Índice

Prólogo 13

Capítulo I
Valoración de los casos y como afrontarlos 15

1. Introducción 15

2. Tipos de casos 15
Casos reales 16

3. Preparación del caso 17

4. Actividad del perito 18
El código Deontológico del perito informático 19

5. Conceptos legales a tener en cuenta 20

6. Guías para el análisis forense 23

7. Conclusiones 27

Capítulo II
Adquisición de evidencias 29

1. Qué nos podemos encontrar 29
Pasos a seguir para preservar la evidencia, cadena de custodia 29

2. Clonado 31

3. Tipos de Clonado 32
Adquisición física de un sistema apagado, una situación ideal 32
En caso de no disponer del hardware adecuado 35
Adquisición a través de una máquina encendida 35

4. Dispositivos Apple, opciones 36
Clonado Target Mode 37
Clonado PXE 38

5. Los hashes, como garantizar la integridad 39

6. Valoración de la situación 41

7. Conclusiones 42

Complicaciones legales y técnicas 42

Capítulo III
Forense en Windows, el sistema de ficheros 43

1. Introducción 43

2. Particiones de discos: MBR y GPT 44

GPT 45

Extracción de particiones GPT 47

Artefactos GPT 47

3. Sistema de ficheros FAT, File Allocation Table 48

Convención de nomenclatura de FAT 50

4. Sistema de ficheros NTFS, New technology File System 50

Clústeres y sectores en una partición NTFS 51

5. MFT (Master File Table) 52

Metadatos almacenados de la MFT 53

Resumen de la estructura: 55

6. Borrado de ficheros en Windows 55

Slack Space en detalle 57

Análisis de fichero y carving 58

Orphan Files 60

7. Conclusiones 60

Capítulo IV
Forense en Windows, los artefactos 63

1. Introducción 63

2. Los Prefetch 63

SuperFetch 64

3. Los Logs 65

4. Ficheros de Hibernación 67

5. Volume Shadow Copy 69

6. Registro del Sistema 70

Cómo se guardan los datos 70

Los subárboles 71

Las Listas MRU 74

7. Eventos EVTX 75
Definición de eventos EVTX 76
8. Herramientas 78
Log Parser 78
9. LNK Shortcuts 79
10. Otras evidencias 80
Navegación 80
Papelera de reciclaje 82
Los metadatos 83
Datos de red 84
11. Conclusiones 84

Capítulo V
Forense en Windows, la volatilidad 85
1. Introducción 85
2. Análisis con herramientas del sistema 86
Información de Procesos activos y Servicios en ejecución 86
Información de Red y conexiones: 87
Información de Ficheros 88
Información de usuarios 89
Información útil del sistema 90
3. Análisis forense de memoria RAM 90
Aplicaciones Metro y modelo de ejecución 91
Swapfile.sys, Pagefile.sys e Hiberfile.sys 92
Tipos de volcados 93
Métodos de adquisición 94
Análisis de procesos en RAM 95
4. Volatility 98
5. Más Volatilidad 108
Comandos y herramientas 108
Herramientas gráficas 109
6. Conclusiones 109

Capítulo VI
Más forense en Windows 111
1. Introducción 111
2. Artefactos diferentes o actualizados 111

Papelera de reciclaje ... 112
Thumbnails ... 113
One Drive ... 115
LOS PREFETCH ... 117

3. Artefactos nuevos: Spartan, Microsoft Edge, Facebook App y Cortana ... 119
Navegador Spartan ... 119
Microsoft Edge Browser ... 121
Facebook APP ... 123
Cortana ... 125
Notification Center (SIC) ... 128

4. Artefactos Similares ... 130
Event Logs ... 130
Internet Explorer ... 131
Usb Activity ... 131
Link Files ... 132

5. Windows server ... 132
FRS Deletion ... 133

6. Conclusiones ... 133

Capítulo VII
Correos electrónicos y otras evidencias ... 135

1. Introducción ... 135

2. Técnicas para la investigación de correo electrónico ... 136

3. Análisis de cabeceras ... 138

4. Cliente de correo Microsoft Outlook ... 142

5. Obtención de correos de Microsoft Exchange con PowerShell ... 143

6. Windows Mail ... 145
Artefactos asociados a Windows Mail ... 148

7. Mozilla Thunderbird ... 150

8. Conclusiones ... 151

Capítulo VIII
Forense en *nix ... 153

1. Introducción ... 153

2. Sistema de Ficheros de Unix ... 153
Estructura ext* ... 154

3. Proceso de análisis en Linux 155
TimeStamp en Linux 157
Históricos 160
Análisis de directorios 160
Comandos muy útiles en forense 161
Análisis de logs 161
Recuperación de ficheros borrados 162

4. Forense de Ram 163
Fmem 163
LIME (Linux Memory Extractor) 164
Análisis plataforma Linux con Volatility 165

5. Análisis de Malware 168
Detección de rootkits 168

6. Sistema de Ficheros de OSX 169
Introducción 169
La arquitectura del sistema 170
El sistema de ficheros 171
La importancia del tiempo 172
Las rutas más importantes dentro del análisis 173

7. Herramientas 178
Plaso 178
Pac4mac 179

8. Conclusiones 181

Capítulo IX
Kit de supervivencia de un perito 183

1. Introducción 183

2. Distribuciones 184
SIFT Workstation de SANS 184
Santoku 184
Caine 184
Deft Zero 185

3. Frameworks 185
Autopsy 185

4. Software Forense 192
FTKImager 192
OSForensics 195

5. Herramientas propias de Windows 195

Powershell 195
6. Comandos 199
Foremost 199
Herramientas del sistema 199
7. Otras herramientas 200
Forensic Foca 200
Herramientas de Nirsoft 200
Herramientas de SysInternals 201
Dumpit 202
Hibr2Bin 203
Sniffer 203
DDrescue 203
Windows Registry Recovery 205
Regripper para datos del sistema 207
8. Análisis de Malware con YARA 209
9. Conclusiones 214

Capítulo X
Informes periciales y la asistencia a juicio 217
1. Introducción 217
2. Redacción del informe 218
Firma digital 219
Estándar nacional para informes 219
3. Aspectos legales a tener en cuenta 221
Juramento o promesa 221
Imparcialidad del perito 221
4. Asistencia a juicio 223
5. Conclusiones 224

Índice alfabético 225

Índice de imágenes 229