


DES V E N D A N D O 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](mailto:novatec@novatec.com.br)  
Site: [www.novatec.com.br](http://www.novatec.com.br)  
Twitter: [twitter.com/novateceditora](https://twitter.com/novateceditora)  
Facebook: [facebook.com/novatec](https://facebook.com/novatec)  
LinkedIn: [linkedin.com/in/novatec](https://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

# Sumário

<b>Sobre os autores.....</b>	<b>11</b>
<b>Prefácio .....</b>	<b>13</b>
<b>capítulo 1 ■ Computação Forense – conceitos gerais .....</b>	<b>15</b>
1.1 Introdução.....	15
1.2 Crimes cometidos com o uso de equipamentos computacionais.....	17
1.2.1 Equipamento computacional utilizado como ferramenta de apoio aos crimes convencionais.....	17
1.2.2 Equipamento computacional utilizado como meio para a realização do crime ...	18
1.3 Principais exames forenses em informática .....	19
1.4 Exercícios .....	21
<b>capítulo 2 ■ Locais de crime envolvendo equipamentos computacionais.....</b>	<b>25</b>
2.1 Definição e conceitos gerais.....	25
2.2 Atuação do perito em locais de crime e em buscas e apreensões envolvendo dispositi- vos computacionais .....	26
2.2.1 Buscas e apreensões de informática.....	26
2.2.2 Locais de crime de informática .....	28
2.3 Identificação de dispositivos computacionais.....	29
2.3.1 Computadores pessoais (PCs) e discos rígidos.....	29
2.3.2 Notebooks .....	32
2.3.3 Servidores .....	33
2.3.4 Mainframes.....	34
2.3.5 Armazenamento portátil.....	34
2.3.6 Elementos de rede .....	35
2.3.7 Telefones celulares e PDAs .....	36
2.3.8 Estabilizadores e no-breaks .....	36
2.3.9 Scanners e impressoras multifuncionais .....	37
2.4 Apreensão de equipamentos computacionais.....	37
2.4.1 O que apreender?.....	38
2.4.2 Como apreender? .....	39
2.4.3 Descrição do material apreendido .....	39
2.4.4 Acondicionamento e transporte de equipamentos computacionais .....	40
2.5 Cuidados especiais.....	41
2.5.1 Computadores pessoais (PCs).....	41
2.5.2 Notebooks .....	42

2.5.3 Servidores .....	43
2.5.4 Mainframes .....	44
2.5.5 Armazenamento portátil .....	44
2.5.6 Elementos de rede .....	45
2.5.7 Telefones celulares e PDAs .....	45
2.5.8 Estabilizadores e no-breaks .....	45
2.5.9 Scanners e impressoras multifuncionais .....	46
2.6 Exercícios .....	46

### **Capítulo 3 ■ Exames forenses em dispositivos de armazenamento computacional ..... 51**

3.1 Características da mídia de armazenamento digital .....	51
3.1.1 Fragilidade .....	51
3.1.2 Facilidade de cópia .....	52
3.1.3 Sensibilidade ao tempo de vida .....	53
3.1.4 Sensibilidade ao tempo de uso .....	53
3.2 Fases do exame forense em dispositivos de armazenamento computacional .....	53
3.2.1 Fase 1 – Preservação .....	54
3.2.2 Fase 2 – Extração .....	61
3.2.3 Fase 3 – Análise .....	65
3.2.4 Fase 4 – Formalização .....	70
3.3 Principais ferramentas .....	77
3.3.1 Forensic ToolKit .....	77
3.3.2 EnCase .....	79
3.4 Principais desafios .....	80
3.4.1 Quantidade de arquivos .....	80
3.4.2 Existência de senhas .....	80
3.4.3 Criptografia .....	85
3.4.4 Esteganografia .....	86
3.5 Dicas de quesitação .....	87
3.6 Exercícios .....	88

### **Capítulo 4 ■ Exames em aparelhos de telefonia celular ..... 93**

4.1 Conceitos gerais .....	93
4.2 Fase 1 – Preservação .....	94
4.3 Fase 2 – Extração .....	95
4.3.1 Extração manual .....	95
4.3.2 Extração automática .....	96
4.4 Fase 3 – Análise .....	98
4.5 Fase 4 – Formalização .....	99
4.6 Polêmica .....	100
4.7 Dicas de quesitação .....	100
4.8 Recomendações práticas .....	101
4.9 Considerações finais .....	102
4.10 Exercícios .....	102

<b>Capítulo 5 ■ Análise de sites e mensagens eletrônicas.....</b>	<b>105</b>
5.1 Principais conceitos .....	105
5.1.1 A Internet e a World Wide Web (WWW) .....	105
5.1.2 Endereços IP .....	106
5.1.3 Domain Name System (DNS) .....	107
5.1.4 O papel dos provedores de acesso à Internet .....	108
5.2 Análise de sites.....	110
5.2.1 Verificação de conteúdo.....	110
5.2.2 Determinação dos responsáveis pelo conteúdo .....	111
5.3 Análise de mensagens de correio eletrônico .....	111
5.4 Dicas para elaboração do laudo.....	114
5.5 Exercícios.....	115
<b>Capítulo 6 ■ Pornografia infanto-juvenil.....</b>	<b>117</b>
6.1 Pedofilia .....	117
6.2 A legislação .....	117
6.3 Como caracterizar?.....	118
6.4 Compartilhamento de arquivos.....	119
6.4.1 eMule .....	119
6.4.2 Kazaa .....	121
6.4.3 LimeWire.....	121
6.4.4 Mensagens de correio eletrônico.....	122
6.5 Locais de crime e de busca e apreensão relacionados à pornografia infanto-juvenil....	123
6.6 Exercícios.....	125
<b>Capítulo 7 ■ Anexos com conteúdo digital .....</b>	<b>127</b>
7.1 Funções unidirecionais (Hash) .....	128
7.2 Geração da mídia óptica .....	129
7.3 Verificação da mídia óptica .....	132
7.4 Garantia da integridade do material questionado.....	134
7.5 Exercícios.....	135
<b>Considerações finais.....</b>	<b>139</b>
<b>Gabarito .....</b>	<b>140</b>
<b>Apêndice A ■ Exemplo de laudo de local de informática .....</b>	<b>141</b>
<b>Apêndice B ■ Exemplo de laudo de dispositivo de armazenamento computacional ..</b>	<b>153</b>
<b>Apêndice C ■ Exemplo de laudo de dispositivo de armazenamento computacional ..</b>	<b>163</b>

<b>Apêndice D ■ Exemplo de laudo de exame de telefone celular .....</b>	<b>179</b>
<b>Apêndice E ■ Exemplo de laudo de exame de Internet.....</b>	<b>187</b>
<b>Apêndice F ■ Exemplo de laudo de exame de Email.....</b>	<b>191</b>
<b>Referências .....</b>	<b>197</b>
<b>Índice remissivo .....</b>	<b>198</b>