

Aprenda Computação Forense

**Um guia para iniciantes para buscar,
analisar e proteger evidências digitais**

William Oettinger

Packt>

Novatec

Copyright © Packt Publishing 2020. First published in the English language under the title 'Learn Computer Forensics – (9781838648176)'

Copyright © Packt Publishing 2020. Publicação original em inglês intitulada 'Learn Computer Forensics – (9781838648176)'

Esta tradução é publicada e vendida com a permissão da Packt Publishing.

© Novatec Editora Ltda. [2021].

Todos os direitos reservados e protegidos pela Lei 9.610 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

Tradução: Lúcia A. Kinoshita

Revisão gramatical: Mônica d'Almeida

ISBN do impresso: 978-65-86057-55-3

ISBN do ebook: 978-65-86057-56-0

Histórico de impressões:

Abril/2021 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

E-mail: novatec@novatec.com.br

Site: <https://novatec.com.br>

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

GRA20210413

Sumário

Prefácio	10
Seção 1 ■ Adquirindo evidências.....	14
Capítulo 1 ■ Tipos de investigações computacionais.....	15
Diferenças nas investigações computacionais	16
Investigações criminais	18
Investigações corporativas	30
Resumo	43
Perguntas.....	43
Leitura complementar	44
Capítulo 2 ■ Processo de análise forense.....	45
Considerações anteriores à investigação	46
Compreendendo as informações sobre o caso e as questões legais.....	57
Compreendendo a aquisição de dados	59
Entendendo o processo de análise.....	65
Informando seus achados	74
Resumo	79
Perguntas.....	80
Leitura complementar	81
Capítulo 3 ■ Aquisição de evidências	82
Exploração das evidências	82
Compreensão do ambiente de investigação forense.....	86
Validação de ferramentas.....	87
Criação de mídias esterilizadas.....	91
Criação da imagem forense.....	99
Resumo	115
Perguntas.....	116
Leitura complementar	117

Capítulo 4 ■ Sistemas computacionais	118
Compreendendo o processo de boot	118
Compreendendo os sistemas de arquivos (filesystems)	134
Compreendendo o sistema de arquivos NTFS	145
Resumo	156
Perguntas	156
Leitura complementar	157
 Seção 2 ■ Investigação	158
 Capítulo 5 ■ Processo de investigação computacional	159
Análise da linha do tempo	160
Análise de mídia	177
Pesquisa de strings	179
Recuperação de dados apagados	182
Resumo	184
Perguntas	185
Leituras complementares	186
 Capítulo 6 ■ Análise de artefatos do Windows	187
Entendendo os perfis de usuário	188
Conhecendo o Registro do Windows (Windows Registry)	190
Determinando o uso de contas	192
Determinando se o usuário tinha conhecimento de arquivos	198
Identificando localizações físicas	210
Explorando a execução de programas	214
Conhecendo os dispositivos USB/conectados	216
Resumo	218
Perguntas	219
Leituras complementares	220
 Capítulo 7 ■ Análise forense da memória RAM	221
Básico sobre a memória	221
Memória de acesso aleatório?	223
Identificando fontes de memória	225
Capturando a RAM	227
Explorando ferramentas para análise de RAM	232
Resumo	239
Perguntas	240
Leitura complementar	241

Capítulo 8 ■ Análise forense de emails – técnicas de investigação	242
Conhecendo os protocolos de emails	243
Decodificando emails.....	246
Entendendo a análise de clientes de email	251
Entendendo a análise de webmails.....	255
Resumo	258
Perguntas.....	259
Leitura complementar	260
 Capítulo 9 ■ Artefatos da internet	 261
Entendendo os navegadores.....	261
Redes sociais.....	283
Compartilhamento de arquivos Peer-to-Peer	288
Computação em nuvem.....	293
Resumo	297
Perguntas.....	298
Leitura complementar	299
 Seção 3 ■ Relatórios.....	 300
 Capítulo 10 ■ Escrevendo o relatório.....	 301
Como fazer anotações de modo eficaz.....	301
Escrita do relatório.....	303
Resumo	310
Perguntas.....	310
Leitura complementar	311
 Capítulo 11 ■ Ética da testemunha especialista.....	 312
Conhecendo os tipos de processos judiciais	313
Iniciando a fase de preparação.....	315
Entendendo o curriculum vitae.....	316
Entendendo o testemunho e as evidências	319
Entendendo a importância do comportamento ético.....	322
Resumo	325
Perguntas.....	325
Leituras complementares.....	327

Respostas das Avaliações	328
Capítulo 1.....	328
Capítulo 2.....	328
Capítulo 3.....	328
Capítulo 4.....	329
Capítulo 5.....	329
Capítulo 6.....	329
Capítulo 7.....	330
Capítulo 8.....	330
Capítulo 9.....	330
Capítulo 10.....	331
Capítulo 11.....	331
 Índice remissivo	 333