

MARÍA ELENA DARAHUGE
LUIS E. ARELLANO GONZÁLEZ

MANUAL DE INFORMÁTICA FORENSE

(PRUEBA INDICIARIA
INFORMÁTICO FORENSE)

Bases metodológicas:
científica, sistémica, criminalística,
tecnológica-pericial y marco legal



ÍNDICE

| | |
|---|------|
| PRÓLOGO | XIII |
| PREFACIO..... | XV |
| CAPÍTULO 1. ESTRUCTURA GENERAL | 1 |
| Orientación para la lectura del manual..... | 2 |
| CAPÍTULO 2. LA PROBLEMÁTICA DE LA INFORMÁTICA FORENSE | 5 |
| El surgimiento de la Informática Forense, su inserción social, judicial y tecnológica | 7 |
| Concepto de Informática Forense..... | 9 |
| CAPÍTULO 3. IMPLANTACIÓN PERICIAL CRIMINALÍSTICA | 11 |
| Características destacables en la disciplina | 12 |
| Clasificación por su relación con el lugar del hecho | 12 |
| Causas de alteración del lugar del hecho | 14 |
| CAPÍTULO 4. IMPLANTACIÓN INFORMÁTICA | 19 |
| CAPÍTULO 5. IMPLANTACIÓN JUDICIAL | 23 |
| El delito informático propio e impropio | 25 |
| La reconstrucción del hecho | 25 |
| La reconstrucción metodológica del hecho | 27 |
| El lugar del hecho virtual propio e impropio | 28 |
| Prueba documental clásica (bibliográfica, foliográfica y pictográfica) e informática..... | 33 |
| Elemento probatorio pertinente y conducente | 34 |
| Prueba pericial informático forense | 34 |
| Relaciones con otras disciplinas | 35 |
| CAPÍTULO 6. INFORMÁTICA FORENSE - LA PRUEBA DOCUMENTAL INFORMÁTICA... | 37 |
| Principios y relaciones periciales informático forenses..... | 37 |
| La prueba documental informática..... | 38 |
| Definición y relaciones | 38 |
| Inteligencia estratégica | 39 |
| La entrevista..... | 39 |
| CAPÍTULO 7. INSERCIÓN LEGAL DEL PERITO EN INFORMÁTICA FORENSE - LA INSPECCIÓN JUDICIAL | 47 |
| Generalidades | 47 |
| Legalidad de la requisitoria pericial..... | 49 |
| Entorno legal del perito | 49 |

| | |
|--|-----|
| Formalidades de la aceptación del cargo | 50 |
| Diligencias previas en el Juzgado | 51 |
| Requisitos legales y formales de la inspección judicial | 52 |
| Artículos pertinentes del Código de Procedimientos Penal de la Nación (CPPN) | 52 |
| Responsabilidad legal del perito informático forense: posesión, protección, análisis, preservación y devolución de la prueba | 54 |
| Legislación de fondo, el perito como testigo y el falso testimonio | 55 |
| Legislación de forma | 57 |
| Legislación complementaria, leyes y proyectos | 58 |
| Jurisprudencia | 58 |
| CAPÍTULO 8. ACTIVIDADES PERICIALES COMPLEMENTARIAS | 61 |
| La aceptación del cargo | 61 |
| El informe pericial informático forense impreso y virtual | 63 |
| El párrafo de presentación | 64 |
| El objeto de la pericia y los puntos de pericia (tarea transdisciplinaria) | 65 |
| Los elementos ofrecidos (equipos, programas, indicios y rastros) | 68 |
| Las operaciones realizadas | 70 |
| Las conclusiones | 70 |
| CAPÍTULO 9. LA IMPUGNACIÓN | 73 |
| Revisión legal | 73 |
| La relación del perito con las partes y con los abogados de las mismas | 74 |
| Control, revisión y exigencia de legalidad en las herramientas utilizadas | 78 |
| Revisión científica, tecnológica y técnica | 79 |
| Revisión lógica | 80 |
| Revisión formal | 81 |
| CAPÍTULO 10. VALOR PROBATORIO DE LA PRUEBA INDICIARIA INFORMÁTICO FORENSE | 83 |
| Prueba documental informática (recaudos procesales) | 83 |
| Inserción de la prueba documental informática | 84 |
| Pertinencia de la prueba documental informática | 85 |
| El acceso y resguardo de la documental informática | 89 |
| La certificación de la documental informática | 89 |
| Recolección estratégica de la documental informática | 91 |
| Prueba pericial | 92 |
| En el delito informática propio e impropio | 92 |
| CAPÍTULO 11. UN EJEMPLO DE DELITO INFORMÁTICO PROPIO (EL PHISHING) | 93 |
| Herramienta de análisis del lugar del hecho real | 100 |
| Herramienta de análisis del lugar del hecho virtual | 100 |
| CAPÍTULO 12. GUÍA PARA EJECUTAR LA RECOLECCIÓN DE LA DOCUMENTAL INFORMÁTICA | 101 |
| CAPÍTULO 13. MARCO TECNOLÓGICO PERICIAL (la pericia informático forense en la práctica) | 105 |
| Listas de Control del Equipo del perito informático forense | 106 |
| Herramientas de <i>hardware</i> y <i>software</i> del perito informático forense | 109 |
| Elementos de <i>hardware</i> del laboratorio del perito informático forense | 109 |
| Equipo fijo de Laboratorio - Estación de trabajo | 110 |
| Equipo móvil de Laboratorio | 111 |

| | |
|--|-----|
| Componentes de hardware de uso específico | 112 |
| Laboratorios que trabajan para la Justicia y recuperan datos | 112 |
| Equipo para la autenticación y duplicación de evidencia del disco rígido | 113 |
| Herramientas de <i>software</i> para Informática Forense | 113 |
| Conjunto de herramientas integradas en un solo paquete de <i>software</i> de arranque en modo "en vivo" (live) disponibles para CD, DVD, Pendrive - Programas de <i>Software Libre</i> | 113 |
| Conjunto de herramientas integradas en un solo paquete de <i>software</i> - Productos Comerciales | 116 |
| Herramientas individuales e integradas en paquetes de función específica | 118 |
| Herramientas de funciones específicas | 121 |
| Borrado seguro, limpieza y desinfección | 122 |
| Duplicación de discos | 122 |
| Duplicación en forma remota | 123 |
| Manejo de Particiones | 123 |
| RED | 123 |
| Recuperación de archivos eliminados | 123 |
| En Windows | 124 |
| Recuperación de archivos con claves | 124 |
| Recuperación de archivos de la papelera de reciclaje | 124 |
| Telefonía, Celulares, PDA, GPS | 125 |
| Herramientas para la elaboración del informe pericial | 125 |
| Clasificación e identificación de las pericias informático forenses | 126 |
| Nomenclatura | 126 |
| Ejemplos | 126 |
| Etapas del Marco Tecnológico Pericial | 127 |
| Tarea a realizar en el Laboratorio | 127 |
| I – Etapa: Acceso a los recursos dubitados | 130 |
| II – Etapa: Identificación y registro | 130 |
| III – Etapa: Autenticación, duplicación y resguardo de la prueba | 131 |
| Procedimiento | 131 |
| Duplicación y autenticación de la prueba | 132 |
| Procedimiento para el resguardo de la prueba y preparación para su traslado | 134 |
| IV – Etapa: Detección, recolección y registro de indicios probatorios | 134 |
| Alternativa I, para el acceso con el equipo encendido | 135 |
| En sistemas operativos Microsoft Windows | 144 |
| Certificación matemática de los archivos | 144 |
| Envío de la evidencia a través de una conexión remota | 144 |
| Ejecución de un intérprete de comando legítimo | 144 |
| Registro de la fecha y hora | 144 |
| Descarga de la memoria RAM | 145 |
| Verificación de los usuarios conectados al sistema y de los usuarios con acceso remoto | 145 |
| Verificación de las fechas y hora de acceso, creación o modificación de todos los archivos | 146 |
| Verificación de los puertos abiertos | 147 |
| Verificación de las aplicaciones asociadas con los puertos abiertos | 148 |
| Verificación de los procesos activos | 149 |
| Verificación de las conexiones actuales y recientes | 150 |
| Revisión de los registros de eventos o sucesos del sistema operativo | 151 |

| | |
|--|-----|
| Verificación de la base de datos del Registro del sistema operativo | 152 |
| Examinar los archivos de configuración del sistema operativo | 155 |
| Verificación y obtención de las claves de los usuarios del sistema..... | 155 |
| Verificación de archivos relevantes | 155 |
| Herramientas | 155 |
| Descarga de los archivos temporales | 155 |
| Verificación de los enlaces a archivos rotos | 156 |
| Verificación de los archivos de navegación por Internet..... | 156 |
| Verificación y descarga de los archivos de correo electrónico | 157 |
| Cliente de correo Outlook Express | 158 |
| Cliente de correo Microsoft Outlook..... | 158 |
| Cliente de correo Netscape Messenger | 158 |
| Documentar los comandos utilizados durante la recolección de datos en la respuesta al incidente..... | 158 |
| Generación de un script o secuencia de comandos..... | 159 |
| Respuesta a incidentes | 159 |
| Alternativa II, con el equipo apagado | 161 |
| Procedimiento..... | 163 |
| V - Análisis e interpretación de los indicios probatorios. Reconstrucción y/o simulación del incidente..... | 163 |
| Procedimiento para el análisis e interpretación de los indicios probatorios..... | 163 |
| Elementos a examinar en el disco duro (Anexo - Lista de control de Análisis de discos) | 165 |
| Discos rígidos de computadoras portátiles..... | 166 |
| Aspectos a considerar de los sistemas de archivos de los sistemas operativos..... | 167 |
| Estructura del inodo..... | 169 |
| Niveles de almacenamiento en el sistema de archivos | 171 |
| Nivel físico | 172 |
| Nivel de clasificación de la información | 172 |
| Esquema de particiones de BSD..... | 173 |
| Nivel de unidades de asignación | 173 |
| Nivel de gestión del espacio de almacenamiento | 173 |
| Unidades de asignación (FAT Clusters)..... | 174 |
| Gestión del espacio de almacenamiento (Table FAT)..... | 174 |
| Entradas de directorios..... | 175 |
| Nivel de clasificación y almacenamiento del nivel de aplicación..... | 175 |
| Análisis de particiones de los discos duros | 175 |
| Herramientas..... | 176 |
| En Windows XP | 177 |
| En Windows | 180 |
| Análisis de los datos de las unidades de CD-R y CD-RW - DVD y dispositivos con memoria flash..... | 181 |
| Visualización de diferentes tipos de archivos | 182 |
| Búsqueda de texto y palabras claves..... | 183 |
| Análisis del espacio no utilizado o no asignado | 183 |
| Áreas del sistema de archivo que contienen datos borrados o eliminados..... | 184 |
| Espacio no asignado..... | 184 |
| Eliminación o borrado de información en el disco rígido | 185 |
| Listar los directorios ocultos de la papelera | 186 |
| Estructura de INFO2 | 187 |
| Eliminación segura de los datos..... | 188 |
| Análisis de datos ocultos..... | 189 |
| Tipo: Enmascaramiento..... | 191 |

| | |
|--|------------|
| Archivos protegidos con claves | 193 |
| Tipo: ocultamiento de información..... | 194 |
| Herramientas | 194 |
| Espacio no asignado, desperdiciado y libre | 195 |
| Tipo: alteración del entorno | 198 |
| Herramientas | 198 |
| Código malicioso o <i>Malware</i> | 198 |
| Métodos de invasión o ataque | 199 |
| Modos de control de la invasión o ataque..... | 199 |
| Modo de distribución o impregnación..... | 199 |
| Objetivos del código hostil | 200 |
| Análisis del correo electrónico | 203 |
| Características del encabezado de los mensajes..... | 205 |
| Descripción de encabezado..... | 205 |
| Aspectos importantes a considerar en el análisis del encabezado del mensaje.... | 208 |
| Herramientas para el análisis del encabezado de correo electrónico | 209 |
| Visualización de encabezados en diferentes clientes de correo electrónico..... | 209 |
| Verificación de los archivos de impresión..... | 210 |
| Análisis de código malicioso | 210 |
| Sitios de programas antivirus con la descripción de los distintos tipos de virus..... | 210 |
| Herramientas de Antivirus | 210 |
| Herramientas de control remoto | 211 |
| Herramientas exploradoras de red y de vulnerabilidades | 211 |
| Herramientas rastreadoras de la red o sniffers | 211 |
| Herramientas detector de DDoS (denegación distribuida de servicio) | 212 |
| Herramientas bombas lógicas y bombas de tiempo..... | 212 |
| Herramientas para el Registro de las acciones efectuadas por teclado y/o mouse..... | 212 |
| Herramientas para eliminación de huellas..... | 212 |
| Procedimiento..... | 213 |
| Análisis de celulares, PDA, GPS..... | 213 |
| VI - Cotejo, correlación de datos y conclusiones | 215 |
| Técnicas posibles a utilizar para el cotejo y correlación de los datos | 215 |
| Procedimiento para el cotejo y correlación de los datos | 215 |
| Procedimiento para la elaboración de conclusiones | 216 |
| Elementos a cotejar y correlacionar | 216 |
| Fecha y hora | 216 |
| Tablas de enrutamiento | 216 |
| Tabla ARP | 217 |
| Tabla de procesos activos | 217 |
| Tipo de sistema operativo..... | 218 |
| Sistemas de Archivos..... | 218 |
| Resguardo de herramientas de <i>hardware</i> y <i>software</i> utilizados en la pericia..... | 218 |
| APÉNDICE 1: ESTUDIO DE UN CASO REPRESENTATIVO. | 221 |
| APÉNDICE 2: PROCEDIMIENTO ANTE LA REQUISITORIA PERICIAL | 229 |
| APÉNDICE 3: EL MÉTODO SISTÉMICO (RESUMEN) | 235 |
| Visión sistémica de la investigación | 236 |
| Entrevista previa o licitación | 237 |
| Relevamiento de la información | 239 |

| | |
|--|------------|
| Selección de la metodología de análisis | 240 |
| Generación del modelo conceptual..... | 240 |
| Generación de los modelos complementarios | 241 |
| Programación y codificación..... | 241 |
| Prueba y ejecución en paralelo | 242 |
| Capacitación, supervisión y soporte de la aplicación | 242 |
| Retroalimentación..... | 244 |
| Síntesis | 244 |
| APÉNDICE 4: INFORMACIÓN COMPLEMENTARIA | 247 |
| Requisitoria pericial | 247 |
| Título VII - Participación criminal | 249 |
| Dibujo pericial complementario..... | 252 |
| Croquis ilustrativo. | 252 |
| Condiciones esenciales | 253 |
| Elementos | 253 |
| Dibujos auxiliares..... | 254 |
| Fotografías durante la inspección judicial..... | 259 |
| APÉNDICE 5: MANUAL DE AUTOPSY..... | 261 |
| Introducción | 262 |
| Emulador Cygwin | 262 |
| Instalación - Configuración y Acceso | 262 |
| Instalación de Cygwin..... | 262 |
| Ejecución de Cygwin y acceso al intérprete de comandos (shell)..... | 267 |
| Instalación de Sleuth Kit..... | 267 |
| Instalación de Autopsy..... | 268 |
| Descripción General de Autopsy..... | 269 |
| Ejecución de Autopsy en Cygwin | 271 |
| Creación de un caso en Autopsy | 272 |
| Opción Analyze- Analizar | 275 |
| Opción Keyword Search – Búsqueda de palabras claves | 279 |
| Comando “grep” (filtrar) | 280 |
| Opción File Type – Tipo de Archivo..... | 281 |
| Image Details – Detalles de la Imagen | 282 |
| Opción Meta Data - Metadatos | 283 |
| Aclaraciones acerca de NTFS y FAT | 284 |
| Opción Data Unit – Unidad de Datos | 284 |
| Aclaraciones sobre el sistema de archive FAT | 286 |
| Timeline Mode – Modo Línea de Tiempo..... | 286 |
| Image Integrity – Integridad de la Imagen | 289 |
| Event Sequencer - Secuencia de sucesos | 289 |
| Hash Database – Base de datos de <i>Hash</i> | 289 |
| Usos de las bases de datos - Database Uses | 290 |
| Configuración en Autopsy | 291 |
| Referencias..... | 291 |
| Anexo I - Herramientas de Sleuth Kit..... | 292 |
| Anexo II - Comando: sorter | 292 |
| APÉNDICE 6: RELACIONES CON LA PRUEBA INDICIARIA NO INFORMÁTICA..... | 293 |
| Expertos en Balística..... | 293 |
| Armas | 293 |
| Proyectiles..... | 294 |

| | |
|---|------------|
| Ropas..... | 295 |
| Huellas plantares (Retrato del paso) y de vehículos | 295 |
| Huellas dactilares | 295 |
| Manchas de sangre..... | 296 |
| Manchas varias (material fecal, meconio, calostro, semen, orina), pelos, fibras naturales o artificiales..... | 296 |
| Documentos | 296 |
| Suposiciones <i>a priori</i> | 296 |
| APÉNDICE 7: LA ESTRUCTURA LÓGICA DEMOSTRATIVA EN LA LABOR PERICIAL..... | 297 |
| Demostración lógica y tecnológica de las conclusiones alcanzadas | 297 |
| APÉNDICE 8: LA REDACCIÓN FINAL | 301 |
| Generación del informe pericial | 302 |
| Preparación de la defensa escrita/oral | 303 |
| Reglas para las citas..... | 305 |
| La posredacción..... | 305 |
| Respecto de la presentación | 306 |
| Respecto de la forma de presentación..... | 306 |
| Entrega formal del informe pericial..... | 307 |
| APÉNDICE 9: LA DEFENSA ORAL..... | 309 |
| La defensa ante el tribunal | 309 |
| Reglas de argumentación generales..... | 315 |
| Reglas para evaluar argumentaciones de los interlocutores | 316 |
| Reglas para construir nuestras propias argumentaciones..... | 317 |
| La defensa ortodoxa | 318 |
| Las lagunas pasajeras | 318 |
| Las metáforas..... | 319 |
| Las respuestas estrictas..... | 320 |
| Consideraciones prácticas para la argumentación oral | 320 |
| APÉNDICE 10: GLOSARIO COMPLEMENTARIO BÁSICO | 321 |
| APÉNDICE 11: RESUMEN DE LÓGICA PROPOSICIONAL | 325 |
| APÉNDICE 12: LA INSPECCIÓN JUDICIAL | 329 |
| Generalidades..... | 329 |
| Situaciones posibles en la inspección judicial..... | 331 |
| Metodología de trabajo | 333 |
| Acta de inspección o secuestro | 337 |
| APÉNDICE 13: MISCELÁNEAS | 339 |
| Listado de Claves BIOS - CMOS | 339 |
| Award | 339 |
| Ami | 339 |
| Phoenix | 339 |
| Otras | 339 |
| Varios fabricantes..... | 340 |
| Toshiba..... | 340 |
| IBM Aptiva BIOS..... | 340 |
| Listado de Puertos utilizados por Troyanos..... | 340 |

| | |
|---|-----|
| APÉNDICE 14: LA YAPA | 355 |
| ANEXO 1: DIAGRAMAS CONCEPTUALES | 365 |
| Marco científico investigativo | 365 |
| Esquema de investigación..... | 365 |
| ANEXO 2: MODELO DE INFORME PERICIAL | 371 |
| ANEXO 3: MODELOS DE NOTAS | 375 |
| ANEXO 4: FORMULARIOS. | 381 |
| Lista de control de <i>hardware</i> en la inspección y reconocimiento judicial..... | 381 |
| Formulario de registro de evidencia..... | 382 |
| Rótulos para las evidencias..... | 383 |
| Formulario – Recibo de efectos..... | 384 |
| Formulario para la Cadena de Custodia..... | 385 |
| Lista de control de respuesta a incidentes..... | 386 |
| Lista de control de análisis de discos..... | 387 |
| BIBLIOGRAFÍA | 389 |
| Libros..... | 389 |
| Jurídica..... | 389 |
| Informática Forense | 389 |
| Sistemas operativos – Protocolos y redes – Seguridad informática..... | 390 |
| Investigación..... | 391 |
| RFC – Request for Comment..... | 392 |
| Normas | 392 |
| Internet..... | 392 |
| Fraudes, delitos informáticos y crimen en el ciberespacio | 392 |
| Seguridad informática | 392 |
| RFC y estándares | 393 |
| Auditoría..... | 393 |
| Códigos de ética | 393 |
| Jurídica..... | 394 |
| Colegio de abogados | 394 |
| Criminalística..... | 394 |
| Grupos de discusión..... | 395 |
| De interés general..... | 395 |

MARÍA ELENA DARAHUGE
LUIS E. ARELLANO GONZÁLEZ

MANUAL DE INFORMÁTICA FORENSE II

(PRUEBA INDICIARIA
INFORMÁTICO FORENSE)

Bases teóricas complementarias.
Metodología suplementaria:
computación móvil (tablet, celulares,
iPhone, iPad, iPod, GPS, Mac, imágenes,
audio, video, Android, CD, DVD)



ÍNDICE

| | |
|--|-----|
| PRÓLOGO | VII |
| PREFACIO..... | IX |
| ESTRUCTURA GENERAL..... | XXI |
| Orientación para la lectura del manual..... | XXI |
| PRIMERA PARTE - TEORÍA | |
| Capítulo 1 - Revisión de conceptos | |
| La naturaleza pericial de la Informática forense | 3 |
| Confiar en el cargo y no exigir idoneidad..... | 7 |
| Extrañas dependencias periciales | 9 |
| Comparación de perfiles profesionales..... | 10 |
| La Informática forense y sus especialidades..... | 15 |
| El vocablo “prueba”..... | 15 |
| Prueba documental clásica | 15 |
| Prueba documental informática..... | 19 |
| Breve guía de recolección de prueba documental informática | 20 |
| Capítulo 2 - Las medidas previas, preliminares o prueba anticipada en Informática forense | |
| Características | 24 |
| Requisitos doctrinarios..... | 24 |
| Fallo relacionado..... | 29 |
| Capítulo 3 - Revisión jurisprudencial | |
| Fallos relacionados..... | 31 |
| La resolución por Cámara | 40 |
| Capítulo 4 - Criterios a tener en cuenta | |
| Las posibilidades de falsificación de mensajes de correo electrónico | 45 |
| Ejemplo de accionar ante eventualidad previsible | 46 |
| El uso de formas alternativas de resolución de conflictos..... | 48 |
| Tratamiento de residuos informáticos | 49 |
| La basura ciberespacial | 50 |
| Los riesgos de contaminarse..... | 52 |
| ¿Por qué debemos proteger el ciberespacio?..... | 52 |
| Inserción legal de la problemática | 56 |
| División de responsabilidades y tareas..... | 57 |

| | |
|--|-----|
| Capítulo 5 - La cadena de custodia informático forense | |
| Cadena de custodia vs. privacidad | 66 |
| La cadena de custodia en la práctica informático forense | 66 |
| Capítulo 6 - El contrato electrónico y la Informática forense | |
| Características del documento digital..... | 70 |
| El contrato digital, como forma de celebración contractual a distancia (entre ausentes)... | 72 |
| El problema de la jurisdicción en el contrato electrónico internacional | 75 |
| La prueba documental informática en el entorno regional | 78 |
| Capítulo 7 - El rol del perito informático forense en el proceso judicial | |
| Lo que se espera | 85 |
| Síntesis | 90 |
| SEGUNDA PARTE - PROCEDIMIENTOS | |
| Capítulo 8 - Procedimiento de aplicación general para teléfonos celulares | |
| Etapa de identificación, registro, protección, embalaje y traslado | 99 |
| Identificación y registro..... | 99 |
| Protección del dispositivo..... | 99 |
| Posibles estados en que se puede encontrar el dispositivo | 99 |
| Encendido..... | 99 |
| Apagado | 100 |
| Embalaje y traslado | 100 |
| Procedimiento para la recolección y protección de información – Elementos a recolectar | 100 |
| Recolección de información de la tarjeta SIM | 101 |
| Dispositivos iPhone | 101 |
| Sistema de archivos | 102 |
| Procedimientos y medidas preventivas para la protección, embalaje y traslado de dispositivos..... | 102 |
| Consideraciones previas..... | 102 |
| Procedimiento para iPhone encendido..... | 103 |
| Pantalla activa: Puede o no tener el código de acceso y la opción auto-bloqueo activa | 103 |
| Aislamiento del dispositivo de la red celular e inalámbrica | 103 |
| Procedimiento: El dispositivo tiene el código de acceso activado y está bloqueado para responder | 104 |
| Procedimiento para la comprobación del estado del código de acceso..... | 104 |
| Procedimiento para la verificación y secuencia del posible borrado remoto (<i>wipe</i>) .. | 105 |
| Procedimiento para iPhone apagado..... | 105 |
| Identificación y registro | 105 |
| Procedimiento para la identificación de dispositivos iPhones liberados (<i>jailbroken</i>) | 105 |
| Etapa de recolección y adquisición de datos | 106 |
| Procedimientos de recolección de datos en dispositivos iPhone e iPad..... | 106 |
| Consideraciones previas..... | 106 |
| Método de recolección física | 106 |
| Procedimiento para la preparación de la duplicación de la memoria Flash NAND | 107 |
| Procedimiento para ejecutar la herramienta iRecovery | 107 |
| Descripción del método de duplicación de la partición de datos de usuario del dispositivo utilizando el método de Jonathan Zdziarski | 108 |

| | |
|---|-----|
| Ejemplo del método de duplicación en un dispositivo liberado | 110 |
| Método de recolección lógica | 111 |
| Procedimiento para la recolección lógica de dispositivos iPhone..... | 112 |
| Método de recolección a partir de archivos de resguardo..... | 112 |
| Procedimiento para la recolección lógica a partir de los archivos resguardados con la herramienta iPhone Backup Extractor | 113 |
| Resguardos encriptados | 113 |
| Procedimiento para la recolección lógica de dispositivo iPhone, iPod táctil e iPad del resguardo efectuado con iTunes..... | 114 |
| Procedimiento para la recolección en iPhones | 115 |
| Etapa de análisis de datos | 115 |
| Análisis de la primera partición del sistema de archivo de iPhone (liberado) | 115 |
| Consideraciones previas..... | 115 |
| Análisis de la información adquirida o recolectada de los dispositivos iPhone..... | 117 |
| Procedimiento para la conversión de los archivos “.plist” | 117 |
| Consideraciones previas..... | 117 |
| Procedimiento para el montaje de imágenes “.dmg” en Mac | 117 |
| Procedimiento para el montaje de imágenes “.dmg” en Linux..... | 118 |
| Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux – Recuperación de archivos fragmentados..... | 118 |
| Consideraciones previas..... | 118 |
| Otras herramientas que efectúan la búsqueda de fragmentos de archivos | 119 |
| Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux – Recuperación de archivos con cadenas de caracteres ASCII | 120 |
| Consideraciones previas..... | 120 |
| Procedimiento para la creación de una línea de tiempo | 120 |
| Consideraciones previas..... | 120 |
| Procedimiento para el análisis de las bases de datos de sms con un editor en hexadecimal..... | 122 |
| Consideraciones previas..... | 122 |
| Procedimiento para el análisis de la estructura de directorios y partición de almacenamiento de datos en iPhone | 124 |
| Consideraciones previas..... | 124 |
| Procedimiento para el análisis de las aplicaciones preinstaladas en iPhone..... | 137 |
| Consideraciones previas | 137 |
| Análisis de la tarjeta SIM del teléfono iPhone | 155 |
| Revisión de conceptos..... | 155 |
| Dispositivos iPod..... | 155 |
| Etapa de identificación, registro, protección, embalaje y traslado de dispositivos iPod | 156 |
| Procedimiento con el iPod encendido..... | 156 |
| Etapa de recolección y adquisición de datos..... | 157 |
| Procedimientos de recolección de datos en dispositivos iPod | 157 |
| Consideraciones previas..... | 157 |
| Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh | 158 |
| Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh..... | 158 |
| Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh | 158 |
| Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh | 158 |
| Procedimiento para crear la imagen del dispositivo iPod con una estación de trabajo de Informática forense de Macintosh con el comando dc3dd | 159 |

| | |
|---|-----|
| Observación..... | 159 |
| Procedimiento para crear la imagen del dispositivo iPod con la herramienta de libre disponibilidad, FTK Imager, Forensic Tool Kit en una computadora con sistema operativo Windows..... | 159 |
| Procedimientos sintetizados de recolección en diferentes modelos de iPod | 163 |
| Etapa de análisis de datos | 164 |
| Procedimiento para el análisis del sistema de archivos de iPod..... | 164 |
| Consideraciones previas..... | 164 |
| Procedimiento para el análisis del archivo de imagen del dispositivo iPod en una computadora Mac | 165 |
| Consideraciones previas..... | 165 |
| Síntesis – Lista de control..... | 169 |
| Capítulo 9 - Computadoras Apple Macintosh | |
| Consideraciones previas..... | 171 |
| Procedimiento para la preparación de la estación de trabajo de Informática forense Apple Macintosh | 173 |
| Instalación del sistema operativo..... | 173 |
| Síntesis – Lista de Control..... | 175 |
| Etapa de recolección y adquisición de datos..... | 175 |
| Procedimiento de adquisición de una imagen de una computadora Macintosh con una computadora Macintosh..... | 175 |
| Consideraciones previas..... | 175 |
| Secuencia de pasos para la preparación de adquisición de la imagen..... | 177 |
| Procedimiento alternativo para la adquisición o duplicación de la imagen utilizando un CD de Linux en vivo | 181 |
| Consideraciones previas..... | 181 |
| Síntesis – Lista de control..... | 182 |
| Efectuar la imagen de Macintosh a Macintosh..... | 182 |
| Efectuar la imagen de una computadora dubitada Macintosh con un CD/DVD de arranque o inicio en vivo | 182 |
| Procedimiento para determinar la fecha y hora en Macintosh | 182 |
| Consideraciones previas..... | 182 |
| Procedimiento para la recolección de datos de memoria volátil en un sistema desbloqueado..... | 183 |
| Consideraciones previas..... | 183 |
| Procedimiento para la recolección de datos de memoria volátil en un sistema bloqueado | 186 |
| Consideraciones previas..... | 186 |
| Síntesis – Lista de control – Descarga de la memoria volátil..... | 189 |
| Procedimiento para la recolección de datos en el modo de usuario único (Single User Mode) | 189 |
| Consideraciones previas..... | 189 |
| Etapa de análisis de datos | 191 |
| Procedimiento para el análisis de la información del inicio del sistema operativo y los servicios asociados..... | 191 |
| Consideraciones previas..... | 191 |
| Procedimiento para el análisis del sistema de archivos HFS+ de la imagen recolectada..... | 191 |
| Procedimiento para el análisis de directorios especiales (<i>bundle</i>) en el sistema de archivos HFS+ de la imagen recolectada | 195 |
| Consideraciones previas..... | 195 |

| | |
|--|-----|
| Procedimiento para el análisis de archivos de configuración de red | 195 |
| Consideraciones previas..... | 195 |
| Procedimiento para el análisis de archivos ocultos..... | 196 |
| Consideraciones previas..... | 196 |
| Procedimiento para el análisis de aplicaciones instaladas | 196 |
| Consideraciones previas..... | 196 |
| Procedimiento para el análisis de espacio de intercambio (<i>swap</i>) y de hibernación .. | 197 |
| Consideraciones previas..... | 197 |
| Procedimiento para el análisis de sucesos o registros (<i>logs</i>) del sistema..... | 197 |
| Consideraciones previas..... | 197 |
| Procedimiento para el análisis de información de las cuentas de usuarios | 198 |
| Consideraciones previas..... | 198 |
| Procedimiento para el análisis del directorio de inicio (<i>Home</i>)..... | 198 |
| Consideraciones previas..... | 198 |
| Procedimiento para descifrar la carpeta de inicio del usuario cifrada por el servicio FileVault..... | 201 |
| Consideraciones previas..... | 201 |
| Síntesis – Lista de control | 202 |
| Procedimiento para la recuperación de datos del navegador web Safari de la imagen adquirida..... | 203 |
| Consideraciones previas..... | 203 |
| Caché del navegador | 204 |
| Íconos de la URL de los sitios (<i>webpagelcons.db</i>)..... | 205 |
| Archivos plist | 205 |
| Sitios más visitados (<i>TopSites.plist</i>)..... | 205 |
| Marcadores (<i>Bookmarks.plist</i>) | 205 |
| Descargas de archivos (<i>Downloads.plist</i>) | 206 |
| Historial (<i>History.plist</i>) | 207 |
| Última sesión (<i>LastSession.plist</i>)..... | 207 |
| Cookies.plist | 208 |
| Síntesis – Lista de control | 208 |
| Procedimiento para la función del navegador Safari como visor de archivos en el sistema operativo de Microsoft Windows..... | 209 |
| Consideraciones previas..... | 209 |
| Ubicación de los archivos plist en el sistema operativo de Microsoft Windows.... | 209 |
| Procedimiento para la recuperación y análisis de elementos de correo electrónico e iChat de la imagen adquirida..... | 213 |
| Consideraciones previas..... | 213 |
| Procedimiento para la recuperación de mensajes del cliente de correo de Microsoft Entourage de Office: Mac 2008 para Mac | 216 |
| Procedimiento para la recuperación y análisis de la libreta de direcciones (<i>Address Book</i>) de la imagen adquirida..... | 216 |
| Consideraciones previas..... | 216 |
| Procedimiento para la recuperación y análisis de datos del iChat de la imagen adquirida | 217 |
| Consideraciones previas..... | 217 |
| Síntesis – Lista de control | 218 |
| Apple Mail..... | 218 |
| Libreta de direcciones..... | 219 |
| iChat..... | 219 |
| Procedimiento para la recuperación y análisis de fotografías de la imagen adquirida | 219 |

| | |
|---|-----|
| Consideraciones previas..... | 219 |
| Características de la aplicación iPhoto..... | 220 |
| Ubicación de los archivos de iPhoto..... | 221 |
| Síntesis – Lista de control..... | 223 |
| Procedimiento para la recuperación y análisis de películas y videos de la imagen adquirida..... | 224 |
| Consideraciones previas..... | 224 |
| Síntesis – Lista de control..... | 227 |
| Procedimiento para la recuperación y análisis de archivos del procesador de texto Word y de documentos portables (PDF)..... | 227 |
| Consideraciones previas..... | 227 |
| Síntesis – Lista de control..... | 233 |
| Procedimiento para el análisis del historial de conexiones de dispositivos..... | 234 |
| Consideraciones previas..... | 234 |
| Procedimiento para el análisis de conexiones Bluetooth..... | 234 |
| Consideraciones previas..... | 234 |
| Procedimiento para el análisis de conexiones VNC..... | 234 |
| Consideraciones previas..... | 234 |
| Procedimiento para el análisis de la aplicación Volver a mi Mac (Back to My Mac)..... | 235 |
| Consideraciones previas..... | 235 |
| Capítulo 10 - Android | |
| Consideraciones previas..... | 237 |
| Componentes de hardware de los celulares Android..... | 237 |
| Componentes de software de los celulares Android..... | 238 |
| Estructura del sistema de archivos en Android..... | 240 |
| Estructura del encabezado (entrada de directorio)..... | 241 |
| Tipos de memoria en los dispositivos Android..... | 243 |
| Sistemas de archivos..... | 243 |
| Procedimiento para crear un emulador de un dispositivo Android..... | 244 |
| Etapa de recolección y adquisición de datos..... | 245 |
| Procedimiento para la duplicación de los dispositivos USB de almacenamiento (UMS - USB Mass Storage) en dispositivos Android..... | 245 |
| Consideraciones previas..... | 245 |
| Procedimiento para la recolección lógica de datos en dispositivos Android..... | 247 |
| Consideraciones previas..... | 247 |
| Procedimiento para la recolección lógica de datos con AFLogical..... | 251 |
| Procedimiento para la recolección física de datos..... | 254 |
| Consideraciones previas..... | 254 |
| Procedimiento para el acceso como usuario <i>root</i> por medio de las herramientas de software..... | 255 |
| Procedimiento para el método AFPhysical de imagen física del disco de las particiones de la memoria Flash NAND de Android..... | 259 |
| Síntesis – Lista de control..... | 264 |
| Etapa de análisis de datos..... | 265 |
| Procedimiento para el análisis del núcleo del sistema operativo Linux..... | 265 |
| Procedimiento para descargar la memoria RAM en Android..... | 276 |
| Procedimiento para el análisis de la línea de tiempo en YAFFS2..... | 278 |
| Consideraciones previas..... | 278 |
| Procedimiento para el análisis del sistema de archivos YAFFS2 con las áreas de reserva OOB..... | 278 |
| Consideraciones previas..... | 278 |

| | |
|---|-----|
| Procedimiento para el análisis de fragmentos (<i>carving</i>) del sistema de archivos..... | 279 |
| Procedimiento para el análisis del sistema de archivos con el comando strings..... | 280 |
| Procedimiento para el análisis del sistema de archivos con el visor en hexadecimal <i>ncurses-hexedit</i> | 280 |
| Procedimiento para el análisis del contenido de los directorios del sistema de archivos de Android..... | 283 |
| Procedimiento para la creación de la línea de tiempo en el sistema de archivos FAT de la tarjeta SD..... | 290 |
| Procedimiento para el análisis del sistema de archivos FAT de la tarjeta SD..... | 292 |
| Procedimiento para el análisis de las aplicaciones en Android..... | 293 |
| Aplicación de mensajes..... | 294 |
| Aplicación de ayuda de mensajes..... | 295 |
| Aplicación de Navegador de Internet..... | 295 |
| Aplicación de contactos..... | 299 |
| Aplicación de Explorador de Medios..... | 301 |
| Aplicación Google Maps..... | 302 |
| Aplicación Gmail..... | 304 |
| Aplicación de correo..... | 305 |
| Aplicación Dropbox..... | 305 |
| Aplicación Adobe Reader..... | 305 |
| Aplicación Youtube..... | 305 |
| Aplicación Cooliris Media Gallery..... | 306 |
| Aplicación Facebook..... | 306 |

Capítulo 11 - Discos ópticos

| | |
|---|-----|
| Análisis forense de almacenamiento de discos ópticos..... | 307 |
| Consideraciones previas..... | 307 |
| Composición física..... | 307 |
| Tabla de especificaciones de discos ópticos..... | 308 |
| Técnicas de escritura en los discos ópticos..... | 308 |
| Sistemas de archivos..... | 309 |
| Etapa de identificación, registro, protección, embalaje y traslado..... | 310 |
| Identificación y registro..... | 310 |
| Protección de los discos ópticos..... | 310 |
| Rotulado de los discos compactos..... | 311 |
| Embalaje y traslado..... | 311 |
| Etapa de recolección y adquisición de datos..... | 311 |
| Procedimiento para la duplicación de discos ópticos CD y DVD..... | 311 |
| Consideraciones previas..... | 311 |
| Etapa de análisis de datos..... | 314 |
| Procedimiento para la preparación del análisis de los discos ópticos..... | 314 |
| Procedimiento para el análisis del sistema de archivo ISO9660..... | 316 |
| Consideraciones previas..... | 316 |
| Procedimiento para el análisis del sistema de archivo Joliet..... | 319 |
| Procedimiento para el análisis del sistema Rock Ridge..... | 319 |
| Procedimiento para el análisis del sistema UDF..... | 320 |
| Procedimiento para el análisis del sistema HFS y HFS+ (Apple Macintosh)..... | 321 |
| Procedimiento para el análisis del sistema El Torito..... | 321 |
| Procedimiento para el análisis de la imagen adquirida con Autopsy para Windows..... | 321 |
| Procedimiento general para el análisis de discos ópticos y/o de sus respectivas imágenes..... | 325 |
| Consideraciones previas..... | 325 |

| | |
|--|-----|
| Capítulo 12 - Dispositivos de navegación vehicular por GPS Tom Tom | |
| Consideraciones previas..... | 329 |
| Etapas de identificación, registro, protección, embalaje y traslado de dispositivos de GPS Tom Tom | 330 |
| Etapas de recolección y adquisición de datos | 330 |
| Procedimientos de recolección de datos en dispositivos de GPS Tom Tom | 330 |
| Etapas de análisis de datos..... | 332 |
| Procedimiento para el análisis de datos en dispositivos de GPS Tom Tom | 332 |
| Capítulo 13 - Miscelánea | |
| Características del software de bloqueo de escritura..... | 335 |
| Procedimiento del uso de software bloqueador de escritura..... | 335 |
| Referencia acerca del software bloqueador de escritura | 336 |
| Dispositivos BlackBerry | 339 |
| Consideraciones previas | 339 |
| Tipos de almacenamiento de archivos en dispositivos BlackBerry..... | 340 |
| Etapas de identificación, registro, protección, embalaje y traslado..... | 340 |
| Procedimiento: El dispositivo tiene el código de acceso | 340 |
| Etapas de recolección y adquisición | 341 |
| Procedimiento para la adquisición física de datos..... | 341 |
| Procedimiento para la adquisición de datos a partir del archivo de resguardo..... | 342 |
| Consideraciones previas..... | 342 |
| Etapas de análisis de datos | 343 |
| Procedimiento para el análisis de los datos del archivo de resguardo..... | 343 |
| Procedimiento para el análisis de archivos de imágenes..... | 344 |
| Consideraciones previas..... | 344 |
| Procedimiento de identificación de los metadatos del archivo de la imagen .. | 350 |
| Análisis del contenido de la imagen..... | 360 |
| Detección de rostros e imágenes de adultos | 361 |
| Herramientas para reconocimiento de caras | 363 |
| Herramientas para el análisis de los metadatos del archivo de la imagen..... | 363 |
| Procedimiento para el análisis de los archivos de audio y video | 364 |
| Consideraciones previas..... | 364 |
| Tipos de archivos de audio y video..... | 364 |
| Procedimiento para el análisis del contenido del video forense..... | 386 |
| Guía para el procedimiento de video de la Agencia Federal de Investigaciones (FBI) | 387 |
| Herramientas para el análisis de video de vigilancia | 391 |
| Formulario de registro de evidencia de video | 393 |
| Anexo 1 - Procedimiento para la cadena de custodia en la pericia de informática forense | |
| Procedimiento..... | 397 |
| Duplicación y autenticación de la prueba | 398 |
| Operaciones a realizar | 399 |
| Recolección y registro de evidencia virtual..... | 400 |
| Equipo encendido | 400 |
| Procedimiento para el acceso a los dispositivos de almacenamiento volátil..... | 401 |
| Procedimiento con el equipo encendido | 401 |
| Equipo apagado | 402 |
| Procedimiento para la detección, recolección y registro de indicios probatorios... .. | 402 |
| Procedimiento para el resguardo de la prueba y preparación para su traslado..... | 404 |
| Traslado de la evidencia de Informática forense | 405 |
| Inventario de hardware en la inspección y reconocimiento judicial..... | 406 |

| | |
|--|-----|
| Formulario de registro de evidencia de la computadora..... | 407 |
| Formulario de registro de evidencia de celulares..... | 408 |
| Rótulos para las evidencias | 409 |
| Formulario - Recibo de efectos..... | 409 |
| Formulario para la cadena de custodia..... | 410 |
| Formulario de responsables de la cadena de custodia | 411 |
| Modelo de Acta de inspección o secuestro. | 412 |
| Modelo de Acta de escribano | 413 |

Anexo 2 - Estructura demostrativa judicial

| | |
|----------------------------------|-----|
| El problema de la prueba | 416 |
| El problema de la redacción..... | 417 |

Anexo 3 - La notificación por correo electrónico (ley 14.142, pcia. de Bs. As.)

| | |
|--|-----|
| El correo epistolar y el aviso de retorno. | 419 |
| El correo electrónico y el concepto de <i>No Repudio</i> | 420 |
| La casilla profesional y la casilla personal | 422 |
| La casilla profesional como dato filiatorio..... | 422 |
| Los servicios disponibles y los servicios necesarios..... | 424 |

Anexo 4 - Uniformar las formas y formar los uniformes

| | |
|--|-----|
| El peso del bronce | 431 |
| Idoneidad: capacitación vs. aceleración | 431 |
| Informe estructurado vs. estructura informal | 433 |
| Las contradicciones evidentes | 433 |

Anexo 5 - Contradicciones judiciales

| | |
|--|-----|
| Reflexión doctrinaria | 441 |
| El problema subjetivo..... | 445 |
| La "vulnerabilidad" ante la copia ilegítima (e ilegal) | 445 |
| La acción penal en manos del Estado | 447 |

Anexo 6 - Modelos

| | |
|--|-----|
| Modelo de oficio a ISP | 449 |
| Modelo de ofrecimiento de prueba documental informática y pericial informático forense en subsidio | 450 |

Anexo 7 - La yapa

| | |
|---------------------------|-----|
| | 453 |
| BIBLIOGRAFÍA | 455 |