandes de se armazenar.

A criptografia em dois sentidos é semelhante à de sentido único, ou seja, através de algoritmos, a informação original é transformada em um texto ininteligível. Porém, nesse caso, é necessária a utilização de informações confidenciais, conhecidas como chaves, para

efetuar codificação e para decifrar a mensagem. Desse modo, essa técnica é muito utilizada na transmissão de dados sensíveis por canais de comunicação inseguros, pois, mesmo que pessoas não autorizadas visualizem o texto criptografado, somente o destinatário possuidor da chave criptográfica conseguirá realizar o processo inverso e chegar aos dados iniciais.

É importante sempre buscar por programas instalados no equipamento analisado que executem essa tarefa, pois, dessa maneira, pode ser possível determinar o algoritmo utilizado, ou, até mesmo, manipular o próprio software para decodificar o conteúdo do arquivo e/ou sistema. É fundamental que o perito tenha conhecimentos avançados sobre este assunto, a fim de descobrir possíveis códigos criptografados no dispositivo examinado e buscar por ferramentas capazes de recuperar a informação original.

4.4 - Esteganografia

A esteganografia, que em grego significa “escrita encoberta”, é o estudo e uso de técnicas para fazer com que uma forma escrita seja disfarçada em outra a fim de mascarar o seu verdadeiro sentido. A principal diferença entre a criptografia e a esteganografia está em seus propósitos: enquanto a primeira tenta codificar o conteúdo, a segunda tenta camuflar a existência de uma mensagem dentro de outra.

Durante a análise dos dados contidos em um disco rígido, é fácil para o perito caracterizar a existência de informações criptografadas e, após isso, acaba tendo toda a sua atenção e esforço focados para decodificá-las, afinal os usuários não se preocupariam em proteger o conteúdo de arquivos irrelevantes. No caso da esteganografia, a mensagem pode estar escondida dentro de arquivos considerados comuns para o uso convencional do computador, como documentos, imagens, vídeos etc. Dessa forma, surge uma grande vantagem em relação à criptografia, pois, além de ser muito difícil identificar a presença de uma mensagem oculta, ela pode ser amplamente transmitida sem levantar suspeitas.

Essa técnica de camuflar informações também tem sido muito utilizada por empresas para proteger arquivos próprios que possuem direitos autorais, de modo que, quando reveladas, elas podem provar e demonstrar que a propriedade intelectual de determinado arquivo lhe pertence. Este tipo de aplicação é conhecido como marca d’água digital (*watermarking*). Além disso, também números seriais podem ser inseridos em mídias de fácil reprodução no meio digital, como vídeos e músicas. Assim, caso uma mesma cópia seja distribuída de forma

indiscriminada e ilegalmente, é possível identificar a origem do vazamento. Este tipo de técnica é comumente conhecido como impressão digital (*fingerprinting*). Outra prática de esteganografia na área comercial é feita pelas empresas HP e Xerox. As suas impressoras adicionam minúsculos pontos amarelos em cada página, os quais possuem codificados os números de série do equipamento, bem como a data e a hora da impressão.

Existem atualmente várias outras técnicas de esteganografia, desde mais simples a muito mais complexas do que as apresentadas aqui, o que acaba dificultando o trabalho do perito. Caso ele não descubra o tipo utilizado para ocultar a mensagem, uma alternativa é verificar se há softwares específicos instalados no dispositivo examinado, pois, desse modo, pode ser possível determinar a técnica praticada, ou, até mesmo, usar o próprio software para descobrir o conteúdo do arquivo.

Capítulo 5 - Principais aspectos jurídicos presentes na Perícia Forense Computacional

Por todo este trabalho é possível encontrar diversos aspectos legais que estão relacionados com a Perícia Forense Computacional, desde a falta de leis para punição de alguns delitos cibernéticos, até aqueles que regulamentam a atuação do perito durante a investigação. Este capítulo tem o objetivo de reuní-los e debater sobre suas características, apresentando os eventuais avanços na legislação brasileira.

O trabalho do perito, independente da área, consiste em executar atividades técnico-científicas de nível superior de descobertas, de defesa, de recolhimento e de exame de vestígios em procedimentos pré-processuais e judiciários. De acordo com a lei nº 12.030, de 17 de setembro de 2009, os peritos oficiais de natureza criminal, ou seja, aqueles designados a investigar delitos, foram classificados em peritos criminais, que geralmente trabalham em locais de crime e nos Institutos de Criminalística, peritos médico-legistas que, juntamente com os peritos odontolegistas, atuam convencionalmente nos Institutos Médicos Legais (IML) e são responsáveis pelas análises das vísceras e demais vestígios coletados durantes os exames de corpo de delito. Essa mesma lei, em seu artigo 2o, rege que “No exercício da atividade de perícia oficial de natureza criminal, é assegurado autonomia técnica, científica e funcional, exigido concurso público, com formação acadêmica específica, para o provimento do cargo de perito oficial.” Ou seja, há uma contradição na lei no que tange ao exercício da função de perito, pois ele não necessita de conhecimentos em Direito, embora atue diretamente com delegados, promotores e juízes, isto é, cargos que exigem estudos profundos da legislação. Cientes dessa falha e do que isso pode acarretar, os órgãos organizadores de concursos públicos para peritos criminais incluem em seus exames diversas questões relacionadas às principais áreas do Direito. Mas, de um modo geral, podemos afirmar que o perito computacional é um profissional habilitado, com conhecimentos tanto em informática, quanto em direito, especialista em analisar vestígios digitais e em produzir provas técnicas que servirão de apoio para a decisão de um juiz.

O perito, por ser uma autoridade investigativa oficial, possui uma norma que rege todo o seu trabalho, indicando sua função, seu objetivo, os procedimentos que devem ser executados e os limites de sua conduta. Nesse caso, a norma em questão é o decreto-lei Nº 3.689 de 3 de outubro de 1941, mais conhecido como Código de Processo Penal ou simplesmente CPP, que, em seus 811 artigos, regulamenta a função do Estado na apuração das infrações penais, nos julgamentos e na aplicação de punições cabíveis. Esta lei estabelece, entre outras coisas, como

deve ser o inquérito policial, a ação penal, a busca e apreensão, a prova criminal, os exames e as perícias. É ele que determina, por exemplo, em seu artigo 158o que: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.”. Outro regimento importante é o determinado pelo artigo 170o: “Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.”. Ou seja, vai diretamente de encontro com a recomendação existente em todo o trabalho de não alterar os dados contidos no disco, preservar as evidências e garantir a cadeia de custódia, isto é, o perito deve assegurar a proteção e idoneidade da prova, a fim de evitar questionamentos quanto à sua origem ou estado inicial, pois qualquer suspeita pode anulá-la e colocar em risco toda a investigação policial.

O Código Penal Brasileiro, instituído pelo Decreto-Lei 2.848 de 07 de dezembro de 1940, é o conjunto de normas que o Estado emprega para prevenir ou reprimir os fatos que atentem contra a segurança e a ordem social. Ele é composto por duas partes: Parte Geral e Parte Especial. Na primeira, são descritos e explicitados os conceitos e compreensões gerais sobre a aplicação da lei penal, do crime, das medidas de segurança, entre outros. Já na Parte Especial é onde ocorre a tipificação dos crimes e o estabelecimento das penas relativas. É justamente nessa parte que existe uma brecha na legislação brasileira aproveitada pelos criminosos cibernéticos.

Conforme o inciso XXXIX do artigo 5o, "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Isto quer dizer que é necessário que o crime e a respectiva pena para eventual aplicação legal estejam exatamente e literalmente descritos no Código Penal. Um dos objetivos dessa tipificação dos crimes é evitar que haja prejuízo da incolumidade do cidadão e que ele viva sob ameaça e medo, porque não é sabedor daquilo que pode ou não fazer na sociedade em que encontra. Da mesma forma, ela restringe a atuação dos julgadores e autoridades responsáveis pela lei e a ordem social, no sentido de que não haja aplicação de pena para situações não descritas antecipadamente como inconvenientes e consideradas proibidas. Tudo isso para manter a estabilidade social e jurídica. Por conta disso, toda e qualquer alteração no Código Penal deve ser proposta através de projetos de lei, precisando ser aprovada na Câmara dos Deputados e no Senado Federal, além de ser sancionada pelo Presidente da República para poder entrar em vigor.

A demora existente desde a elaboração de um projeto de lei até a sua promulgação, passando por todos os trâmites legais, impede que se tenha uma legislação mais moderna e que atenda

as demandas atuais da sociedade. O Código Penal Brasileiro, por exemplo, foi instituído a mais de setenta anos, ainda sob a égide da Constituição Autocrática de 1937 e em plena II Guerra Mundial. Ao longo do tempo, com o surgimento de novas tecnologias e mudanças nas condutas comportamentais moralmente aceitas, houve sérias e importantes modificações sociais que requereram (e ainda requerem) ajustes ou legislações paralelas. Podemos citar como exemplo a Lei dos Crimes Hediondos, a Lei Maria da Penha que trata da violência doméstica, a Lei que proíbe a ingestão exagerada de bebidas alcoólicas por condutores de veículos, e tantas outras que também introduziram novos artigos e ou adequaram os existentes no Código Penal.

Na área de informática, os criminosos se aproveitam da falta de tipificação de algumas práticas lesivas para invadir computadores e aplicar golpes ou danificar sistemas. Um deles, julgado pelo Tribunal de Justiça de São Paulo, tratava de uma acusação de *phishing scam*, isto é, um vírus que rouba os dados pessoais digitados pelos usuários. O Ministério Público acusou o réu de interceptação de dados, com base na Lei 9.296/95, porque não há outra lei em que se possa basear a acusação. Como resultado, o desembargador relator absolveu o acusado, por entender que não se trata de interceptação de dados, o caso é de furto, mas não é possível enquadrá-lo dessa forma. Segundo Higor Vinícius Nogueira Jorge, delegado de polícia, professor da Academia de Polícia e especialista na investigação de crimes cibernéticos, cerca de 10% dos casos de transtornos provocados por meios virtuais não são punidos, porque não se enquadram ao previsto no Código Penal e também não têm legislação específica. Para evitar que essa situação continue, há alguns projetos de lei tramitando na Câmara de Deputados e no Senado Federal com o objetivo de tipificar algumas práticas cometidas na rede de computadores como crimes virtuais.

Um deles é o PL 84/1999, considerado o mais completo texto legislativo já produzido sobre crimes informáticos no país e consiste em um projeto substitutivo, apresentado pelo então Senador Eduardo Azeredo, que aglutinou três projetos de lei que já tramitavam no Congresso Nacional, e, segundo sua própria descrição, tem o propósito de tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares. Esse projeto, conhecido como “Lei Azeredo”, foi aprovado pela Câmara dos Deputados em 2003 e modificado pelo Senado em 2008. Em virtude dessas alterações, resta apenas que ele volte à Câmara para nova votação e seja sancionado pelo Presidente da República. Regimentalmente não é possível mais fazer mudanças no corpo do texto, ele só pode ser aprovado integralmente, ter algum de seus artigos vetado por inteiro ou

ser descartado de vez. Na prática, com a aprovação dessa legislação, as seguintes condutas passarão a ser consideradas crimes, todos de natureza dolosa:

- Acesso não autorizado a rede, dispositivo de comunicação ou sistema informatizado;
- Obtenção, transferência ou fornecimento não autorizado de dado público;
- Dano;
- Divulgação ou utilização indevida de dado pessoal;
- Inserção ou difusão de código malicioso;
- Inserção ou difusão de código malicioso seguido de dano;
- Estelionato eletrônico;
- Atentado contra a segurança de serviço de utilidade pública;
- Falsificação de dado eletrônico ou documento público;
- Falsificação de dado eletrônico ou documento particular;
- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado.

Além da tipificação de crimes, a Lei Azeredo regulamenta também que deve haver a guarda, por parte dos provedores e durante três anos, dos dados de acessos dos usuários (logs) e que sites de conteúdo colaborativo, como *Youtube*, *Orkut* e *Facebook*, possuem responsabilidades pelas informações inseridas e atos praticados dentro de sua rede.

Porém, esta lei é alvo de críticas de diversos setores da sociedade, onde inclusive ganhou o apelido de “AI-5 Digital”. Juristas e deputados dizem que ela define crimes já existentes, como dano e estelionato, que regulamenta o compartilhamento de arquivos (tarefa atribuída à reforma da lei de Direitos Autorais que está sendo revista pelo Ministério da Cultura) e que, de acordo com o parlamentar Paulo Teixeira, “grande parte dos tipos penais propostos apresenta redação significativamente aberta e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática - independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente - já corresponderia à consecução da atividade criminosa”. Outro deputado, Emiliano José diz que o projeto “tem um conteúdo antidemocrático, que atende aos interesses da área de direitos autorais dos EUA, além da Federação Brasileira de Bancos (Febraban) e dos grandes escritórios de advocacia. Além disso, o projeto tira o anonimato da rede, que é um direito da cidadania contemporânea.” Já os provedores são contra devido aos custos relativos à contratação e manutenção de pessoal para atender e processar os pedidos judiciais ou de autoridades para acesso aos dados de conexão, além das empresas de menor porte não possuírem infraestrutura necessária para o armazenamento dessas informações por tanto tempo. Grupos de ativistas, de direitos do

consumidor e relacionados à privacidade alegam que a aprovação da lei como está cria um ambiente de vigilantismo e significa um perigo para o anonimato e para a privacidade na internet. Eles consideram que havendo a guarda de logs, porém sem regulamentação de acesso e uso dessas informações (nenhum artigo da lei normatiza as condições de segurança para esse armazenamento), as empresas podem utilizar esses dados dos usuários para outros fins, além de acharem exagerado o tempo de 3 anos. Outros pontos do projeto também são motivos de controvérsias, como o que sugere que os provedores noticiem, de modo sigiloso, às autoridades casos de usuários que tenham conduta suspeita na rede, dando ao provedor o poder de polícia. De acordo com o texto proposto, as pessoas que praticam atividades cotidianas na internet, como, por exemplo, o compartilhamento de música, ou que possuam computadores infectados por um vírus e o espalharem, mesmo de forma não intencional, podem ser severamente punidas.

Diante de tantas polêmicas, o Ministério da Justiça fez uma consulta pública (tanto online quanto offline) durante o ano de 2010, da qual participaram advogados, acadêmicos e defensores dos direitos civis na internet, para definir as relações entre usuários, provedores e autoridades e servir como base de princípios para a legislação sobre questões eletrônicas. O resultado da consulta se tornou um projeto de lei civil, conhecido como o Marco Civil da Internet, que estabelece um conjunto claro de direitos e responsabilidade dos usuários, define fortes princípios de neutralidade da rede e protege os intermediários de serem responsabilizados criminalmente devido a conteúdos gerados pelos usuários.

O Marco Civil é tido como mais brando e com regras mais completas e proporcionais. Em relação à polêmica guarda dos registros de conexão, ele prevê que ela seja feita pelas empresas capazes de atribuir os endereços IPs, companhias conhecidas no jargão do setor como *Autonomous System* (AS), e pelo prazo de um ano, podendo ser estendido. Além disso, para obter o log é preciso uma ordem judicial. Havendo um crime naquele horário e a suspeita do usuário ter cometido essa violação, é necessária outra ordem judicial para a associação entre o número do IP e o dono do número. Na proposta do ex-senador Azeredo, os dados poderiam ser obtidos por uma simples requisição de autoridade, policial ou não. Outra divergência entre as duas leis é que o Marco Civil isenta claramente os provedores de responsabilidades por informações e atos de terceiro. O Marco Civil da Internet não surgiu para ser um contraponto ao projeto de lei 84/99, mas um complemento, tanto que diz expressamente que a tipificação dos crimes na web precisa ser regulamentada por outras leis. Os dois projetos poderiam funcionar juntos, mas há várias contradições entre eles, principalmente opiniões contrastantes sobre o que é a rede e o que deve ser preservado nela.

Grande parte dos direitos garantidos pelo Marco Civil pode inviabilizar excessos da legislação de crimes digitais.

Atualmente, vem sendo organizado por deputados envolvidos na redação do Marco Civil e que se opõem à visão de Azeredo um projeto de lei alternativo para enquadrar delitos virtuais ainda não existentes na legislação. Esse grupo espera apressar a aprovação do Marco Civil para só depois apresentar o seu contraponto mais ponderado, porém ainda incompleto e pouco desenvolvido. Esse projeto alternativo, oficialmente protocolado na Câmara em 29/11/2011, é mais enxuto por considerar que os outros crimes já estão em outras leis e que regulação demais pode travar a inovação, a criatividade e potencial democrático da internet, resumindo-se a tipificar apenas três crimes: 1) Invadir rede de computadores, dispositivo de comunicação ou sistema informatizado; 2) Utilizar, alterar ou destruir as informações obtidas ou causar dano ao sistema informatizado; e 3) Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores ou sistema informatizado sem a autorização de seu legítimo titular. Apesar de estar em estágio inicial, o projeto pode tramitar com rapidez e tem chance de ultrapassar a Lei Azeredo e entrar em vigor antes, dependendo do nível de consenso entre os parlamentares.

Embora a popularização dos computadores no Brasil tenha ocorrido há pouco mais de quinze anos, já foi suficiente para provocar grandes mudanças nos quadros sociais e comportamentais, exigindo das autoridades ações perante os novos desafios surgidos. Entre essas demandas, está a criação e alteração de leis para regulamentar o uso das novas tecnologias e evitar que haja supressão de direitos. Com a aprovação do Marco Civil, de um projeto de lei que tipifica os chamados “crimes de alta tecnologia” e a reforma da lei de direitos autorais, proposta pelo Ministério da Cultura, o Brasil pode ser o país com a legislação mais progressista de internet no mundo e tornar-se “líder em cultura digital”, de acordo com Lawrence Lessig, criador da licença *Creative Commons*, e maior autoridade em direitos autorais na era digital.

Conclusão

Desde o seu surgimento, a humanidade, utilizando-se de sua capacidade única de raciocínio, criou procedimentos, métodos, mecanismos e ferramentas para auxiliá-la na execução de atividades, sejam elas caçar, trabalhar ou se divertir. Surgido em 1946, com 30 toneladas, ocupando uma área de 180m2 e com o intuito de realizar cálculos balísticos, o computador, juntamente com a internet, revolucionou o nosso modo de se comunicar, adquirir e transmitir informações, criando a chamada “Era Digital” ou “Era da Informação”. Ao longo do tempo, seus componentes e arquitetura foram incorporados por outros dispositivos, como celulares, TVs, aparelhos hospitalares etc, permitindo a eles novas funcionalidades e melhor desempenho. Atualmente, a facilidade e a velocidade com que o computador processa, armazena e transmite dados por toda a sua rede, tornou-o um bem de consumo muito desejado – e por diversas vezes indispensável – em muitas empresas e casas de todo o mundo. Estima-se que no mundo existam 2,5 bilhões de computadores em uso, sendo 85 milhões só no Brasil, e a tendência é que essa expansão continue nos próximos anos.

Governos e empresas, ao notarem esse progresso, passaram a oferecer diversos serviços aos seus cidadãos e clientes, como emissão de documentos, transações bancárias, vendas de produtos, entre outros, gerando assim uma enorme quantidade de dados sigilosos. Porém, esse grande volume de informações pessoais circulando pelas redes do mundo inteiro atraiu criminosos, que começaram a se especializar e até recrutar pessoas com conhecimentos na área de computação para a realização de novas práticas ilegais. Como em qualquer área, a prevenção é, sem dúvida, a melhor maneira para combater tais ataques. Deve-se, não só dispor de equipamentos e sistemas de alta tecnologia, como também instruir as pessoas a os utilizar com segurança. Entretanto, quando ela se torna ineficaz ou inexistente e ocorre um ataque, é necessário que haja uma investigação para apuração e análise dos vestígios deixados e, desse modo, esclarecer o que aconteceu, como e quem praticou tais atos ilícitos. A Perícia Forense Computacional é a área que envolve a análise e coleta de vestígios e evidências digitais em equipamentos computacionais envolvidos em procedimentos ilícitos e crimes de qualquer natureza. Dentro dessa visão, este trabalho de graduação apresentou os principais conceitos sobre o assunto, descreveu como deve ser a atuação do perito durante a investigação, detalhou os principais tipos de exames forenses, incluindo os principais

procedimentos que podem ser realizados, e discutiu os principais aspectos jurídicos e legais relacionados com crimes cibernéticos e presentes na Perícia Forense Computacional.

Os dispositivos de armazenamento computacional, principalmente os discos rígidos, têm aumentado de tamanho, e as técnicas forenses devem ser cada vez mais apuradas, a fim de realizar uma investigação com maior qualidade. Inúmeros são os crimes cometidos com o uso de equipamentos computacionais. Assim, a Perícia Forense Computacional deve estar preparada para identificar e apontar as possíveis evidências digitais deixadas na cena do crime, transpondo desafios e relatando a materialidade, a dinâmica e a autoria dos delitos.

Porém, é necessário que a legislação brasileira também se aprimore cada vez mais, pois não há, entre nossas leis, itens que possam coibir ou mesmo punir alguns delitos praticados por hackers, como a disseminação de vírus. A aprovação de leis que tipifiquem crimes cibernéticos é urgente, não só para dinamizar os processos como para reduzir a sensação de impunidade de criminosos em questões que se mostram dúbias e não terminam em condenação. O projeto 84/1999, conhecido como Lei Azeredo, veio para cobrir essa lacuna, porém trouxe tipos de pena abrangentes, causando insegurança jurídica e desestímulo à inovação.

Tecnicamente, é possível criar o crime baseado nas noções de direitos e deveres do cidadão garantidas pela Constituição, porém, faz pouco sentido definir crimes antes de garantir direitos e deveres do cidadão no ambiente online. Surge então o Marco Civil da Internet, um importante projeto de lei, elaborado após diversas consultas à sociedade, que busca estabelecer regras, direitos, deveres e princípios para o uso da rede de computadores. Ele traz um equilíbrio entre o direito à liberdade de expressão e os interesses relacionados a privacidade e segurança. O Marco Civil não é um contraponto à propostas de enquadramento dos crimes na internet, pelo contrário, ele diz explicitamente que a tipificação precisa ser regulamentada por outras leis.

Na última década, essa abordagem pioneira criada pelo Brasil para políticas digitais foi encarada por muitos países ao redor do mundo como um modelo para promover a inovação e a abertura online. O único entrave é a demora por parte do poder legislativo e executivo para apresentar, deliberar e aprovar tais políticas.

Referências Bibliográficas

FARMER, Dan / VENEMA, Wietse. **Perícia Forense Computacional**. 1ª ed. São Paulo: Pearson Prentice Hall, 2007.

ELEUTÉRIO, Pedro Monteiro da Silva / MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. 1ª ed. São Paulo: Novatec, 2011.

SANTOS, Moacyr Amaral. **Primeiras linhas de direito processual civil**. São Paulo: Saraiva, 2004.

CARROLL, Ovie L.; BRANNON, Stephen K.; SONG, Thomas. **Computer Forensics: Digital Forensic Analysis Methodology. United States Attorneys ' Bulletin**. Volume 56, Número 1, 2008.

DAOUN, Alexandre Jean; GISELE, Truzzi De Lima. **Crimes informáticos o direito penal na era da informação**. ICoFCS 2007 – Proceedings of The Second International Conference Of Forensic Computer Science Volume 2, Número 1. 2007.

FREITAS, Andrey. **Perícia Forense Aplicada à Informática**. Trabalho de Curso de Pós-Graduação "Lato Sensu"em Internet Security. IBPI. 2003.

NOBLETT, Michael G. **Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence.** Proceedings of the 11th INTERPOL Forensic Sciense Symposium. 1995.

PEREIRA, Evandro; FAGUNDES, Leonardo. **Forense Computacional: fundamentos, tecnologias e desafios atuais**. Simpósio Brasileiro em Segurança da Informação e de Sistemas computacional. Rio de janeiro: 2007.

VARGAS, R. G. Processos **e Padrões em Perícia Forense Aplicado a Informática**.

REIS, Marcelo Abdala dos; GEUS, Paulo Lício. **Forense Computacional: Procedimentos e Padrões**. Instituto de Computação da Universidade Estadual de Campinas. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-marcelo.reis-forense.padroes.pdf> Acesso em: 28 mai. 2008

GADELHA, Julia. **A evolução dos computadores**. Disponível em: <http://www.ic.uff.br/~aconci/evolucao.html> Acesso em: 23 abr. 2011.

Evolução dos computadores. Disponível em: <http://www.idealdicas.com/evolucao-dos-computadores/> Acesso em: 23 abr. 2011.

MEIRELLES, Fernando S. **22ª Pesquisa Anual do Uso de TI, 2011**. Disponível em: <http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/GVpesqTI2011PPT.pdf> Acesso em: 26 abr. 2011.

CRUZ, Elaine Patricia. **Pesquisa mostra que Brasil tem 85 milhões de computadores em uso**. Disponível em: <http://agenciabrasil.ebc.com.br/noticia/2011-04-19/pesquisa-mostra-que-brasil-tem-85-milhoes-de-computadores-em-uso> Acesso em: 26 abr. 2011.

BRASIL. Decreto-Lei Nº 3.689, de 3 de outubro de 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm> Acesso em: 26 abr. 2011.

Wikipedia. **Data remanence**. Disponível em: <http://en.wikipedia.org/wiki/Data_remanence> Acesso em: 08 nov. 2011.

Aker Security Solutions. **Como efetuar exclusão segura dos dados do disco (Wipe)?**. Disponível em: <http://www.aker.com.br/108/10802002.asp?ttCD_CHAVE=457> Acesso em: 08 nov. 2011.

National Institute of Standards and Technology. **Guidelines for Media Sanitization**. Gaithersburg, 2006. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf> Acesso em: 08 nov. 2011.

National Software Reference Library. **Introduction to the NSRL**. Disponível em: <http://www.nsrl.nist.gov/> Acesso em: 08 nov. 2011.

Microsoft. **NTFS Technical Reference**. Disponível em: <http://technet.microsoft.com/en-us/library/cc758691(WS.10).aspx/> Acesso em: 08 nov. 2011.

HUDSON, Andrew. **NTFS: A File System with Integrity and Complexity**. Disponível em: <http://www.osnews.com/story/24076/NTFS_A_File_System_with_Integrity_and_Complexity> Acesso em: 08 nov. 2011.

Wikipedia. **Rainbow table**. Disponível em: <http://en.wikipedia.org/wiki/Rainbow_table> Acesso em: 08 nov. 2011.

ATWOOD, Jeff. **Rainbow Hash Cracking**. Disponível em: <http://www.codinghorror.com/blog/2007/09/rainbow-hash-cracking.html> Acesso em: 08 nov. 2011.

CALÔR FILHO, Marcos Muniz. **Kerberos - Autenticação em Sistemas Distribuídos**. Disponível em: <http://www.gta.ufrj.br/grad/99_2/marcos/criptografia.htm> Acesso em: 08 nov. 2011.

CASTELLÓ, Thiago; Vaz, Verônica. **Assinatura Digital**. Disponível em: <http://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html> Acesso em: 08 nov. 2011.

FONSECA, Thiago. **Esteganografia**. Disponível em: <http://www.gta.ufrj.br/grad/07_2/thiago_castello/AplicaesdaEsteganografia.html> Acesso em: 08 nov. 2011.

CHIRIGATI, Fernando; KIKUCHI, Rafael; GOMES, Talita. **Esteganografia**. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/tecnicas.html> Acesso em: 08 nov. 2011.

FERRO, Hugo; SANTOS, Nathália. **Perícia Forense Computacional: a importância do perito ao se analisar um cenário**. Disponível em: <http://www.viajus.com.br/viajus.php?pagina=artigos&id=3980> Acesso em: 08 nov. 2011.

TOMÁS, Eliane. **Crimes Informáticos: Legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime**. Disponível em: <http://www.artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html> Acesso em: 08 nov. 2011.

REINO, Alfredo. **Informática Forense**. Disponível em: <http://doc.jurispro.net/articles.php?lng=pt&pg=9717> Acesso em: 08 nov. 2011.

O Brasil contra o Cibercrime. Disponível em: <https://www.safernet.org.br/site/sites/default/files/resumo-da-apresentacao_PLS-Azeredo_Valor-16-10-2006.pdf> Acesso em: 08 nov. 2011.

SILVA, Vandeler. **Código Penal Brasileiro**. Disponível em: <http://www.infoescola.com/direito/codigo-penal-brasileiro/> Acesso em: 08 nov. 2011.

BRASIL. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm> Acesso em: 08 nov. 2011.

BRASIL. Lei Nº 12.030, de 17 de setembro de 2009. Dispõe sobre as perícias oficiais e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12030.htm> Acesso em: 08 nov. 2011.

Lei de crimes virtuais deve agilizar processos e reduzir impunidade. Gazeta de Limeira. Disponível em: <http://www.gazetadelimeira.com.br/Noticia.asp?ID=50081> Acesso em: 08 nov. 2011.

Agência Câmara. **Falta de lei sobre crimes digitais leva à impunidade, diz especialista**. Disponível em: <http://tecnologia.uol.com.br/seguranca/ultimas-noticias/2010/12/29/falta-de-lei-sobre-crimes-virtuais-leva-a-impunidade-diz-especialista.jhtm> Acesso em: 08 nov. 2011.

NUNES, Emily; CARDOSO, Ismael. **Comissão da Câmara retira da pauta PL sobre crimes na internet**. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI5462517-EI12884,00-Comissao+da+Camara+retira+da+pauta+PL+sobre+crimes+na+internet.html> Acesso em: 08 nov. 2011.

BIDDLE, Ellery. **Brazil: Cybercrime Law Could Restrict Fundamental Rights, Internet Openness**. Disponível em: <http://advocacy.globalvoicesonline.org/2011/11/08/brazil-cybercrime-law-could-restrict-fundamental-rights-internet-openness/> Acesso em: 08 nov. 2011.

POSSETI, Helton. **PL 84/99, do senador Azeredo, deve ser superado pelo Marco Civil da Internet**. Disponível em: <http://www.teletime.com.br/24/08/2011/pl-84-99-do-senador-azeredo-deve-ser-superado-pelo-marco-civil-da-internet/tt/237850/news.aspx> Acesso em: 08 nov. 2011.

CARDOSO, Ismael. **Lei Azeredo é "imprecisa", diz autor de projeto alternativo**. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI5310037-EI12884,00-Lei+Azeredo+e+imprecisa+diz+autor+de+projeto+alternativo.html> Acesso em: 08 nov. 2011.

Terra. **Lei de cibercrimes causa polêmica em seminário na Câmara**. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI5311374-EI12884,00-Lei+de+cibercrimes+causa+polemica+em+seminario+na+Camara.html> Acesso em: 08 nov. 2011.

CABRAL, Rafael. **Três projetos e duas leis**. Disponível em: <http://blogs.estadao.com.br/link/tres-projetos-para-duas-leis/> Acesso em: 08 nov. 2011.

CABRAL, Rafael. **Marco Civil da Internet versus Lei Azeredo**. Disponível em: <http://blogs.estadao.com.br/link/marco-civil-versus-lei-azeredo/> Acesso em: 08 nov. 2011.

GROSSMANN, Luís. **Sem acordo ou apoio, Câmara "congela" projeto de crimes cibernéticos**. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28521&sid=18> Acesso em: 08 nov. 2011.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=3186> Acesso em: 24 jun. 2008.