Sumário

Introdução 1

1. O Que é Informação? 3
2. Segurança da Informação 3

Capítulo I – Terminologia Pericial e Convenções 5

1. Terminologias 5
2. Convenções 6

Capítulo II – O Grupo de Respostas a Incidentes 9

1. O Projeto 10
2. Missão do *CSIRT* 11
3. Implantando 11
4. Interagindo com Outros Setores da Empresa 12
5. Resultados 13
6. A Equipe 14
7. Política de Segurança 14
   - 7.1. Definição 14
   - 7.2. Amplitude 15
   - 7.3. Análise de Riscos 16
   - 7.4. Ameaças 16

7.5. Vulnerabilidades 16
7.6. Ativos 17
7.7. Risco 17
7.8. Infraestrutura 19
7.9. Sistemas 20
7.10. Recursos Disponíveis 21
7.11. Auditoria 21
7.12. Política de Senhas 21
7.13. Administração de Usuários 22
7.14. Política de Acesso à *Web* 22
7.15. Política de Uso de *Softwares* 24
7.16. Política de Antivírus 24
7.17. Política de *Patchs*, *Updates* e *Service Packs* 24
7.18. Acesso Discado, *VPN* e Outros Acessos Externos 25
7.19. Outras Políticas 25
7.20. Responsabilidades do Usuário 26
8. Atuando em um Incidente 26
8.1. Notificação do Incidente 26
8.2. Avaliação Inicial 27
8.3. Complementando Informações 27
8.4. Reunir Documentação de Apoio 27
8.5. Preparando uma Lista de Suspeitos 27
8.6. Investigando um Incidente 28
8.6.1. Iniciando a investigação 28
8.6.2. Realizando a perícia 28
8.6.3. Resposta inicial ao incidente 29
8.6.4. Elaborando o Relatório 29
8.6.5. Obtendo a Aprovação Final 30

CAPÍTULO III – A COMPUTAÇÃO FORENSE 31
1. Os Primeiros Crimes 32

2. Panorama Atual ... 32
3. Principais Modalidades ... 33
4. O Local de Crime ... 33
4.1. Áreas Imediatas ... 36
4.2. Áreas Mediatas ... 36
5. Caso Real ... 37

CAPÍTULO IV – PROCEDIMENTOS BÁSICOS PARA A COMPUTAÇÃO FORENSE ... 41
1. Recomendações, Princípios e Definições Apresentadas pela IOCE ... 42
1.1. Recomendações ... 42
1.2. Princípios ... 43
1.3. Definições ... 43
2. Procedimentos Básicos ... 44
2.1 Coleta de Evidências ... 44
2.2. Apreensão, Transporte e Armazenamento de Evidências ... 45
2.3. O Laboratório ... 46
2.4. A Perícia ... 46
2.5. Documentação e Laudo Pericial ... 48
3. Etapas da Perícia ... 48

CAPÍTULO V – ANÁLISE A QUENTE ... 51
1. Direcionando para uma Mídia Externa ... 52
2. Direcionando para uma Estação Pericial ... 52
3. Examinando o Histórico de Comandos do Shell ... 54
4. Listando Usuários Autenticados ... 55
5. Listando Conexões Estabelecidas ... 56
6. Listando Processos Ativos ... 58
7. Listando Portas Abertas ... 60
8. Ferramentas para Realização de Exames a Quente ... 63
8.1. *COFEE* ... 63

8.2. *E-Fense Live Responder* e o *Aperio* ... 65
9. Análise a Frio ... 65
10. A Duplicação Pericial ... 65
11. Bloqueio de Escrita ... 66
12. *Hardwares* Duplicadores de Disco ... 67
13. *Software* de Duplicação Pericial ... 68
14. Fazendo uma Duplicação Pericial ... 69

CAPÍTULO VI – OBJETOS DE PERÍCIA ... 71
1. O Computador ... 71
1.1. *Hardware* ... 71
1.2. *Software* ... 72
1.3. O Disco Rígido ... 73
1.4. O *Layout* do Disco Rígido ... 74
1.5. Sistemas Operacionais ... 75
2. Conceitos em Sistema de Arquivos ... 75
2.1. Sistema de Arquivos ... 75
2.2. FAT (*File Allocation Table*) ... 76
2.3. NTFS (*New Technology File System*) ... 77
2.4. EXT – *Extended File System* ... 77
2.5. CDFS – *Compact Disc File System* ... 77
2.6. HFS E (HFS+) – *Hierarchical File System* ... 78
2.7. UFS – Unix File System ... 78
2.8. *Clusters* ... 78
2.9. *Cluster Bitmap* ... 79
2.10. *Root Folder* (Pasta Raiz) ... 79
2.11. *File Entries* (Entrada de Arquivos) ... 79
2.12. *File Slack* (Folga do Arquivos) ... 80
2.13. Tamanho Lógico do Arquivo (*Logical File Size*) ... 80
2.14. Tamanho Físico do Arquivo (*Physical File Size*) ... 80

2.15. *RAM Slack* (Folga da RAM) 82

CAPÍTULO VII – INICIANDO A PERÍCIA 83

1. Identificando os Equipamentos 83
2. Evidências do Usuário 85
3. Evidências de Sistema 85
4. Histórico de Documentos 86
5. Indícios de Navegação na Internet 87
   - 5.1. Histórico 88
   - 5.2. Arquivos Temporários 88
6. Registro do *Windows* 89
7. Iniciando um Caso 92
   - 7.1. Identificando o Nome do Computador 92
   - 7.2. Identificando a Configuração de Fuso Horário 92
   - 7.3. Determinando Quando o Equipamento Foi Desligado pela Última Vez 93
   - 7.4. Último Acesso a Arquivos 95
   - 7.5. Registro de Dispositivos USB 95
   - 7.6. Arquivos Recentes 95

CAPÍTULO VIII – ANÁLISE DE METADADOS DE ARQUIVOS 97

1. Metadados dos Sistemas de Arquivos – *MAC Times* 98
   - 1.1. Exemplo 99
2. Metadados de Arquivos de Imagens 101
3. Metadados do *Microsoft Office* 103

CAPÍTULO IX – INVESTIGANDO CRIMES NA REDE 111

1. Estabelecendo uma Identidade na *Internet* 112
   - 1.1. O Protocolo *TCP/IP* 112
   - 1.2. O Endereço *IP* 113
   - 1.3. Atribuindo um Endereço *IP* 114

1.4. Análise de *LOGS* ... 115
1.4.1. Formato do *log* Padrão do *IIS* ... 115
1.4.2. Formato do *log* padrão ao apache ... 119
5. Investigação e Rastreamento de *E-mails* ... 121
6. Determinação de Origem e Autoria ... 122
7. O Correio Eletrônico ... 124
8. Buscando a Origem de um *E-mail* ... 125
8.1. O Cabeçalho de um *E-mail* (*E-mail Header*) ... 125
8.2. *HELO* ... 132
8.3. *MAIL FROM:* ... 132
8.4. *RCPT TO:* ... 132
8.5. *DATA* ... 133
8.6. *QUIT* ... 134
8.7. *Relaying* ... 136
8.8. O Cabeçalho *RECEIVED:* ... 137
8.9. Cabeçalhos Comuns ... 140
8.10. *X-HEADERS* (Cabeçalhos X) ... 142

REFERÊNCIAS BIBLIOGRÁFICAS ... 145

ANEXOS ... 147