Capítulo 0

Introdução à Computação Forense

Deivison Pinheiro Franco – Gustavo Pinto Vilar
Luiz Eduardo Marinho Gusmão – Luiz Rodrigo Grochocki

A Computação Forense é a vertente das Ciências Forenses que objetiva a análise do vestígio cibernético. A fim de que possamos compreender melhor os conceitos, princípios e desenvolvimento de ideias que serão apresentados no decorrer deste livro, faz-se mister nivelarmos alguns conhecimentos intrínsecos à Computação Forense.

A Computação Forense

A Computação Forense é a ramificação da Criminalística que tem como objetivo a análise de vestígios cibernéticos, englobando os elementos que os orbitam. Esse aspecto a torna uma área multidisciplinar, que abrange diferentes áreas das Ciências Forenses. Isso pode ser visto diariamente nos Institutos de Criminalística, onde os peritos de informática interagem com os peritos de áreas como contabilidade e audiovisual.

Essa cooperação acompanha o próprio movimento de migração do analógico para o digital visto na sociedade moderna. Até pouco tempo atrás, os peritos daquelas áreas analisavam livros-caixa e fitas VHS. Atualmente, examinam relatórios eletrônicos extraídos a partir de sistemas contábeis e vídeos codificados no formato H.264. A própria documentoscopia, que tradicionalmente lidava apenas com documentos em papel, hoje já trata de arquivos assinados com certificados digitais e montagens feitas eletronicamente.

Indo além, a evolução tecnológica faz com que a Computação Forense permeie áreas nunca antes imagináveis como: a balística, ao tratar da fabricação caseira de armas de fogo por meio de impressoras 3D; a medicina, em função da análise de dispositivos médicos, como marca passos; e a perícia em acidentes de trânsito, que pode contar com o auxílio da eletrônica embarcada.

Outro aspecto envolve a atualização tecnológica, uma vez que os computadores estão cada vez mais presentes no nosso dia a dia, seja por meio de um simples relógio de pulso, que hoje tem mais poder de processamento do que o computador que auxiliou o pouso do homem na lua, ou seja através do conceito de "Internet das Coisas" (*Internet of Things* – IoT), que está revolucionando a forma com que interagimos com os objetos ao nosso redor.

Esse fenômeno de capilaridade tecnológica é chamado de computação ubíqua ou pervasiva, que representa a evolução da área, que passou dos grandes computadores que ocupavam inteiras para os dispositivos portáteis, tão comuns atualmente.

Finalmente, é importante frisar que, apesar da tecnologia estar presente no ambiente forense, os profissionais não devem se lançar cegamente em sua direção. Ao contrário, precisam se dedicar a estudá-la para tomar consciência de sua amplitude e potencialidade. "É difícil dizer o que é impossível, pois a fantasia de ontem é a esperança de hoje e a realidade de amanhã" - é com esse pensamento de Goddard[1], que oferecemos aos leitores o raciocínio que justificou a construção da presente obra.

A complexidade e a evolução da computação

Segundo a 27ª pesquisa anual do uso de TI 2016[2] realizada pelo Centro de Tecnologia de Informação Aplicada da FGV-EAESP existem no Brasil cerca de 244 milhões de dispositivos conectáveis à internet, ou seja, mais de um dispositivo por habitante.

1 Robert Hutchings Goddard foi um físico experimental estadunidense que viveu entre 1882 e 1945, cujo trabalho e pesquisa foram diretamente dedicados e responsáveis pelas viagens espaciais. Também engenheiro aeroespacial, Goddard foi considerado o pai dos foguetes modernos, tendo sido responsável pela construção do primeiro foguete de combustível líquido que existiu.

2 Disponível em: http://bit.ly/pesquisaanual - Acesso em 25 de julho de 2016.

A "Internet das Coisas", segundo previsões, atribuirá endereços lógicos a todos os dispositivos do planeta, criando uma grande rede na qual tudo estará conectado, desde eletrodomésticos até veículos automotores, abrindo espaço para os temas a serem discutidos na presente obra e que beiram os limites da ficção científica. A reboque dessas revoluções tecnológicas, surgem novas práticas ilícitas e antiéticas que dependem de análises especializadas dos profissionais de Computação Forense.

O cenário atual aponta que cerca de 77 mil brasileiros sofrem ataques cibernéticos por dia[3] e, provavelmente por falta de educação tecnológica ou conhecimentos de Computação Forense, apenas 21% deles denunciam o ataque.

São cerca de 2.100 ataques/hora a sistemas governamentais[4], fato que foi alvo de pauta do Fórum Econômico Mundial, no qual seus líderes colocaram os ataques cibernéticos, a incidência massiva de fraude, o roubo de dados e a desinformação digital entre os 10 maiores riscos às Nações.

Chamam a atenção as cifras referentes aos custos dos crimes cibernéticos (Figura 1). De acordo com o relatório da Allianz Global Corporate & Specialty[5], foram 7,7 bilhões de dólares só no Brasil, ou seja, se trata de campo promissor para os profissionais atuantes na prevenção, reposta a incidentes e remediação dos crimes cibernéticos.

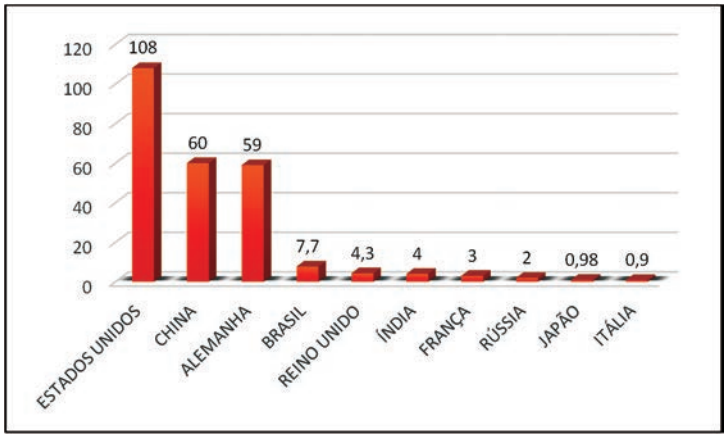

Figura 1 – Custo do crime cibernético no mundo, em bilhões de dólares.

PARA SABER MAIS

Reportagem mostra a importância da Computação Forense em grandes operações policiais, como a "Lava Jato".

Fonte: http://bit.ly/lavajatoglobo - Acesso em 01 de junho de 2016.

Os avanços tecnológicos ampliaram significativamente as possibilidades de comércio, comunicação e relacionamento interpessoal, porém, a formação de profissionais e a educação tecnológica não acompanhou o ritmo desse vertiginoso crescimento.

3 Disponível em: http://bit.ly/relatoriosymantec - Acesso em 25 de abril de 2016.

4 Disponível em: http://bit.ly/freqataques - Acesso em 25 de abril de 2016.

5 Disponível em: http://bit.ly/boletimrisco - Acesso em 13 de maio de 2016.

O trabalho da Perícia Forense Computacional demanda, além de profissionais capacitados e investimentos em soluções de TI, tempo para execução dos respectivos exames. Dessa forma, os profissionais que atuam em Computação Forense terão que lidar com a variação das complexidades dos exames periciais. Nesse contexto, alguns fatores se mostram preponderantes:

Fator humano: Se relaciona à capacidade humana de compreensão e tratamento da informação, dos vestígios e suas análises em nível de raciocínio, deduções e conclusões. O fator humano é afetado por diversas variáveis como estado emocional, cansaço, sono, calor e outros;

Fator tecnológico: Diz respeito às facilidades e dificuldades impostas pela tecnologia, principalmente no tocante à velocidade de processamento da informação (tempo) como também na limitação de tamanho das mídias de armazenamento atuais (espaço);

Fator legal: Se conecta aos parâmetros impostos pela legislação no tratamento do vestígio cibernético, já que a análise desse deve obedecer, além dos princípios científicos, os ditames de ordem legal e processual.

Mesmo diante da evolução do processamento e armazenamento de informações, previstas pelas Leis de Moore[6], em que o número de transistores colocados em um circuito integrado dobraria a cada dois anos[7], e Kryder[8], em que a densidade e a capacidade de armazenamento dos discos rígidos dobrariam de tamanho entre 18 e 24 meses, o ser humano pode não ser capaz de processar as informações e produzir resultados em tempo hábil de forma a atender à legislação pertinente.

CURIOSIDADE

Sunway TaihuLight é o supercomputador mais poderoso do planeta, com 10.649.600 (dez milhões, novecentos e quarenta e nove mil e seiscentos) núcleos de processamento, pode realizar 93 quadrilhões de cálculos por segundo. Possui ainda 1.31 petabytes de memória primária.

A SAMSUNG lançou o maior disco rígido do mundo: Um SSD de aproximadamente 16 TB.

Fonte: http://bit.ly/computadorveloz - Acesso em 26 de julho de 2016.

Fonte: http://bit.ly/discogrande - Acesso em 26 de julho de 2016.

Terminologia e conceitos básicos da Computação Forense

Alguns termos foram adotados e padronizados na Computação Forense a fim de consolidar a terminologia pericial, assim sendo, alguns conceitos e terminologias relevantes para a leitura deste livro serão apresentados a seguir:

- **Algoritmo de *hash* criptográfico (função de *hash* criptográfico):** função matemática cujo resultado é um valor de tamanho fixo, gerado a partir de uma entrada de tamanho arbitrário. Na Computação Forense, os arquivos geralmen-

6 Gordon Earle Moore, químico e PhD em química e física, co-fundador da empresa Intel.

7 Em 2011 a lei de Moore foi atualizada, pois o número de transistores passou a dobrar a cada 18 meses.

8 Mark Kryder, engenheiro elétrico, Ph.D. em Engenharia Elétrica e Física, foi vice-presidente sênior da empresa de fabricação de discos rígidos SEAGATE.

te são utilizados como parâmetros de entrada dessas funções, o que permite identificar se dois ou mais arquivos possuem conteúdos idênticos. Outra característica importante das funções *hash* é a unidirecionalidade, ou seja, a partir de seu resultado é impraticável produzir o parâmetro de entrada. Muito usados no controle de integridade de arquivos e mídias de armazenamento, haja vista a baixíssima probabilidade de dois arquivos distintos submetidos à mesma função produzirem o mesmo resultado;

- **Análise *live* (análise a quente, análise *online*, análise viva ou *live analysis*):** tipo de análise realizada diretamente no equipamento questionado com o sistema operacional em funcionamento. É destinada à análise do dispositivo e dos dados em tempo de execução. Tal análise, apesar de aumentar a superfície de exposição da evidência e alterá-la de forma involuntária, pode ser a única forma de identificar e salvaguardar a evidência de natureza volátil. Deve ser aplicada de acordo com as técnicas recomendadas para o tipo específico de equipamento e evidência, sendo que os procedimentos realizados durante o exame devem ser documentados;
- **Análise *post-mortem* (análise a frio, análise *offline*, análise morta ou *dead analysis*):** tipo de exame realizado quando se deseja aumentar o grau de preservação da evidência questionada. Nesse tipo de exame, opta-se por criar uma imagem forense (cópia exata) da evidência, protegendo-a contra gravações involuntárias. Esse tipo de perícia é o mais recomendado quando não há necessidade de preservação dos dados voláteis presentes em um determinado equipamento no momento de sua arrecadação ou quando a presença de criptografia nas mídias secundárias não for detectada;
- **Análise Forense Computacional:** tipo de análise realizada em dispositivos computacionais, tanto em *software* quanto em *hardware,* com foco na análise de evidências cibernéticas, a fim de trazer à tona elementos indicativos de autoria, materialidade e dinâmica de fatos, geralmente relacionados a violações legais;
- **Antiforense:** recurso usado para encobrir a existência, quantidade e a qualidade de evidências de determinado recurso computacional. Também pode objetivar dificultar a análise das evidências ou torná-la impraticável;
- **Arquivo Composto (ou Arquivo Container):** arquivo binário cujo conteúdo é formado por outros arquivos, como os arquivos compactados e os utilizados pelas suítes Libre Office e Microsoft Office;
- **Arquivo Imagem (Imagem Pericial ou Imagem Forense):** arquivo que contém a cópia exata da mídia submetida a exame. Dependendo das opções escolhidas pelo perito durante o processo de cópia, o arquivo pode ser fragmentado em arquivos menores ou pode ser compactado. Sua integridade é garantida pelas funções de *hash*;
- **Cadeia de Custódia:** registro detalhado de todos os passos, pessoas, ambientes, mídias e informações direta ou indiretamente relacionadas à perícia. É fundamental para instrumentar o processo e dar suporte a investigações ou contestações posteriores, sem que todo o processo pericial seja comprometido. Esse assunto teve suas diretrizes e procedimentos estabelecidos na portaria número 82, de 16 de julho de 2014 da Secretaria Nacional de Segurança Pública do Ministério da Justiça - SENASP/MJ;
- **Computação na nuvem:** termo utilizado para caracterizar os serviços de internet que oferecem recursos computacionais, como processamento e arma-

zenamento, situados em servidores cuja localização geográfica é transparente para o cliente;

- **Criptografia:** estudo e aplicação de métodos que transformam a informação plana e aberta em um conjunto de dados ininteligíveis às partes não autorizadas. Tem como principal objetivo permitir a troca de mensagens sigilosas em um ambiente inseguro;
- ***Deep Web*:** é o termo dado à parte da internet cujo conteúdo não está indexado pelos serviços de busca mais populares, como o Google. O acesso, geralmente, é feito por meio navegação anônima. Está repleta de páginas com conteúdo de caráter clandestino, como pornografia infantil e comércio ilegal de drogas;
- **Duplicação Pericial (Duplicação Forense):** é o processo de aquisição de uma evidência cibernética, na qual é realizada a cópia bit a bit de determinada informação, resultando na criação de um arquivo imagem ou de uma mídia duplicada;
- **Imagem Digital:** arquivo criado ou editado por meio eletrônico, geralmente máquinas fotográficas digitais ou *softwares* como o Adobe Photoshop;
- **Intrusão:** atividade de caráter voluntário, que leva à violação das políticas de segurança da informação de uma organização, podendo ter origem local ou remota;
- **Laudo (Parecer Técnico):** documento técnico científico de caráter formal, elaborado pelo perito. Apresenta o resultado da análise pericial de modo compreensível aos interessados e responsáveis pelo julgamento do mérito, dispensando-os da necessidade de conhecimento técnico aprofundado e reduzindo o risco de interpretação equivocada por parte dos mesmos. Para alcançar esse objetivo, o documento pode ser enriquecido com ilustrações, fotografias e croquis, visando a facilitação de seu entendimento;
- ***Malware*:** programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador;
- **Mídia Questionada (Mídia de Prova):** é a mídia objeto da investigação. Os tipos mais comuns são *pendrives*, discos rígidos externos ou inseridos em computadores, bem como as mídias ópticas;
- **Mídia de Destino:** suporte para o qual o conteúdo das mídias questionadas é copiado, de modo a preservá-las contra alterações não intencionais;
- **Vestígio Cibernético (Vestígio Digital):** qualquer informação de valor probatório que tenha sido armazenada ou transmitida em meio digital e que pode ser utilizada para comprovação de um crime. Na Computação Forense, um computador pode ser o meio ou o alvo de uma atividade criminosa, cabendo ao analista pericial a coleta de vestígios que possam levar à autoria dos delitos cometidos;
- ***Wipe*:** técnica empregada para apagamento seguro de mídias. Usada principalmente para reutilização de mídias de apoio aos exames periciais, evitando que informações anteriormente existentes contaminem uma nova análise pericial.

PARA SABER MAIS

Alguns desses conceitos e outros termos podem ser encontrados na RFC 2828 (*Internet Security Glossary*) – http://bit.ly/rfc2828 - Acesso em 01 de junho de 2016.

Normas técnicas e procedimentos em Computação Forense

No Brasil, a legislação não é taxativa quanto ao uso de normas, regimentos ou procedimentos específicos, bem como não exige titulação ou certificação do profissional que atua na área de Computação Forense. Aliás, cumpre ressaltar, que os profissionais da área de informática sequer têm conselho profissional, a exemplo dos conselhos de engenharia ou medicina.

Porém, o Código de Processo Penal (CPP) exige que o perito oficial ou nomeado tenha curso superior e faça uso de métodos aceitos pela comunidade científica. Em especial nos órgãos de perícia oficial, o perito, além de ter que ser aprovado em concurso público, deve atender a exigências como ter formação superior específica e participar de curso de formação oficial. O profissional deve seguir regras impostas através de Instruções Normativas, Procedimentos Operacionais Padrão, Manuais e certificações profissionais e de laboratórios. Já nas perícias *ad hoc*, são considerados o notório saber, a titulação, as certificações e a reputação do profissional.

Em Computação Forense segue-se a teoria da hierarquia das normas, na qual a está legislação constitucional está no topo da pirâmide e na base estão os documentos infraconstitucionais. Neste capítulo serão abordados os documentos mais usados como o Procedimento Operacional Padrão SENASP/MJ, a ISO/IEC 27037/2013 e ISO/IEC 27000. Bem como, as certificações mais populares na área.

Normas técnicas

Quando se trata de qualquer tipo de regramento ou ordenamento deve-se ter em mente a balança da Justiça, ou seja, sempre deve haver uma forma de pesar qual regramento deve ser aplicado no caso concreto. Na Computação Forense não é diferente, pois o profissional se depara com uma infinidade de normas oficiais, normas técnicas e procedimentos operacionais, sejam eles nacionais ou internacionais, sendo que, em um dado momento, deve escolher qual tem melhor aplicação.

No âmbito público, as normas só se tornam impositivas quando regulamentadas, porém, o perito sempre tem a autonomia técnico-científica. O exemplo mais claro disso é a não obrigatoriedade do perito seguir rigorosamente normas técnicas, a exemplo da ISO/IEC 27037/2013, senão por regulamento do órgão de perícia oficial.

Importante ressaltar que Regulamento Técnico é um documento normativo, de uso obrigatório, que dispõe sobre processos, métodos periciais e requisitos técnicos, incluindo as disposições administrativas cabíveis. Poderá ainda, normatizar o uso de terminologia, estrutura de laudos, etc. Sendo assim, os Regulamentos Técnicos são emitidos por autoridades competentes a nível federal, estadual e municipal, bem como podem ser emitidos em âmbito privado. Tendo no âmbito público especial função de regulamentar a utilização de normas e procedimentos.

Entre os documentos que tratam das perícias de informática, alguns como Regulamentos Técnicos, Procedimento Operacional Padrão e Normas Técnicas merecem desataque, pois são documentos oriundos do consenso e aprovados por uma instituição re-

conhecida, que fornece regras, diretrizes ou características para produtos ou processos e métodos de produção conexos, cujo cumprimento e adoção são voluntários[9].

O consenso deriva de grupos de trabalho que têm a participação de especialistas e são abertos a comunidade interessada, sintetizando os conhecimentos de ciência, tecnologia e prática, em uma norma. Diferente do Regulamento Técnico, a norma tem aplicação voluntária, ou seja, a Norma Técnica só é obrigatória quando referendada por um ato jurídico.

No âmbito da Computação Forense, as normas podem ser divididas de acordo com sua abrangência a nível de associações: nacionais, regionais e internacionais.

Essas normas são editadas e emitidas por associações, como a Associação Brasileira de Criminalística, a Sociedade Brasileira de Ciências Forenses, a *International Society of Forensic Computer Examiners*, etc.

No nível nacional as normas são editadas e emitidas pelo organismo nacional de normalização, que deve ter legitimidade para editar e publicar normas e, ainda, reconhecimento e consenso das instituições e da comunidade cientifica. No Brasil, podemos citar a Associação Brasileira de Normas Técnicas (ABNT), que foi responsável pela tradução da norma ISO/IEC 27037/2012.

PARA SABER MAIS

A NBR ISO/IEC 27037:2013 é a tradução e revisão da norma ISO/IEC 27037:2012 que traz as diretrizes para identificação, coleta, aquisição e preservação de evidência digital.

No nível regional, as normas são editadas e emitidas por entidades como a AMN-Mercosul, COPANT e CEN, que incluem um conjunto de países próximos ou uma região.

Finalmente, no nível internacional, as normas são editadas e emitidas por organismos internacionais como a ITU, ISO e IEC, que têm abrangência mundial.

Procedimento Operacional Padrão (POP) ou Norma Operacional Padrão (NOP)

O principal objetivo do POP é padronizar e minimizar os riscos na execução de tarefas relativas a Computação Forense. Ou seja, um POP bem feito e atualizado é instrumento fundamental da qualidade e eficiência da perícia.

UM POUCO DE HISTÓRIA

Os Procedimentos Operacionais Padrão ganharam maior popularidade com a revolução industrial e a automatização dos processos industriais. O exemplo mais clássico da padronização pode ser encontrado na indústria automobilística, a exemplo da linha de produção do Ford T.

Em Computação Forense, o POP aumenta a previsibilidade dos resultados esperados e minimiza os riscos, inclusive aqueles decorrentes de imperícia e negligência.

9 Disponível em: http://bit.ly/inmetrobr - Acesso em 04 de junho de 2016.

Também permite selecionar e fazer uso adequado das ferramentas forenses e demais recursos tecnológicos.

No Brasil, o ato normativo que tem maior amplitude é a obra denominada "Procedimento Operacional Padrão: Perícia Criminal", publicada pelo Ministério da Justiça, através da Secretaria Nacional de Segurança Pública. Esse documento traz uma padronização mínima para as perícias criminais em todo território nacional e lança luz sobre a área de computação em quatro POPs:

- **Exame Pericial de Mídia de Armazenamento Computacional:** tem a finalidade de orientar o profissional de perícia da área de computação a realizar exames que envolvam dados contidos em mídias de armazenamento computacional, como os discos rígidos, *pendrives* e cartões de memória;
- **Exame Pericial de Equipamento Computacional Portátil e de Telefonia Móvel:** serve como um guia para o perito realizar exames que envolvam computadores portáteis e telefones móveis como, por exemplo, celulares e *tablets*;
- **Exame Pericial de Local de Informática:** apresenta orientações ao profissional que realizará exames que envolvam locais de informática ou que demandem a análise do vestígio cibernético *in loco*;
- **Exame Pericial de Local de Internet:** tem a finalidade de orientar o perito de informática a investigar crimes ocorrido ou auxiliados pela internet.

PARA SABER MAIS

Os Procedimentos Operacionais Padrão têm revisão periódica, sendo que o POP SENASP/MJ foi lançado em 2013 e há uma expectativa de que em 2016 seja revisado e ampliado. Maiores informações podem ser obtidas na página da Secretaria Nacional de Segurança Pública – SENASP/MJ através do endereço: http://bit.ly/minjustbr - Acesso em 04 de agosto de 2016.

Os crimes cibernéticos e seus vestígios

Os crimes envolvendo equipamentos computacionais vêm aumentado, impulsionados pelas facilidades disponibilizadas pela tecnologia, pela velocidade da comunicação e pela própria especialização dos criminosos. Por envolver questões técnicas específicas, a justiça necessita de um profissional capaz de auxiliar a apuração dos crimes que envolvem o uso de computadores.

Para a Symantec[10], a criminalidade cibernética pode assumir muitas formas e ocorrer em qualquer hora ou lugar. Da mesma forma, os criminosos cibernéticos usam métodos diferentes, segundo suas habilidades e seus objetivos.

A definição de crime cibernético, ainda de acordo com Symantec, é qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de *hardware*. O computador ou dispositivo pode ser o agente, o facilitador ou o alvo do crime. O delito pode ocorrer apenas no computador ou fora dele. Para compreender melhor a ampla variedade de crimes cibernéticos, é necessário dividi-los em duas categorias gerais. Na primeira, o computador é apenas uma ferramenta de auxílio aos criminosos, que praticam crimes conhecidos, como sonegação fiscal, compra de votos em eleições, tráfico

10 Disponível em: http://bit.ly/nortoncc – Acesso em 25 de abril de 2016.

de entorpecentes e falsificação de documentos. Ou seja, se o dispositivo computacional não existisse, tal crime poderia continuar a ser praticado, utilizando outros meios. Já no segundo tipo, o computador é a peça central para o empreendimento do crime. Fraudes bancárias pela internet, compartilhamento de pornografia infantil por redes sociais e pichação de um site governamental são exemplos de crimes que não existiriam sem o uso de computadores.

No Brasil, foi a Lei 12.737/2012, sancionada em 2 de dezembro de 2012, que promoveu alterações no Código Penal Brasileiro, acrescentando-lhe os artigos 154-A e 154-B, a fim de tipificar os chamados delitos ou crimes informáticos praticados em âmbito nacional.

O QUE DIZ A LEI

Lei 12.737, de 30 de novembro de 2012

Invasão de dispositivo informático

Art. 154-A – Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de três meses a um ano e multa.

Art. 154-B – Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, estados, Distrito Federal ou municípios ou contra empresas concessionárias de serviços públicos.

Como o crime cibernético pode englobar uma gama muito ampla de transgressões, a compreensão de suas várias vertentes é essencial para identificar a ação mais adequada para ser adotada em um determinado caso.

Assim, é necessário recorrer a profissionais especializados, com amplo conhecimento em computação, segurança da informação, direito digital e outras áreas afins. Esse profissional deve ser capaz de identificar a autoria, a materialidade e a dinâmica de um crime praticado com auxílio da tecnologia.

Em um local de crime convencional, um vestígio pode significar um instrumento deixado no ambiente ou um fio de cabelo. Na informática, no entanto, os vestígios são digitais – zeros e uns, que poderão representar os mais diversos tipos de informação, como conversas *online*, histórico de navegação e programas maliciosos.

Aspectos e temas abordados no Tratado de Computação Forense

Identificação, Isolamento, Coleta e Preservação do Vestígio Cibernético

Um dos maiores desafios na Computação Forense é delimitar a abrangência de um determinado cenário criminoso, no qual a principal evidência é a informação digital. A

correta identificação, isolamento, coleta e preservação dos vestígios dessa natureza são fatores imprescindíveis para se chegar à autoria e à materialidade do crime. Uma vez que esses vestígios não são confinados em perímetro bem definido, mas espalhados em uma série de ambientes que precisam ser devidamente tratados, o leitor precisa enriquecer o seu cabedal de conhecimento com relação aos aspectos básicos do trato do vestígio cibernético, desde a busca e à manutenção da cadeia de custódia. Esse é o objetivo principal do Capítulo 1.

Fundamentos de Sistemas de Arquivos

O sistema de arquivos é a camada de *software* responsável pelo acesso aos dados armazenados nas mídias computacionais, como discos rígidos, *pendrives*, e cartões de memória. Os dados são armazenados, geralmente, na forma de arquivos, separados hierarquicamente em pastas, ficando a cargo do sistema de arquivos a criação, modificação e exclusão dos arquivos, garantindo a integridade das informações. Com o crescimento da capacidade das mídias e do tamanho dos arquivos, o controle de acesso aos dados torna-se uma tarefa cada vez mais complexa, exigindo o uso de sistemas de arquivos cada vez mais robustos e confiáveis. Os sistemas operacionais mais populares oferecem suporte a vários sistemas de arquivos, que vão desde sistemas simples como o FAT16 até sistemas mais sofisticados, como ReiserFS, HDFS e GDFS. Assim, o Capítulo 2 aborda os sistemas de arquivos e a forma de persistência das informações nas principais unidades de armazenamento.

Exames em Mídias de Armazenamento

Análise de discos rígidos, *pendrives* e mídias ópticas estão entre os tipos exame pericial mais comuns realizados nos Institutos Periciais e Polícias Científicas. Logo, saber como como lidar com os vestígios armazenados nesses dispositivos é fundamental para o trabalho do perito de informática. Pensando nisso, os autores do Capítulo 3 apresentam instruções sobre como lidar com mídias de armazenamento e como tratar os dados contidos nelas, desde a preservação até a análise.

Exames em Locais de Internet

Entender como os serviços de internet se comportam e a natureza dos protocolos envolvidos no processo de comunicação e distribuição de informações é de fundamental importância para proceder os exames em ambientes dessa natureza. Sendo assim, o Capítulo 4 apresenta as técnicas para tratar, coletar, examinar e analisar os vestígios relacionados a crimes digitais que envolvem a internet. Nele são abordadas as ferramentas e os métodos utilizados para a investigação de ilícitos em mensagens de e-mail, páginas web, redes sociais e comunicadores instantâneos.

Exames em Redes de Computadores e Dados de Interceptação Telemática

Com o aumento da conectividade do mundo moderno, as redes de computadores se tornaram fundamentais para praticamente qualquer tipo de comunicação, ocasionando em milhões de bytes de dados sigilosos transmitidos diariamente por esse meio. Como o crime organizado também utiliza a internet para realização dos mais variados delitos,

o Profissional da Computação Forense tem como desafio coletar e examinar essa grande massa de dados, extraindo evidências relevantes para a investigação. Outra questão importante é a volatilidade desse tipo de informação. Logo, o Capitulo 5 trata dos exames forenses em redes de computadores e interceptação telemática, apresentando ferramentas e formas de interpretação dos resultados colhidos por meio dessas ferramentas.

Exames em Imagens Digitais

O avanço programas de edição de imagens e a popularidade dos dispositivos móveis equipados com câmeras digitais abriu um leque de possibilidades para a perícia em imagens digitais. O conhecimento dessa área pode, inclusive, ser aplicado em outros ramos da perícia, como a documentoscopia. As técnicas, quando devidamente aplicadas, permitem a extração de informações úteis para as investigações, conforme é mostrado no Capítulo 6.

Exames em Constatação de Pornografia Infanto-juvenil

A Constatação de Pornografia Infanto-juvenil representa um grande desafio à perícia forense. Aliado ao aumento dos casos investigados, está a evolução de técnicas que e ferramentas que fortalecem o anonimato dos criminosos envolvidos. Além de tratar das questões legais, separando o que é transtorno e o que é crime, o Capítulo 7 apresenta métodos de trabalho que visam tornar o exame pericial mais eficaz.

Exames em Computação Embarcada

Os sistemas embarcados são cada vez mais comuns no cotidiano das pessoas e empresas. Com o advento da "Internet das Coisas" e dos dispositivos portáteis, a tendência é que os sistemas embarcados se tornem onipresentes. Por esse motivo, os dispositivos embarcados são fontes ricas em informações que podem auxiliar na elucidação de crimes. Devido às características desses dispositivos, esse tipo de exame pode permear as mais diversas áreas das Ciências Forenses, como perícias em veículos, aeronaves e equipamentos médicos. Formas adequadas de lidar com os equipamentos embarcados são tratadas no Capítulo 8.

Exames em Equipamentos Computacionais Portáteis e de Telefonia Móvel

Dispositivos móveis estão presentes na vida de quase todas as pessoas, principalmente, na forma de telefones celulares e *tablets*. Assim, o exame pericial desses equipamentos pode fornecer evidências e informações preciosas para uma investigação. No entanto, a grande diversidade de marcas, modelos e sistemas operacionais, bem como o ciclo de vida muito rápido desses produtos, oferece um desafio considerável para os peritos de Computação Forense. Diferentemente dos métodos clássicos de exame de computadores, não existe um método à prova de falhas para a realização de perícias em dispositivos móveis. Por esse motivo, o Capítulo 9 trará os principais aspectos que devem ser considerados para garantir a preservação da prova material aliada à recuperação do máximo possível de informação desses equipamentos.

Exames em Computação na Nuvem

A mudança de paradigma da computação tradicional para a Computação na Nuvem, fez com que itens logicamente relacionados possam estar geograficamente separados. Isso tornou possível o acesso a praticamente todo o tipo de informação a partir de qualquer dispositivo computacional.

Entretanto, poucos são os usuários que se preocupam com a segurança dessas informações, preferindo confiar cegamente nas empresas que fornecem serviços dessa natureza. Por essa razão, a segurança de todos esses dados compartilhados vem sendo estudada arduamente por pesquisadores. Nesse contexto, o perito Forense Computacional tem a responsabilidade de enfrentar um novo desafio. Esse importante tema será tratado no capítulo 10, no qual serão apresentados os aspectos relevantes no processo de garimpagem de informações importantes para resolução de casos envolvendo serviços na nuvem.

Exames em Detecção de Intrusão

A exploração de vulnerabilidades para invasão de sistemas, redes, dispositivos móveis e até mesmo ambientes em nuvem é uma prática crescente e preocupante em um mundo altamente conectado. Se, por um lado, essa conectividade cria um ambiente de compartilhamento de informações em uma velocidade que não para de crescer, ao mesmo tempo traz novas preocupações e desafios. Baseado nisso, o Capítulo 11 apresenta os conceitos relativos à detecção de intrusões e vulnerabilidades, além de mencionar ferramentas e técnicas para a coleta e análise de evidências encontradas nessas situações.

Exames em *Malwares*

Devido ao aumento da quantidade de dispositivos computacionais conectados, a distribuição de programas maliciosos associados à prática criminosa cresce diariamente. Consequentemente, o exame desse tipo de aplicativo é cada vez mais comum. Adicionalmente, a alta diversidade de métodos distintos de atuação faz com que os exames periciais desse tipo criem novos desafios aos especialistas em Computação Forense. Dessa forma, o propósito do Capítulo 12 é apresentar conceitos fundamentais e objetivos sobre a análise de *malwares*, juntamente com as ferramentas e as técnicas que irão auxiliar na identificação do comportamento e da autoria desse tipo de *software*.

Exames em Dados Criptografados

O Capítulo 13 apresenta as técnicas para tratamento de dados criptografados encontrados em análises periciais, abordando as ferramentas para detecção e processamento desses dados, incluindo os métodos utilizados para decifrá-los.

Técnicas Antiforenses

A Computação Forense enfrenta uma série de desafios durante a análise de materiais questionados, como a capacidade cada vez maior dos dispositivos de armazenamento. Entretanto, esse aumento não é nem de longe, o mais complexo dos desafios. Com a evolução das técnicas de análise e das ferramentas forenses, bem como da disseminação do conhecimento, surgiram as denominadas Técnicas Antiforenses, que têm como objetivo dificultar ou, até mesmo, impossibilitar que o processo investigatório ocorra de