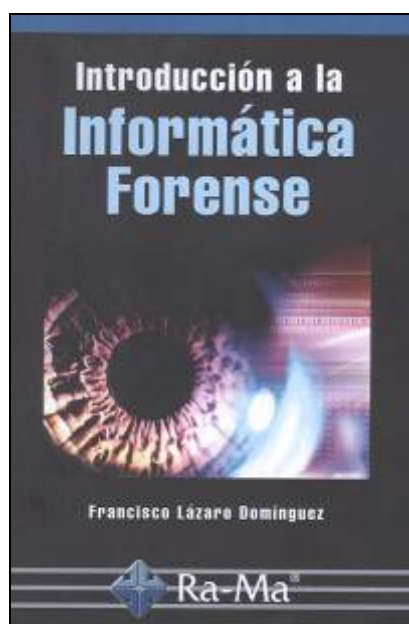




ÍNDICE

INTRODUCCIÓN	17
CAPÍTULO 1. SE HA ESCRITO UN CRIMEN DIGITAL	23
1.1 UN DÍA COMO OTRO CUALQUIERA	23
1.2 INTERVENCIÓN.....	25
1.2.1 Los primeros en llegar	25
1.2.2 Apagado sin más.....	25
1.2.3 Objetos intervenidos	26
1.3 LA AMENAZA DIGITAL	27
1.3.1 El delito informático	28
1.3.2 Evaluación del riesgo.....	29
1.3.3 Los motivos del agresor.....	30
1.3.4 Amenazas internas y externas.....	31
1.4 DINÁMICA DE UNA INTRUSIÓN	32
1.4.1 Footprinting.....	33
1.4.2 Escaneo de puertos y protocolos	34
1.4.3 Enumeración	35
1.4.4 Penetración y despliegue de exploits.....	35
1.4.5 Puertas traseras	36
1.4.6 Borrando huellas.....	36
CAPÍTULO 2. LA INVESTIGACIÓN FORENSE	37
2.1 ETAPAS DE UNA INVESTIGACIÓN FORENSE	37
2.1.1 Adquisición (Imaging).....	38

2.1.2	Análisis	39
2.1.3	Presentación.....	39
2.1.4	La línea de tiempo	40
2.2	REQUISITOS DE LA INVESTIGACIÓN FORENSE	41
2.2.1	Aceptabilidad	41
2.2.2	Integridad.....	41
2.2.3	Credibilidad	42
2.2.4	Relación causa-efecto.....	42
2.2.5	Carácter repetible	42
2.2.6	Documentación.....	42
2.3	VALORACIÓN JURÍDICA DE LA PRUEBA DIGITAL	44
2.3.1	Interés legal de la prueba	44
2.3.2	Prueba física y prueba personal.....	44
2.3.3	Cualificación del investigador forense	45
2.3.4	La adquisición: fase crucial	45
	CAPÍTULO 3. SOPORTES DE DATOS	47
3.1	PROCEDIMIENTOS DE ADQUISICIÓN	47
3.1.1	EnCase & Linen.....	49
3.1.2	dd	50
3.1.3	dcfldd, dc3dd y ddrescue	52
3.1.4	AIR	53
3.1.5	Adquisición por hardware	54
3.1.6	MD5 y SHA.....	55
3.1.7	Cálculo de MD5 con Linux	56
3.2	DISCOS, PARTICIONES Y SISTEMAS DE ARCHIVOS	56
3.2.1	NTFS.....	57
3.2.2	FAT.....	58
3.2.3	ext2, ext3, ext4	60
3.2.4	HFS, HFS+, JFS, ReiserFS, etc	61
3.3	MODELO DE CAPAS	62
3.3.1	Nivel 1: dispositivos físicos	62
3.3.2	Nivel 2: volúmenes y particiones	63
3.3.3	Nivel 3: sistemas de archivos	64
3.3.4	Nivel 4: bloques de datos	64
3.3.5	Nivel 5: metadatos	65
3.3.6	Nivel 6: nombre de archivo	66
3.3.7	Nivel 7: journaing.....	66

3.4	RECUPERACIÓN DE ARCHIVOS BORRADOS.....	67
3.4.1	Dinámica del borrado de archivos	68
3.4.2	Sector/, cluster/ y file slack.....	69
3.5	ANÁLISIS DE UNA IMAGEN FORENSE CON TSK.....	70
3.5.1	Componentes de TSK	71
3.5.2	Adquisición de un soporte de datos	73
3.5.3	Instalación de TSK	74
3.5.4	Análisis de la imagen.....	74
3.5.5	Análisis del sistema de archivos.....	76
3.5.6	Listado de archivos	79
3.5.7	Recuperando archivos borrados.....	81
3.6	ANÁLISIS DE ARCHIVOS	82
3.6.1	Firmas características.....	82
3.6.2	Documentos	84
3.6.3	Archivos gráficos.....	85
3.6.4	Multimedia.....	87
3.6.5	Archivos ejecutables.....	89
3.6.6	Exclusión de archivos conocidos.....	90
3.7	DATA CARVING	91
3.7.1	Cuando todo lo demás falla.....	92
3.7.2	Extracción de archivos.....	92

CAPÍTULO 4. ANÁLISIS FORENSE DE SISTEMAS MICROSOFT WINDOWS

4.1	RECOPILANDO INFORMACIÓN VOLÁTIL.....	96
4.1.1	Fecha y hora del sistema	96
4.1.2	Conexiones de red abiertas	97
4.1.3	Puertos TCP y UDP abiertos	98
4.1.4	Ejecutables conectados a puertos TCP y UDP	99
4.1.5	Usuarios conectados al sistema	100
4.1.6	Tabla de enrutamiento interna	101
4.1.7	Procesos en ejecución.....	102
4.1.8	Archivos abiertos.....	103
4.2	ANÁLISIS FORENSE DE LA RAM	103
4.2.1	Captura de RAM completa con dd.....	104
4.2.2	Volcado de RAM.....	105
4.3	ADQUISICIÓN DE SOPORTES.....	106
4.3.1	Adquisición con EnCase	107

4.3.2	Adquisición con FTK Imager.....	108
4.3.3	Otros métodos	109
4.4	ANÁLISIS POST MORTEM	110
4.4.1	Análisis con EnCase	110
4.4.2	AccessData FTK	112
4.4.3	Captain Nemo.....	115
4.4.4	Mount Image Pro.....	116
4.4.5	FileDisk	116
4.5	INVESTIGACIÓN DEL HISTORIAL DE INTERNET	117
4.5.1	Microsoft Internet Explorer	118
4.5.2	X-Ways Trace	119
4.5.3	iehist	120
4.5.4	Historial de navegación en Mozilla/Firefox.....	120
4.5.5	Chrome	122
4.6	LA PAPELERA DE RECICLAJE.....	122
4.6.1	Análisis de la papelera con Rifiuti.....	124
4.6.2	Funcionamiento de la papelera en Windows Vista/7	124
4.7	COOKIES	125
4.8	CORREO ELECTRÓNICO.....	126
4.8.1	Formatos PST y DBX Folders.....	127
4.8.2	Otros clientes de correo.....	128
4.8.3	Paraben's E-Mail Examiner.....	128
4.9	BÚSQUEDA DE CARACTERES.....	129
4.9.1	SectorSpy, Disk Investigator y Evidor	129
4.9.2	X-Ways Forensics	130
4.10	MET ADATOS	131
4.10.1	Cómo visualizar los metadatos de un documento.....	132
4.10.2	Metadata Assistant.....	133
4.10.3	FOCA.....	134
4.10.4	Metadatos EXIF.....	135
4.11	ANÁLISIS DE PARTICIONES NTFS Y FAT	136
4.11.1	Runtime DiskExplorer	137
4.11.2	Recuperación de archivos borrados	137
4.11.3	Runtime GetDataBack.....	138
4.11.4	EasyRecovery Professional	139
4.11.5	R-Studio.....	140

4.12	EL REGISTRO DE WINDOWS	141
4.12.1	Estructura y archivos del Registro	142
4.12.2	Análisis off line con Windows Registry Recovery	143
4.12.3	RegRipper	144
CAPÍTULO 5. ANÁLISIS FORENSE DE SISTEMAS		
LINUX/UNIX.....	145	
5.1	HERRAMIENTAS DE CÓDIGO LIBRE	146
5.1.1	¿Qué es exactamente el código libre?	146
5.1.2	Linux en la investigación forense.....	146
5.1.3	Poniendo en marcha una estación de trabajo con Linux	147
5.1.4	Descarga, compilación e instalación de herramientas.....	148
5.1.5	Montaje automático de particiones.....	148
5.2	ESTRUCTURA TÍPICA DE UN SISTEMA LINUX.....	151
5.2.1	Arquitectura y sistemas de archivos	151
5.2.2	Jerarquía de directorios	152
5.2.3	Archivos y permisos.....	154
5.2.4	Marcas de tiempo	157
5.3	INFORMACIÓN VOLÁTIL.....	157
5.3.1	Fecha y hora del sistema.....	158
5.3.2	Información de interés.....	158
5.3.3	Puertos y conexiones abiertas.....	160
5.3.4	Procesos en ejecución.....	161
5.4	ADQUISICIÓN FORENSE	161
5.4.1	Adquisición con dd	162
5.4.2	Adepto	163
5.5	ANÁLISIS.....	165
5.5.1	La línea de tiempo	165
5.5.2	Herramientas para elaborar una línea de tiempo	166
5.5.3	Recuperación de archivos borrados.....	167
5.6	OTRAS HERRAMIENTAS.....	168
5.6.1	Chkrootkit y Rkhunter	168
5.6.2	Md5deep	170
CAPÍTULO 6. REDES E INTERNET.....		173
6.1	COMPONENTES DE UNA RED	173
6.1.1	Visión general de una red corporativa	174
6.1.2	Archivos de registro	174
6.1.3	Preservación de elementos de evidencia en redes	175

6.1.4	Siguiendo pistas.....	177
6.2	PROTOCOLOS	178
6.2.1	Capa de transporte: TCP.....	180
6.2.2	Puertos	181
6.2.3	Capa de red: IP	182
6.2.4	Enrutamiento	184
6.2.5	Capa de enlace de datos: interfaces Ethernet.....	185
6.2.6	Protocolos de nivel superior: HTTP y SMB.....	187
6.3	ANALIZANDO EL TRÁFICO DE RED.....	190
6.3.1	Wireshark.....	190
6.3.2	Captura de tráfico: hubs, mirroring, bridges.....	191
6.3.3	Utilización de Wireshark	193
6.3.4	Un ejemplo práctico	196
6.4	COMPROBACIÓN DE DIRECCIONES IP	199
6.4.1	Herramientas de traza de red.....	199
6.4.2	Whois o quién es quién en Internet	200
6.4.3	Ping/fping	202
6.4.4	Traceroute/tracert.....	203
6.5	CORREO ELECTRÓNICO	204
6.5.1	Cabeceras e-mail	205
6.5.2	Estructura típica de un encabezado	205

CAPÍTULO 7. INVESTIGACIÓN FORENSE DE DISPOSITIVOS

MÓVILES	209
7.1 TELÉFONOS MÓVILES INTELIGENTES.....	210
7.1.1 Smartphones: pasaporte al siglo XXI	210
7.1.2 Hardware	212
7.1.3 Software.....	213
7.1.4 Información obtenible.....	215
7.2 INVESTIGACIÓN FORENSE DEL APPLE IPHONE	219
7.2.1 Consideraciones generales	219
7.2.2 Adquisición del iPhone mediante iTunes	221
7.2.3 iPhone Backup Extractor	223
7.2.4 Acceso a un backup encriptado	225
7.2.5 Adquisición lógica con herramientas de terceros	226
7.2.6 Adquisición física de un iPhone	227
7.2.7 Jailbreaking.....	228
7.2.8 Adquisición basada en técnicas de jailbreaking	229
7.2.9 Adquisición de otros dispositivos Apple.....	232

7.3	DISPOSITIVOS ANDROID	233
7.3.1	Introducción a Android	234
7.3.2	Adquisición de la tarjeta de memoria	235
7.3.3	Acceso al terminal Android	236
7.3.4	Utilidades de sincronización.....	236
7.3.5	Acceso mediante Android SDK.....	237
7.3.6	Algunas nociones básicas de Android Debug Bridge.....	239
7.3.7	Significado del rooting en Android	240
7.3.8	Adquisición física mediante dd	242
7.3.9	Examen de la memoria	243
7.4	RESTO DE DISPOSITIVOS Y PROCEDIMIENTOS.....	243
7.4.1	Supervivientes	243
7.4.2	Adquisición mediante Cellebrite UFED	244
7.5	PROCEDIMIENTOS Y RIESGOS.....	245
7.5.1	Alteración de las pruebas	245
7.5.2	Recomendaciones ACPO.....	246
7.5.3	Intervención de un dispositivo móvil.....	246
7.5.4	Riesgo legal	249
7.5.5	Privacidad	249
CAPÍTULO 8. INVESTIGACIÓN DE IMÁGENES DIGITALES		251
8.1	INFORMÁTICA FORENSE E IMÁGENES DIGITALES	252
8.2	IMÁGENES MANIPULADAS.....	253
8.2.1	¿Verdadero o falso?	253
8.2.2	¿Cómo funciona una cámara digital?.....	254
8.2.3	Interpolación e inconsistencia estadística	256
8.2.4	Artefactos.....	256
8.2.5	Zonas clonadas.....	257
8.2.6	Inconsistencias en la iluminación	258
8.2.7	E.L.A. (Error Level Analysis)	260
8.3	UTILIZACIÓN COMO HERRAMIENTA FORENSE	261
8.3.1	La imagen digital como prueba.....	262
8.3.2	Recomendaciones SWGIT.....	263
8.3.3	Buenas prácticas	264
8.3.4	Adquisición de imágenes en formato RAW	265
8.4	METADATOS GRÁFICOS.....	266
8.4.1	Exif.....	267
8.4.2	IPTC-IIM y Adobe XMP	267

8.4.3	Instalación y manejo de Exiftool	268
8.4.4	Ejemplo de aplicación	269
8.4.5	Limitaciones	271
CAPÍTULO 9. HELIX.....		273
9.1	UNA DISTRIBUCIÓN DUAL.....	274
9.1.1	¿Qué es Helix?	274
9.1.2	Características y novedades.....	274
9.1.3	Obtención de Helix.....	275
9.1.4	Arranque en vivo	276
9.1.5	CD autoarrancable.....	277
9.2	HELIX SOBRE UN SISTEMA EN FUNCIONAMIENTO	278
9.2.1	Interfaz	279
9.2.2	Información del sistema	280
9.2.3	Examen de la información volátil	281
9.2.4	Información de discos	281
9.2.5	Información de memoria RAM	282
9.3	ADQUISICIÓN DEL SISTEMA EN VIVO	283
9.3.1	Orden de volatilidad.....	283
9.3.2	Adquisición de memoria RAM	284
9.3.3	Recolección de información volátil.....	285
9.3.4	Imágenes de discos	286
9.3.5	Examen de un sistema en funcionamiento	288
9.3.6	Helix3 Pro™ Receiver.....	288
9.4	HELIX AUTOARRANCABLE	291
9.4.1	Live-CD Linux.....	291
9.4.2	Algunos aspectos de interés forense en Helix	292
9.4.3	Helix en una máquina virtual	293
CAPÍTULO 10. HERRAMIENTAS SOFTWARE.....		295
10.1	DISTRIBUCIONES LINUX.....	295
10.1.1	Backtrack.....	295
10.1.2	Knoppix.....	297
10.1.3	SystemRescueCD	299
10.1.4	CAINE	300
10.1.5	Slackware.....	302
10.2	VIRTUALIZACIÓN.....	306
10.2.1	VMware.....	307

10.2.2 VirtualBox.....	308
10.2.3 Listado de herramientas	309
CAPÍTULO 11. CONCLUSIONES.....	313
11.1 ESCENARIOS Y APLICACIONES	314
11.1.1 En el Juzgado	314
11.1.2 Investigaciones en organizaciones y empresas	314
11.1.3 Particulares y compañías de seguros.....	315
11.1.4 Sector público y seguridad nacional	315
11.2 OBSTÁCULOS	316
11.2.1 Destrucción intencionada de la evidencia	316
11.2.2 Tecnologías antiforenses.....	318
11.3 DESAFÍOS PARA EL FUTURO.....	319
11.3.1 Clusters.....	319
11.3.2 Cloud computing.....	321
11.4 ALGUNAS RECOMENDACIONES	323
11.4.1 La vida no es bella.....	323
11.4.2 Para terminar	324
BIBLIOGRAFÍA.....	327
ÍNDICE ALFABÉTICO.....	329