

Perícia Forense Digital

Guia prático com uso do sistema operacional Windows

Nihad A. Hassan

Apress®

Novatec

São Paulo | 2019

First published in english under the title Digital Forensics Basics; A Practical Guide Using Windows OS by Nihad A. Hassan, edition: 1

Copyright © Nihad A. Hassan, 2019

This edition has been translated and published under license from Apress Media, LLC, part of Springer Nature. Apress Media, LLC, part of Springer Nature takes no responsibility and shall not be made liable for the accuracy of the translation.

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Publicação original em inglês intitulada Digital Forensics Basics; A Practical Guide Using Windows OS por Nihad A. Hassan, edição: 1

Copyright © Nihad A. Hassan, 2019

Esta edição foi traduzida e publicada com a autorização da Apress Media, LLC, parte da Springer Nature. Apress Media, LLC, parte da Springer Nature não assume nenhuma responsabilidade pela exatidão da tradução.

Capa desenvolvida por eStudioCalamar

Imagem da capa desenvolvida por Freepik (www.freepik.com)

© Novatec Editora Ltda. [2019].

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: Aldir Coelho Corrêa da Silva

Revisão gramatical: Tássia Carvalho

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-792-3

Histórico de impressões:

Setembro/2019 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

Email: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Sobre o autor	13
Sobre o revisor técnico.....	14
Agradecimentos.....	15
Introdução.....	16
Capítulo 1 ■ Introdução: entendendo a perícia forense digital	20
O que é perícia forense digital?.....	21
Objetivos da perícia forense digital	22
Cibercrime	23
Métodos de ataque dos cibercrimes	23
Como os computadores são usados nos cibercrimes?.....	24
Exemplo de cibercrime	24
Categorias da perícia forense digital.....	28
Perícia forense em computadores	28
Perícia forense móvel.....	28
Perícia forense em redes	29
Perícia forense em bancos de dados	29
Análise forense de dados	29
Usuários da perícia forense digital.....	30
Agentes da lei.....	30
Contencioso cível.....	30
Informação e contrainformação.....	31
Tipos de investigação forense digital	31
Prontidão da perícia forense.....	33
Importância da prontidão na perícia forense para as empresas	33
Evidência digital.....	35
Tipos de evidência digital.....	35
Localização da evidência eletrônica	38
Desafios da obtenção de evidência digital	39
Quem deve coletar a evidência digital?.....	41
Cadeia de custódia	42

Processo de exame da perícia forense digital.....	43
Confisco	44
Obtenção	45
Análise	45
Relatório	46
Guias oficiais do processo de perícia forense digital.....	47
Certificações de perícia forense digital	48
Perícia forense digital versus outras áreas da computação	49
Resumo do Capítulo.....	50
Capítulo 2 = Conceitos técnicos essenciais	52
Representação de dados.....	52
Decimal (base 10)	52
Binário.....	53
Hexadecimal (Base 16).....	54
Esquema de codificação de caracteres do computador.....	56
Estrutura dos arquivos.....	57
Metadados de arquivos digitais	59
Decodificador de timestamps (ferramenta)	62
Análise de hash	62
Como calcular o hash do arquivo	63
Tipos de memória.....	63
Memória volátil.....	64
Memória não volátil	64
Tipos de armazenamento dos computadores	64
Armazenamento primário	65
Armazenamento secundário	66
HPA e DCO.....	71
Considerações sobre recuperação de dados	72
Sistemas de arquivos.....	73
NTFS	73
FAT	74
Ambiente de computação.....	74
Ambiente de computação pessoal	74
Ambiente de computação cliente-servidor.....	75
Ambiente de computação distribuído	75
Computação em nuvem.....	75
Variações nas versões do Windows	77
Endereço IP	77
O que é um endereço IP?.....	78
Recursos e materiais de estudo sobre a perícia forense digital	79
Resumo do Capítulo.....	81

Capítulo 3 = Requisitos de um laboratório de computação forense.....82

Requisitos de instalação física do laboratório.....	84
Controles ambientais.....	86
Equipamento de Hardware.....	87
Mobília e materiais consumíveis.....	89
Sala da evidência.....	89
Estação de trabalho forense.....	90
Estação de trabalho forense comercial pronta para uso.....	91
Software forense.....	92
Ferramentas forenses comerciais.....	92
Ferramentas forenses livres e open source.....	92
Distribuições Linux para a perícia forense digital.....	93
Tecnologia de virtualização.....	94
Sistema de gerenciamento de informações do laboratório (LIMS, Laboratory Information Management System).....	94
Outros programas.....	94
Validação e verificação de hardware e software forense.....	94
Gerente do laboratório.....	95
Requisitos de sigilo.....	96
Backup dos dados do laboratório.....	96
Requisitos de treinamento.....	98
Políticas e procedimentos do laboratório.....	98
Documentação.....	99
Requisitos de certificação do laboratório.....	100
Etapa 1: Autoavaliação.....	100
Etapa 2: Identificação do nível atual de conformidade com os padrões de certificação desejados.....	101
Etapa 3: Fechando a lacuna.....	101
Etapa 4: Implementação.....	101
Etapa 5: Documentação de conformidade com os padrões.....	101
Resumo do Capítulo.....	102

Capítulo 4 = Resposta inicial e tarefas do responsável..... 104

Busca e confisco.....	105
Permissão de busca.....	106
Intimação.....	106
Mandado de busca.....	108
Kit de ferramentas do responsável.....	108
Tarefas do responsável.....	110
Ordem de volatilidade.....	114
Documentando uma cena de crime digital.....	115
Acondicionamento e transporte de dispositivos eletrônicos.....	116

Conduzindo entrevistas	117
Perguntas do responsável quando procurado por um cliente.....	117
Perguntas da entrevista com testemunhas.....	118
Assinatura da testemunha	119
Resumo do Capítulo.....	119
Capítulo 5 = Obtendo evidência digital.....	120
Formato de arquivo da imagem forense	121
Formato Raw	121
AFF.....	121
Expert Witness (EnCase).....	122
Outros formatos de arquivo	122
Validação do arquivo de imagem forense	122
Captura de memória volátil (obtenção em tempo real)	123
Memória virtual (espaço de swap)	124
Os desafios da obtenção da memória RAM.....	125
Capturando a RAM usando a ferramenta DumpIt	127
Belkasoft Live RAM Capturer	128
Capture a RAM com o Magnet.....	129
Capture a RAM com o FTK Imager.....	130
Capturando a memória não volátil (obtenção estática)	132
Métodos de captura da unidade de disco rígido	133
Usando o FTK Imager para capturar a unidade de disco rígido	135
Riscos e desafios da criação da imagem de unidade de disco rígido	141
NAS	141
Unidade de disco rígido criptografada	141
Unidade de disco rígido corrompida ou fisicamente danificada.....	142
Captura de dados na nuvem	142
Captura em rede	143
Limitações das ferramentas forenses.....	143
Outros desafios.....	144
Resumo do Capítulo.....	144
Capítulo 6 = Analisando a evidência digital	145
Analisando imagens forenses da unidade de disco rígido	145
Arsenal Image Mounter.....	146
OSFMount.....	147
Autopsy	148
Analisando a imagem forense da RAM.....	161
Redline	161
Framework Volatility.....	169
Resumo do Capítulo.....	173

Capítulo 7 = Análise forense no Windows	174
Análise de linha do tempo	176
Criando uma linha de tempo usando o Autopsy.....	176
Gere um relatório de linha do tempo usando o Autopsy	178
Recuperação de arquivos	180
Recupere arquivos excluídos usando o Autopsy	180
Perícia forense na lixeira do Windows	180
Remontagem de dados	186
Atribuindo uma ação à conta de usuário associada.....	186
Análise do Registro do Windows	187
Arquitetura do Registro do Windows	187
Capturando o Registro do Windows.....	189
Exame do Registro	190
Recuperação de chaves do Registro excluídas	202
Identificação do formato do arquivo.....	203
Análise forense em recursos do Windows.....	206
Análise no arquivo Prefetch do Windows.....	206
Perícia forense nas miniaturas do Windows	207
Perícia forense nas Jump Lists	208
Perícia forense em arquivos LNK	210
Análise de log de eventos.....	213
Análise de partição de unidade de disco rígido	216
Perícia forense em arquivos minidump do Windows	217
Pagefile.sys, Hiberfil.sys e Swapfile.sys.....	219
Perícia forense nas cópias de sombra de volume do Windows	221
Perícia forense no Windows 10	224
Perícia forense nos recursos do Windows 10	224
Resumo do Capítulo	228
Capítulo 8 = Perícia forense em navegadores web e emails	230
Perícia forense no navegador web	231
IE	231
Navegador web Microsoft Edge	233
Firefox	234
Google Chrome.....	237
History	239
Cookies	241
Top Sites	242
Shortcuts	242
Login Data.....	242
Web Data.....	242
Bookmarks	243
Bookmarks.bak.....	243

Pasta Cache	244
Outras ferramentas de investigação de navegadores web	244
Perícia forense em emails	246
Etapas das comunicações por email	247
Lista de protocolos de email	248
Exame de cabeçalho de email	248
Resumo do Capítulo	261
Capítulo 9 = Técnicas antiforenses	262
Usuários das técnicas antiforenses	263
Classificação das técnicas antiforenses	263
Esteganografia digital	263
Técnicas de destruição de dados e antirrecuperação	269
Técnicas de criptografia	273
Técnicas criptográficas de anônimo	277
Ataques diretos contra ferramentas de computação forense	278
Resumo do Capítulo	278
Capítulo 10 = Coletando evidências em fontes OSINT	280
Objetivos da coleta de OSINT	281
Categorias de OSINT	282
Benefícios da OSINT	284
Desafios impostos pela OSINT	285
Ciclo OSINT	285
A coleta de OSINT e a necessidade de privacidade	286
A OSINT e a darknet	287
Camadas da internet	288
Recursos online	290
Resumo do Capítulo	291
Capítulo 11 = Relatório forense digital	292
Principais elementos do relatório	293
Relatório autogerado	293
Resumo do Capítulo	295