

SUMÁRIO

Agradecimentos	5
Apresentação	7

CAPÍTULO I – COMPUTAÇÃO FORENSE

1.1 – Computação forense	13
1.2 – O processo da computação forense	14
1.3 – Identificação	15
1.4 – Coleta	17
1.5 – Preservação	22
1.6 – Exame	22
1.8 – Apresentação	24
1.9 – Ferramentas forense	25
1.10 – Hardwares forenses	26
1.11 – Exemplos de hardwares forenses	27
1.12 – Write Blocker – TABLEAU	27
1.13 – Write Blocker – WiebeTech	28
1.14 – Duplicador Forense – TABLEAU TXI	29
1.15 – Duplicador Forense – FALCON-NED	29
1.16 – Dispositivos de Captura de Dados – Mobile	30
1.17 – Dispositivos de Captura de Dados – PC 3000 – MOBILE	31
1.18 – Dispositivos de Captura de Dados – REDE – Profishark	32
1.19 – Faraday Bags – Mission Darkness – BlockBox Lab XL	32
1.20 – Faraday Bags – Mission Darkness – BlockBox Touch USB	33
1.21 – Dispositivos de Análise Física – Microscópio Eletrônico	34
1.22 – Disp de Análise Física – Leitores de Chip de memória – ALLSOCKET	34
1.23 – Identificação com placas – Placas de identificação Amarela	35
1.24 – Lacres e embalagens forenses. ELC STARLOCK	36
1.25 – Softwares forenses	36
1.26 – Exemplos de softwares forenses	38

1.27 – Belkasoft X	38
1.28 – Cellebrite UFED e Physical Analyzer	42
1.29 – Magnetic Forensics – Axiom	47
1.30 – Passware – Kit Forensic e Kit Mobile	52
1.31 – MOBILedit – Forensic	56
1.32 – Softwares forenses OpenSource	60
1.32 –TOP 10 – FreeSoftware Forensics	62
Referência bibliográficas	74

CAPÍTULO II – FORENSE EM DISPOSITIVOS MÓVEIS

2.1 – Introdução A perícia em dispositivos móveis	75
2.2 – Desafios neste novo mundo (Não tão novo)	78
2.3 Evidencias potenciais nestes dispositivos	80
2.4 Boas práticas periciais	81
2.5 Entendendo o mobile forense	84
2.6 A importância da perícia em dispositivos móveis	85
2.7 Extração de dados em dispositivos móveis	95
2.8 – A Forense em dispositivos móveis	98
Referência bibliográficas	100

CAPÍTULO III – ISO 27037

3.1 – ISO (International Organization for Standardization)	101
3.2 – ISO 27037	102
3.3 – ISO 27037 – REQUISITOS PARA MANUSEAR AS EVIDÊNCIAS DIGITAIS	106
3.4 – ISO 27037 – PROCESSO DE MANUSEIO	113
3.5 – ISO 27037 – CADEIA DE CUSTÓDIA	118
3.6 – CONCLUSÃO SOBRE A ISO 27037	120
Referência bibliográficas	121

CAPÍTULO IX – AQUISIÇÃO NA PRÁTICA IPHONE 7

4.1 – INTRODUÇÃO	123
4.2 – CASO PRÁTICO - HISTÓRIA	125
4.3 – INÍCIO DO PROCESSO	126

4.4 – PROCESSO DE IDENTIFICAÇÃO (ETAPA 1)	126
4.5 – PROCESSO DE COLETA (ETAPA 2)	137
4.6 – PROCESSO DE AQUISIÇÃO (ETAPA 3)	144
4.7 – PROCESSO DE PRESERVAÇÃO (ETAPA 4)	181
4.8 – DESFECHO FINAL DO CASO	192
Referência bibliográficas	193

CAPÍTULO X – AQUISIÇÃO NA PRÁTICA DE UM ANDROID

5.1 – INTRODUÇÃO	195
5.2 – CASO PRÁTICO - HISTÓRIA	195
5.3 – INÍCIO DO PROCESSO	197
5.4 – COLETA – ETAPA 1	198
5.5 – EXAME – ETAPA 2	230
5.6 – ANÁLISE – ETAPA 3	237
5.8 – CONCLUSÃO	250
Referência bibliográficas	252

CAPÍTULO XI - BUSCANDO MAIS CONHECIMENTO

6.1 – A BUSCA INTERMINAVEL PELO CONHECIMENTO	253
6.2 – ACADEMIA DE FORENSE DIGITAL	258
6.3 – TREINAMENTO PRÁTICO EM ELETRÔNICA E MANUTENÇÃO	260