


DESVENDANDO A
COMPUTAÇÃO
**FORENSE**

Pedro Monteiro da Silva Eleutério
Marcio Pereira Machado

Copyright © 2011 Novatec Editora Ltda.

Todos os direitos reservados e protegidos pela Lei 9610 de 19/02/1998.
É proibida a reprodução desta obra, mesmo parcial, por qualquer processo,
sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates
Editoração eletrônica: Camila Kuwabata e Carolina Kuwabata
Capa: Victor Bittow
Revisão gramatical: Débora Facin

ISBN: 978-85-7522-260-7

Histórico de impressões:

Janeiro/2011 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
Email: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Eleutério, Pedro Monteiro da Silva
Desvendando a computação forense / Pedro
Monteiro da Silva Eleutério, Marcio Pereira
Machado. -- São Paulo : Novatec Editora, 2010.

Bibliografia
ISBN 978-85-7522-260-7

1. Informática 2. Tecnologia e direito
I. Machado, Marcio Pereira. II. Título.

10-14095

CDU-34:007

Índices para catálogo sistemático:

1. Computação forense 34:007
OGF20110113



Computação Forense – conceitos gerais

Neste capítulo são abordados os conceitos gerais de Computação Forense, seu nascimento e sua definição. Também são debatidos os principais tipos de crimes e exames forenses¹ envolvendo equipamentos computacionais.

1.1 Introdução

Com o rápido desenvolvimento dos computadores desde a sua invenção, não demorou muito para esses dispositivos estarem presentes em várias atividades desempenhadas pelo ser humano. Em 1965, Gordon Moore propôs uma lei audaciosa para a época dizendo que o número de transistores que podiam ser impressos em uma pastilha (futuro processador de um computador) dobrava a cada ano. O fato é que, desde aquela época até os dias atuais, isso realmente vem acontecendo, porém não duplicando a cada ano, como previu Moore, e sim a cada aproximadamente 18 meses. Como consequência direta da Lei de Moore, Willian Stallings (2002) destaca que os computadores se tornam cada vez menores, mais rápidos e mais eficientes no consumo de energia. Com tamanha divulgação e popularização, nos dias de hoje, os computadores estão presentes não apenas nas empresas, mas nas casas, nas mãos (telefone celular, PDA², GPS³ etc.) e no dia a dia de pessoas de todo o mundo.

A popularização mundial da Internet, que ocorreu nos anos 90, devido à criação do serviço de World Wide Web (WWW), por Tim Berners-Lee (1989),

-
- 1 Segundo o dicionário Michaelis da Língua Portuguesa (2010), o termo “Forense” significa “Que se refere ao foro judicial / Relativo aos tribunais”.
 - 2 PDA é abreviatura de Personal Digital Assistant, dispositivo computacional portátil.
 - 3 GPS é abreviatura de Global Positioning System, dispositivo portátil utilizado para indicar a posição, com latitude e longitude, em qualquer lugar do planeta Terra.

permitiu que usuários dos diversos computadores espalhados pelo mundo pudessem trocar dados e informações em poucos milissegundos, permitindo maior velocidade e rapidez na comunicação entre máquinas e, consequentemente, entre as pessoas.

Assim como em qualquer outro campo de estudo, a inovação tecnológica traz uma série de benefícios para as pessoas e a comunidade em geral. Todavia, com as vantagens, traz também a possibilidade de realização de novas práticas ilegais e criminosas.

“Crimes sempre deixam vestígios!” – é uma frase dita costumeiramente pelas pessoas. Vestígio, segundo o dicionário Michaelis da Língua Portuguesa, 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 dentro desses equipamentos computacionais é composta por bits (números zeros e uns), em uma sequência lógica.

O Código de Processo Penal (CPP) determina em seu artigo 158 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.” Dessa forma, surge a necessidade de um profissional qualificado, que examine vestígios e produza laudos de interesse à justiça na apuração de um delito, conforme definidos nos caputs dos artigos 159 e 160 do CPP, que dizem, respectivamente: “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.” e “Os peritos elaborarão o laudo pericial, no qual descreverão minuciosamente o que examinarem e responderão aos quesitos formulados.” No caso específico da computação, quem realiza esse trabalho de forma oficial no âmbito criminal é o Perito Criminal em Informática. Entretanto, diversos outros profissionais podem ter a necessidade de realizar exames em computação. São eles: peritos particulares, auditores de sistemas, profissionais de TI e outros. Além disso, juízes, advogados, delegados, promotores e demais profissionais da área de direito também devem conhecer como evidências e provas digitais devem ser corretamente coletadas, apuradas e apresentadas.

Portanto, a Computação Forense tem como objetivo principal 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 crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo.

1.2 Crimes cometidos com o uso de equipamentos computacionais

Apesar de a utilização de computadores não ser uma prática tão recente no mundo do crime, a legislação brasileira ainda não está preparada para tipificar todas as modalidades específicas de crimes cibernéticos. Rosa (2007) também cita que a legislação brasileira necessita de muitos avanços na área. Assim, torna-se importante diferenciar se o computador é utilizado apenas como ferramenta de apoio à prática de delitos convencionais ou se é utilizado como meio para a realização do crime.

1.2.1 Equipamento computacional utilizado como ferramenta de apoio aos crimes convencionais

Nessa modalidade de crime, o computador é apenas uma ferramenta de auxílio aos criminosos na prática de crimes conhecidos, como sonegação fiscal, compra de votos em eleições, tráfico de entorpecentes e falsificação de documentos e outros.

A sonegação fiscal, por exemplo, existe se uma empresa utiliza um sistema de informação para emitir notas fiscais frias ou se a expedição ocorre de forma manual. O mesmo acontece quando um documento é falsificado por meio de um editor de imagens ou é adulterado com o uso de uma caneta esferográfica.

Nesses casos, o computador está associado ao *modus operandi*⁴ do crime. Assim, em muitos casos, exames forenses nesses equipamentos são uma excelente prova técnica, e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença.

Como qualquer outra ferramenta (agendas, veículos, telefones celulares etc.), o computador é utilizado apenas como um elemento auxiliar para a realização de um crime. Por exemplo, se o crime for um assalto a um banco, conforme mostra a figura 1.1, os criminosos poderiam se utilizar do computador

4 Modus operandi é uma expressão em latim que significa "modo de operação", utilizada para designar uma maneira de agir, operar ou executar uma atividade seguindo sempre os mesmos procedimentos.

para armazenar informações, como horários, mapas das agências e nomes de funcionários do banco, ou poderiam utilizar uma agenda convencional de papel para anotar os dados de interesse.

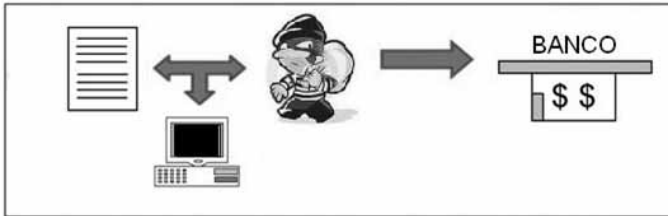


Figura 1.1 – Modalidade de crime mais comum em que o computador é utilizado como ferramenta de apoio.

Pela experiência dos autores, o uso de equipamentos computacionais como ferramenta de apoio aos crimes convencionais corresponde a cerca de 90% dos exames forenses realizados na área de informática⁵ (excluem-se dessa estatística os exames forenses em aparelhos celulares).

1.2.2 Equipamento computacional utilizado como meio para a realização do crime

Nessa modalidade, o computador é a peça central para a ocorrência do crime, ou seja, se o dispositivo não existisse, tal crime não seria praticado. Diferentemente da modalidade anterior, em que crimes convencionais são tipificados, novas formas de delitos surgem devido ao mau uso do computador e da Internet, como ataques a sites, roubo de informações, *phishing*⁶, programas maliciosos para roubo de senhas (*malwares*⁷) e outros. A figura 1.2 ilustra um exemplo de crime dessa modalidade. Se um hacker, em sua casa, desviar dinheiro de uma conta bancária a partir de acesso não autorizado a um Internet Banking, o computador exerce papel principal para a realização do delito. Se ele não existisse, esse crime não poderia ser realizado dessa maneira.

Um exemplo em evidência desse tipo de má utilização de computadores é o compartilhamento de arquivos de pornografia infanto-juvenil por meio da Internet. Muitos pedófilos e usuários baixam e compartilham fotos e vídeos com esse tipo de conteúdo, o que caracteriza crime de acordo com nossa

5 Tais números correspondem a uma aproximação, levando-se em conta exclusivamente a experiência profissional dos autores.

6 Tipo de fraude eletrônica que consiste basicamente em enganar usuários de computadores com o objetivo de “roubar” informações sensíveis, como senhas de bancos e de cartões de crédito.

7 O nome Malware vem do inglês Malicious Software.

legislação vigente⁸, mais precisamente o artigo 241-A do Estatuto da Criança e do Adolescente. Se o computador e a Internet não existissem, tal conduta seria impossível.



Figura 1.2 – Modalidade de crime em que o computador é o meio para a realização do delito.

Outro exemplo é quando se instala um programa de roubo de dados bancários no computador de um usuário. Tal programa pode obter senhas de acesso à Internet Bankings e de cartões bancários de forma indevida. Essa forma de crime somente é possível devido à utilização de computadores.

No entanto, um problema existente hoje em dia é a falta de uma legislação específica para todos os crimes cibernéticos. O país necessita de uma lei que tipifique criminalmente todos os delitos nos quais o computador é utilizado como meio, apesar de alguns já terem sido tipificados, como os presentes no Estatuto da Criança e do Adolescente, e outros serem enquadrados em alguns crimes convencionais, como estelionato e furto. Além disso, é necessário também legislar sobre a responsabilidade dos provedores de acesso à Internet e das conhecidas lan-houses e cyber cafés.

Tais práticas de crime vêm crescendo recentemente. Os autores acreditam que os atuais 10% restantes dos exames forenses realizados na área de informática tendem a crescer e, obviamente, serão maiores em um futuro próximo.

1.3 Principais exames forenses em informática

Considerando o crescente uso dos computadores e da popularização dos dispositivos computacionais portáteis, espera-se que novos tipos de exames forenses na área de informática sejam necessários em um futuro próximo. Da mesma forma, imagina-se que a demanda crescerá bastante nos próximos anos, pois os computadores tornaram-se um excelente mecanismo de investigação, sendo fundamentais para solucionar diversos tipos de delitos. Entretanto, nos dias atuais e dentro da experiência profissional dos autores, os principais exames forenses de informática são:

8 Até a data de publicação desta obra (janeiro/2011).

- **Exames e procedimentos em locais de crime de informática:** consistem principalmente no mapeamento, identificação e correta preservação dos equipamentos computacionais, a fim de permitir melhor seleção do material a ser apreendido, para serem examinados posteriormente em laboratório. Em alguns casos, é necessária a realização de exames forenses ainda no local de crime. O capítulo 2 trata da identificação dos dispositivos computacionais, sua correta preservação, apreensão e posterior acondicionamento, além de descrever os procedimentos fundamentais realizados pelo perito nos locais de crime e em buscas e apreensões envolvendo equipamentos de informática. O apêndice A traz um exemplo de Laudo de Exame de Local de Informática.
- **Exames em dispositivos de armazenamento computacional:** são os exames periciais mais solicitados na Computação Forense e consistem basicamente em analisar arquivos, sistemas e programas instalados em discos rígidos, CDs, DVDs, Blu-Rays, pen drives e outros dispositivos de armazenamento digital de dados. Esses exames são compostos de quatro fases (preservação, extração, análise e formalização) e fazem uso de algumas técnicas, como recuperação de arquivos apagados, quebra de senhas e virtualização⁹. Os principais procedimentos e as técnicas envolvidas nesse tipo de exame estão relatados no capítulo 3. Exemplos desse tipo de laudo podem ser encontrados nos apêndices B e C.
- **Exames em aparelhos de telefone celular:** compreendem basicamente a extração dos dados desses aparelhos, a fim de recuperar e formalizar as informações armazenadas em suas memórias (lista de contatos, ligações, fotos, mensagens etc.), de acordo com a necessidade de cada caso. Tais exames forenses são discutidos no capítulo 4 deste livro, e o apêndice D mostra um exemplo de laudo desse tipo.
- **Exames em sites da Internet:** consistem principalmente na verificação e cópia de conteúdo existente na Internet, em sites e servidores remotos dos mais variados serviços. Além disso, trata-se da investigação do responsável por um domínio de um site e/ou endereço IP¹⁰. Esses tópicos e toda a parte conceitual necessária são discutidos no capítulo 5. O apêndice E mostra um exemplo de Laudo de Exame da Internet.

9 Virtualização é um procedimento técnico que consiste basicamente em emular uma máquina virtual dentro de uma máquina real, conforme explicado na seção 3.2.3.6.

10 O conceito de endereço IP é definido e brevemente explicado na seção 5.1.2.

- **Exames em mensagens eletrônicas (emails):** correspondem basicamente à análise das propriedades das mensagens eletrônicas, a fim de identificar hora, data, endereço IP e outras informações do remetente da mensagem. Mais detalhes são expostos no capítulo 6. Um exemplo de laudo envolvendo rastreamento de email está no apêndice F.

Ressalta-se que existem outros dispositivos computacionais que são passíveis de exames forenses, porém não serão tratados neste livro, como exames em máquinas caça-níqueis, máquinas eletrônicas programáveis, placas de rede, modems, roteadores de rede, procedimentos para interceptação de dados, análise de programas maliciosos (malwares) e outros.

1.4 Exercícios

Questão 1.1 – Os equipamentos computacionais podem ser utilizados em dois grandes tipos de crimes. Assim, tais equipamentos podem ser utilizados:

- a) Como computador pessoal e como estação de trabalho do meliante.
- b) Como ferramenta de apoio aos crimes convencionais e como meio para a realização do crime.
- c) Como estação de trabalho do meliante e como forma de acesso à Internet.
- d) Como material de pesquisa para novos alvos e como dispositivo de roubo de senhas de bancos em geral.
- e) Como ferramenta de suporte para o monitoramento do alvo a ser atacado e como forma de se manter totalmente anônimo durante a realização de um crime.

Questão 1.2 – Uma empresa criminosa acaba de sonegar uma série de impostos pela emissão de notas fiscais frias (falsas). Essa emissão de notas foi realizada com uso de um programa de computador. Assinale a alternativa correta:

- a) O computador foi utilizado como ferramenta de apoio a um crime convencional, pois as notas fiscais frias poderiam ter sido emitidas de forma manual. Assim, o crime de sonegação ocorreria de qualquer forma.

- b) O computador foi utilizado como ferramenta de apoio a um crime convencional. Entretanto, as notas não poderiam ser emitidas de forma manual. Logo, se o computador não existisse, o crime de sonegação não iria ocorrer.
- c) O computador foi utilizado como meio para a realização do crime; afinal, a emissão de notas fiscais falsas só pode ser realizada com uso de um programa de computador.
- d) O computador foi utilizado como meio para a realização do crime, pois, se ele não existisse, o crime não ocorreria.
- e) O computador não serviu de apoio para a realização do crime, pois a sonegação é um crime convencional, e não virtual.

Questão 1.3 – Os exames periciais mais comuns no âmbito da Computação Forense são:

- a) Exames em locais de crime de informática.
- b) Exames em redes peer-to-peer.
- c) Exames em sites da Internet.
- d) Exames em dispositivos de armazenamento computacional.
- e) Exames em mensagens eletrônicas (emails).

Questão 1.4 – Os exames em dispositivos de armazenamento computacional consistem basicamente em analisar o conteúdo de equipamentos em busca de evidências digitais. Assinale a alternativa que não contém um dispositivo de armazenamento computacional:

- a) CD – Compact Disc.
- b) DVD – Digital Versatile Disc.
- c) Mensagem eletrônica – email.
- d) Pen drive.
- e) Disco rígido.

Questão 1.5 – Leia as assertivas a seguir:

- I. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.
- II. No caso específico da computação, quem realiza perícias de forma oficial no âmbito criminal é o Perito Criminal em Informática.
- III. A Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à área de informática.
- IV. O Estatuto da Criança e do Adolescente tipifica alguns crimes relacionados à pornografia infanto-juvenil em que o computador é utilizado como meio.

Assinale a alternativa que contém a quantidade de assertivas verdadeiras:

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4