COMPUTACIÓN FORENSE

Maldonado Avellaneda Carlos Lain

5IV7

1. Introducción

En la era digital actual, la delincuencia y los incidentes de seguridad han encontrado un nuevo campo de acción en los entornos electrónicos donde se desarrollan gran parte de nuestras actividades. La Computación Forense, también conocida como Informática Forense, emerge como una disciplina científica crucial para investigar y resolver estos incidentes. Su objetivo no se limita a encontrar al responsable de un cibercrimen, sino que también abarca la resolución de casos de fraude corporativo, robo de información e incluso delitos tradicionales en los que la evidencia digital es fundamental.

Este trabajo explora en profundidad los fundamentos, metodologías, herramientas y el perfil técnico necesarios en este demandado campo.

2. ¿Qué es la Computación Forense?

2.1. Definición y Objetivos Fundamentales

La Computación Forense es la aplicación de técnicas científicas y analíticas para **identificar, preservar, analizar y presentar evidencia digital** de manera que sea admisible en un proceso legal. No se trata solo de "recuperar datos", sino de seguir un protocolo estricto que garantice la integridad y la cadena de custodia de la prueba.

Sus objetivos principales son:

- **Identificar evidencias:** Determinar qué datos son relevantes para la investigación.
- **Preservar la integridad:** Asegurar que la evidencia original no sea alterada.
- **Analizar la información:** Extraer, reconstruir e interpretar los datos obtenidos.
- **Documentar el proceso:** Crear un registro detallado de todas las acciones realizadas.
- **Presentar hallazgos:** Elaborar un informe claro para una audiencia no técnica, como jueces o directivos.

2.2. Principios Básicos de la Evidencia Digital

La evidencia digital es frágil, por lo que debe regirse por principios universales para ser válida.

- **Integridad:** La evidencia debe permanecer inalterada. Se utilizan funciones hash (como MD5 o SHA-256) para demostrar que una copia forense es idéntica al original.
- **Cadena de Custodia:** Es un registro documentado de todas las personas que han tenido acceso a la evidencia. Una ruptura en esta cadena puede invalidar la prueba.
- **Autenticidad:** Se debe poder demostrar que la evidencia es lo que se afirma que es y que proviene de la fuente declarada.
- **Fiabilidad:** Los métodos y herramientas utilizados deben ser aceptados por la comunidad científica y forense.

3. Aplicaciones de la Computación Forense

Esta disciplina tiene aplicaciones en múltiples sectores:

- **Investigación Criminal:**
    - **Ciberdelitos:** Se utiliza para investigar hackeos, fraudes en línea, robo de identidad y distribución de malware.
    - **Delitos Tradicionales:** Los dispositivos digitales contienen evidencias clave (comunicaciones, ubicaciones) en casos de homicidio, narcotráfico o terrorismo.
- **Cumplimiento Normativo y Auditoría:**
    - Las empresas usan técnicas forenses para asegurar el cumplimiento de regulaciones de protección de datos como el RGPD en Europa o la LFPDPPP en México. Permiten investigar brechas de datos y accesos no autorizados.

- **Sector Corporativo e Investigaciones Internas:**
    - **Respuesta a Incidentes:** Se determina el origen y alcance de un ciberataque para contenerlo.
    - **Investigaciones de Empleados:** Se utiliza para detectar fugas de información, espionaje industrial o uso indebido de recursos.
    - **Protección de la Propiedad Intelectual:** Sirve para investigar el robo de secretos comerciales o proyectos de I+D.
- **Litigios Civiles:**
    - La evidencia digital como correos electrónicos o documentos es a menudo la pieza central en disputas entre empresas o individuos. La forense digital recupera y autentica estos datos.
- **Inteligencia y Contrainteligencia:**
    - Las agencias gubernamentales utilizan estas técnicas para analizar actividades de grupos hostiles y proteger la infraestructura crítica nacional.

4. Fases del Proceso Forense Digital (Versión Extendida)

El proceso forense sigue una metodología estructurada, a menudo denominada "Ciclo de Vida Forense", para garantizar que el tratamiento de la evidencia sea riguroso, defendible y repetible. Cada fase se basa en la anterior y es fundamental para el éxito de la investigación.

4.1. Identificación

Es la fase inicial y estratégica. Aquí no solo se reconoce la existencia de un incidente, sino que se planifica toda la respuesta. Las acciones clave incluyen:

- **Definición del Alcance:** Se establece qué se investiga, los objetivos y los límites. Por ejemplo, ¿se investiga solo a un empleado o a todo un departamento? ¿El periodo de tiempo a investigar es de una semana o un año?
- **Identificación de Fuentes de Evidencia:** Se crea un inventario de todos los posibles dispositivos que puedan contener información relevante. Esto incluye ordenadores de escritorio, portátiles, servidores, teléfonos móviles, tabletas, dispositivos de almacenamiento externo (USB, discos duros), dispositivos de red (routers, switches) e incluso dispositivos IoT (cámaras de seguridad, asistentes inteligentes).
- **Evaluación de la Volatilidad:** Se prioriza la recolección de la evidencia más volátil. La información en la memoria RAM, por ejemplo, se pierde en cuanto el dispositivo se apaga, por lo que su captura debe ser inmediata si es relevante para el caso.

4.2. Preservación y Adquisición

Esta es la fase más crítica y delicada desde el punto de vista técnico, ya que su objetivo es recolectar la evidencia sin alterarla.

- **Aislamiento:** El dispositivo o sistema se aísla de la red para evitar la contaminación de datos (por ejemplo, que un malware continúe borrando archivos) o el acceso remoto no autorizado.
- **Adquisición Forense ("Imaging"):** Nunca se trabaja sobre la evidencia original. En su lugar, se crea una copia exacta, bit a bit, del medio de almacenamiento, conocida como "imagen forense". Para ello, se utilizan **bloqueadores de escritura (write-blockers)**, que son dispositivos de hardware que impiden cualquier operación de escritura en el disco original, garantizando que el proceso de copia no lo modifique de ninguna manera.

- **Verificación de Integridad:** Inmediatamente después de crear la imagen forense, se calcula su "hash" (una firma digital única usando algoritmos como SHA-256). Este mismo cálculo se realiza sobre el disco original. Si ambos hashes coinciden, se demuestra matemáticamente que la copia es una réplica perfecta. Este paso es fundamental para la admisibilidad de la prueba.

4.3. Análisis

Con la copia forense segura en un entorno de laboratorio controlado, el investigador comienza a examinarla para encontrar las "huellas digitales" del incidente.

- **Recuperación de Datos:** Se utilizan técnicas para recuperar archivos que han sido eliminados por el usuario, ya que en la mayoría de los sistemas operativos "eliminar" solo marca el espacio como disponible, pero no borra los datos inmediatamente.
- **Análisis de Artefactos del Sistema:** Se examinan los archivos generados por el sistema operativo, que actúan como un diario de la actividad del usuario. Esto incluye el análisis del registro de Windows (para ver programas instalados, dispositivos USB conectados, etc.), los logs del sistema, el historial de navegación web, archivos temporales y la papelera de reciclaje.
- **Búsqueda de Palabras Clave:** Se realizan búsquedas exhaustivas en todo el disco (incluyendo el espacio no asignado) de términos relevantes para el caso, como nombres, números de cuenta, frases específicas, etc.
- **Análisis de la Línea de Tiempo (Timeline):** Esta es una de las técnicas más poderosas. Se extraen las marcas de tiempo (fecha y hora de creación, modificación y acceso) de miles de archivos y registros del sistema. Luego, se ordenan cronológicamente para reconstruir una secuencia detallada de los eventos: qué hizo el usuario, cuándo lo hizo y en qué orden.
- **Análisis de Memoria Volátil (RAM):** Si se logró capturar la memoria RAM, su análisis puede revelar información crucial que no se guarda en el disco, como procesos en ejecución, conexiones de red activas, contraseñas, claves de cifrado y fragmentos de conversaciones o documentos que no fueron guardados.

4.4. Documentación y Presentación

El trabajo técnico no sirve de nada si no se puede comunicar de forma efectiva.

- **Documentación Continua:** Cada paso, herramienta utilizada y decisión tomada durante el proceso debe ser meticulosamente documentado para asegurar la repetibilidad y la defensa del método.
- **Informe Forense:** Se elabora un informe final que recopila todos los hallazgos[47]. Este documento debe ser claro, objetivo y estar libre de tecnicismos innecesarios, explicando qué se encontró, dónde se encontró y qué significa en el contexto de la investigación.
- **Presentación en Juicio:** Si el caso llega a los tribunales, el perito forense puede ser llamado a declarar como testigo experto para explicar sus hallazgos, defender su metodología y responder a las preguntas de abogados y jueces.

5. Herramientas de Computación Forense

Existe una amplia gama de herramientas para cada fase del proceso.

- **Herramientas de Adquisición:**
    - **FTK Imager:** Popular herramienta gratuita para crear y visualizar imágenes forenses.
    - **dd (y variantes como dcfldd):** Comando potente en GNU/Linux para realizar copias bit a bit.
    - **Guymager:** Herramienta de código abierto con interfaz gráfica para adquisición en Linux.
- **Herramientas de Análisis:**
    - **Autopsy / The Sleuth Kit (TSK):** Suite de código abierto ideal para principiantes y profesionales que permite análisis de archivos, registros y líneas de tiempo.
    - **FTK (Forensic Toolkit):** Suite comercial muy completa, conocida por su potente motor de búsqueda.
    - **EnCase:** Una de las suites comerciales más respetadas en la industria, utilizada por agencias gubernamentales.

- **Suites Forenses Integrales:**
    - **X-Ways Forensics:** Herramienta comercial muy eficiente y valorada por expertos por su velocidad.
    - **Cellebrite UFED:** Líder en el mercado de forense móvil, capaz de extraer datos de una gran variedad de smartphones.
- **Herramientas de Análisis de Red y Memoria RAM:**
    - **Wireshark:** El estándar para el análisis de tráfico de red[59].
    - **Volatility Framework:** Herramienta de código abierto imprescindible para el análisis forense de la memoria RAM, permitiendo extraer procesos, contraseñas y rastros de malware.

6. Nivel Técnico Requerido para Aprender sus Técnicas

La Computación Forense no es para principiantes en informática, requiere una base sólida y aprendizaje continuo.

- **Conocimientos Fundamentales:**
    - **Sistemas Operativos:** Conocimiento profundo de la arquitectura y sistemas de archivos (NTFS, APFS, ext4) de Windows, Linux y macOS.
    - **Redes de Computadoras:** Comprensión de protocolos TCP/IP y conceptos de tráfico de red.
    - **Arquitectura de Computadoras:** Entender el funcionamiento de discos duros y memoria RAM.
    - **Programación y Scripting:** Conocer Python, PowerShell o Bash es invaluable para automatizar tareas.
- **Conocimientos Especializados:**
    - **Ciberseguridad:** Entender las tácticas y técnicas de los atacantes es crucial.
    - **Metodologías Forenses:** Aprendizaje de estándares internacionales como ISO 27037.
    - **Análisis de Malware, Forense en la Nube y Dispositivos Móviles:** Áreas de alta especialización y demanda.

- **Habilidades Blandas:**
    - **Pensamiento Analítico y Metódico:** La paciencia y la atención al detalle son clave.
    - **Curiosidad e Ingenio:** Capacidad de pensar de manera creativa para encontrar evidencias ocultas.
    - **Comunicación:** Habilidad para traducir hallazgos técnicos en un lenguaje claro.
    - **Ética y Profesionalismo:** La integridad es la base de la profesión al manejar información sensible.

7.Nivel Técnico Requerido para Aprender sus Técnicas

La computación forense es una disciplina de alta especialización que se sitúa en la intersección de la informática, la ciberseguridad y el derecho. No es un campo para principiantes absolutos, ya que exige una base técnica sólida y, sobre todo, un compromiso ineludible con el aprendizaje continuo para mantenerse al día con la evolución tecnológica.

7.1. Conocimientos Fundamentales

Estos son los pilares sobre los que se construye la pericia de un analista forense:

- **Sistemas Operativos:** Es indispensable un conocimiento profundo y a bajo nivel de los sistemas operativos más comunes (Windows, Linux y macOS). Esto va más allá del uso como usuario. El analista debe entender:
    - **Sistemas de Archivos:** Cómo NTFS (Windows), APFS (macOS) o ext4 (Linux) gestionan la información, cómo almacenan los metadatos de los archivos (fechas de creación, modificación, acceso) y, fundamentalmente, cómo gestionan el borrado de archivos para poder recuperarlos.
    - **Estructuras Internas:** En Windows, el Registro es una mina de oro de evidencia que documenta casi toda la actividad del usuario: programas ejecutados, dispositivos USB conectados, redes Wi-Fi utilizadas y mucho más.

- **Redes de Computadoras:** Se debe tener una comprensión sólida de los fundamentos de la comunicación en red. Esto es crucial para analizar el tráfico de red capturado (con herramientas como Wireshark) y poder reconstruir sesiones, identificar la fuente de un ataque, detectar la exfiltración de datos o seguir el rastro de comunicaciones maliciosas. Es vital entender el modelo OSI, los protocolos TCP/IP, y servicios como DNS y DHCP.
- **Arquitectura de Computadoras:** El conocimiento del hardware es fundamental para el proceso de adquisición. Entender cómo funcionan los discos duros (HDD/SSD) y la memoria RAM permite al analista saber dónde buscar la evidencia y cómo preservarla sin alterarla.
- **Programación y Scripting:** Aunque no es obligatorio ser un desarrollador de software, tener habilidades de scripting es una ventaja competitiva enorme. Lenguajes como Python, PowerShell o Bash permiten al analista automatizar tareas repetitivas, analizar formatos de logs no convencionales o crear herramientas personalizadas para resolver problemas específicos que las suites comerciales no cubren.

7.2. Conocimientos Especializados

Sobre la base fundamental, se construyen las especializaciones:

- **Ciberseguridad:** Un analista forense debe pensar como un atacante para poder encontrar sus rastros. Entender las Tácticas, Técnicas y Procedimientos (TTPs) de los ciberdelincuentes le da una hoja de ruta sobre qué tipo de evidencia buscar y dónde.
- **Análisis de Malware:** La habilidad para realizar ingeniería inversa básica en software malicioso permite determinar su comportamiento: cómo infectó el sistema, si se comunica con un servidor externo, qué información roba o qué cambios realiza en el sistema.
- **Forense en la Nube y Dispositivos Móviles:** Estas son dos de las áreas de mayor crecimiento y demanda. Requieren conocimientos específicos sobre cómo se almacena la información en servicios como AWS o Azure, y las particularidades de los sistemas de archivos de iOS y Android.

7.3. Habilidades Blandas y Formación Continua

Las habilidades técnicas por sí solas no son suficientes:

- **Pensamiento Analítico y Metódico:** El analista debe ser extremadamente meticuloso y paciente. La atención al detalle es crucial, ya que una sola pieza de evidencia pasada por alto puede cambiar el resultado de un caso.
- **Ética y Profesionalismo:** Se trabaja con información altamente sensible y confidencial. La integridad personal y profesional es la base de la credibilidad del perito. Cualquier duda sobre su ética puede invalidar su testimonio y su trabajo.
- **Comunicación Escrita y Verbal:** Es una de las habilidades más importantes. El analista debe ser capaz de "traducir" sus complejos hallazgos técnicos a un lenguaje claro, conciso y comprensible para audiencias no técnicas como abogados, jueces, jurados o directivos de una empresa.

El camino de aprendizaje a menudo se valida a través de certificaciones reconocidas en la industria, comenzando por las fundamentales como GCFA (GIAC Certified Forensic Analyst) y avanzando hacia otras más especializadas.

8. Conclusión

La Computación Forense es un pilar en la lucha contra el cibercrimen, combinando rigor científico con pericia técnica y una ética inquebrantable. Su correcta aplicación asegura que la evidencia digital sea utilizada de manera válida en procesos legales y administrativos. Con el avance de tecnologías como la nube, el IoT y la inteligencia artificial, el campo enfrenta nuevos desafíos, convirtiéndola en un área de gran proyección futura y en constante evolución.

Bibliografía

- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
- Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.
- Maras, M. H. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones & Bartlett Learning.
- National Institute of Standards and Technology (NIST). Computer Forensic Tool Testing (CFTT) Project.
- Volatility Foundation. Documentación Oficial del Framework Volatility.
- The Sleuth Kit. Wiki y Documentación de Autopsy