Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 6:

Respuesta a Incidentes y Análisis Forense Digital

Sesión 2:

Fundamentos del análisis forense digital

OBJETIVO DE LA SESIÓN:

Conocer los principios básicos del análisis forense digital, los tipos de evidencia digital y cómo recolectarla sin alterarla.

¿Qué es el análisis forense digital?

Es el proceso de **identificar, preservar, analizar y presentar evidencia digital** para apoyar la investigación de un incidente o delito informático.

Principios clave

- **Integridad:** No alterar la evidencia
- **Cadena de custodia:** Registrar quién accede, cuándo y cómo
- **Trazabilidad:** Todo debe poder replicarse

Tipos de evidencia digital

Evidencia	Ejemplo
Archivos	Documentos eliminados o alterados
Logs de eventos	Historial de accesos o errores
Metadatos	Fecha de creación o modificación
Tráfico de red	Capturas de paquetes sospechosos

Herramientas básicas

FTK Imager:
Creación de imágenes forenses

Autopsy:
Análisis de disco

Wireshark:
Captura y análisis de tráfico de red

Wireshark – Analizador de Tráfico de Red

Es un analizador de protocolos de red de código abierto y gratuito, utilizado para capturar y analizar el tráfico de datos en una red, permitiendo observar qué ocurre en ella a un nivel detallado.

Para que sirve?

- Detectar intrusiones y tráfico sospechoso.
- Analizar protocolos (HTTP, DNS, TLS, etc.).
- Ver intentos de sniffing o man-in-the-middle.

Importancia

- Permite visualizar qué pasa en la red en tiempo real.
- Fundamental para responder a incidentes de seguridad.

FTK Imager – Preservación de Evidencias

FTK Imager es una herramienta forense digital gratuita que permite a los investigadores crear imágenes forenses de dispositivos de almacenamiento (como discos duros, USBs, CDs/DVDs) sin alterar la evidencia original.

Para que sirve?

- Generar imágenes bit a bit de dispositivos de almacenamiento.
- Verificar integridad con hashes (MD5, SHA256).
- Exportar archivos/carpetas específicos..

Importancia

- Garantiza que la evidencia se preserve sin alterarla.
- Cumple con el principio de cadena de custodia digital.

Autopsy – Análisis Forense Digital

Plataforma de análisis forense que permite a los investigadores examinar y extraer datos de discos y dispositivos de almacenamiento

Para que sirve?

- Recuperar archivos borrados.
- Revisar historial de navegación, correos y documentos.
- Construir líneas de tiempo de actividad.

Importancia

- Permite a investigadores reconstruir qué ocurrió en un sistema.
- Genera reportes detallados para uso técnico o legal.


Establecer políticas claras y roles definidos
Mantener la calma y seguir los procedimientos establecidos
Priorizar la contención rápida, sin comprometer evidencias
Recolectar y preservar evidencias digitales
Documentar el incidente de forma estructurada
Comunicación efectiva y controlada
Recuperación planificada y monitoreo post-incidente
Realizar lecciones aprendidas y mejora continua
Capacitar regularmente al personal
Probar y simular escenarios regularmente
Buenas prácticas

Buenas prácticas

1. Establecer políticas claras y roles definidos

- **Contar con un plan formal de respuesta a incidentes (IRP)** que incluya procedimientos, herramientas, responsables y mecanismos de escalamiento.
- Designar un **equipo de respuesta a incidentes (IRT/CSIRT)**, con roles claros: coordinador general, analista técnico, vocero, apoyo legal, etc.
- Incorporar la **gestión de incidentes en el SGSI** si la organización aplica ISO/IEC 27001.

Ejemplo práctico:

En una universidad, el equipo TI define que ante cualquier incidente reportado (ej. sospecha de malware), el analista de seguridad evalúa el evento y reporta al responsable de infraestructura, quien decide si aislar o no el equipo afectado.

Buenas prácticas

2. Mantener la calma y seguir los procedimientos establecidos

- No improvisar ni actuar por impulso.
- Evitar apagar sistemas o desconectarlos sin análisis (puede alterar evidencia).
- Registrar cada acción tomada con fecha y hora: esto ayuda a reconstruir lo ocurrido y mantener la cadena de custodia.

Ejemplo práctico:

Ante una intrusión sospechosa, un técnico no debe borrar los archivos infectados inmediatamente. Primero debe aislar el sistema, guardar logs y tomar una imagen del disco si es posible.

Buenas prácticas

3. Priorizar la contención rápida, sin comprometer evidencias

- Aislar los sistemas comprometidos de la red para evitar la propagación.
- Usar técnicas de contención adecuadas: cortar acceso remoto, cambiar credenciales comprometidas, aplicar reglas temporales en firewalls.
- **Evitar "limpiar" el sistema antes de recolectar evidencias** si hay posibilidad de análisis forense.

Consejo:

En entornos críticos, como hospitales o bancos, se recomienda tener planes de contención rápida tipo "playbooks" para malware, accesos no autorizados, ataques DDoS, etc.

Buenas prácticas

4. Recolectar y preservar evidencias digitales

- Capturar logs, capturas de pantalla, volcados de memoria o imágenes de disco.
- Registrar el nombre del archivo, ubicación, hora de creación y modificación.
- Usar herramientas confiables (ej. FTK Imager, Autopsy, WinLogBeat, Wireshark) para preservar la integridad.

Importante:
Toda evidencia debe ser tratada bajo principios forenses (no modificarla) y con cadena de custodia si puede usarse legalmente.

Buenas prácticas

5. Documentar el incidente de forma estructurada

Una buena práctica es llenar una **bitácora de incidente**, que incluya:

Elemento	Descripción ejemplo
Fecha/hora de detección	15/07/2025 10:32
Medio de detección	Antivirus alertó sobre Troyano en carpeta C:\
Usuario afectado	j.rodriguez@institucion.edu.co
Dispositivo/servidor comprometido	Equipo portátil HP, IP interna 192.168.1.100
Acciones tomadas	Aislamiento, recolección de logs, escaneo
Responsable	Analista Seguridad – Andrés Suárez

Buenas prácticas

6. Comunicación efectiva y controlada

- Informar rápidamente a los responsables designados.
- Evitar rumores o desinformación interna.
- Si hay afectación externa (clientes, usuarios, medios), tener mensajes preparados y aprobados para evitar errores o filtraciones.

Ejemplo:
Si se filtra información de usuarios, se debe tener listo un modelo de notificación responsable, acorde con normativas como la Ley de Protección de Datos.

Buenas prácticas

7. Recuperación planificada y monitoreo post-incidente

- Restaurar sistemas desde respaldos limpios y verificar su integridad antes de volver a producción.
- Cambiar contraseñas, revisar reglas de firewall, actualizar software.
- Monitorear durante días o semanas los indicadores de compromiso (IoCs) relacionados.

Consejo:
Incluir **“monitoreo intensivo”** como parte de los procedimientos post-incidente es esencial para detectar persistencia del atacante o reinfección.

Buenas prácticas

8. Realizar lecciones aprendidas y mejora continua

Después de cada incidente:

- Hacer un informe de cierre del incidente con hallazgos, causas raíz, medidas tomadas y recomendaciones.
- Reunir al equipo para hacer una **retroalimentación interna (postmortem).**
- Actualizar los procedimientos, controles y realizar ajustes técnicos si es necesario.

Ejemplo:

Tras un incidente de phishing, se refuerza la capacitación en ingeniería social, se implementa MFA y se ajustan reglas del servidor de correo.

Buenas prácticas

9. Capacitar regularmente al personal

Capacitar al personal TI y no-TI en:

- Identificación de incidentes
- Reporte inmediato
- Uso de canales oficiales de soporte

Hacer campañas de concienciación (phishing simulado, afiches, cápsulas informativas)

Buenas prácticas

10. Probar y simular escenarios regularmente

- Realizar simulacros de respuesta a incidentes al menos 1 vez al año.
- Probar distintos tipos de incidentes: malware, fuga de información, error humano, etc.
- Evaluar la velocidad, calidad de respuesta y documentación del equipo.

Ejercicio sugerido:
Simular que un colaborador abre un archivo infectado desde una USB. Evaluar cómo actúa el equipo: ¿se documenta?, ¿se aísla?, ¿se informa correctamente?, ¿se preserva la evidencia?

Ejercicio 1: Análisis guiado de evidencia digital

Se ha detectado actividad sospechosa en un equipo institucional. Se obtiene un archivo de log (registro de eventos) que debe ser analizado. Los estudiantes deben:

1. Revisar los metadatos de un documento
2. Identificar accesos sospechosos en un log
3. Sugerir hipótesis sobre lo ocurrido

Archivo .LOG

2025-07-15 08:13:45 - INFO - Usuario: carlos - Inicio de sesión exitoso
2025-07-15 08:14:02 - WARNING - Usuario: carlos - Acceso a carpeta restringida: \servidor\finanzas
2025-07-15 08:14:55 - ERROR - Usuario: carlos - Intento fallido de lectura de archivo confidencial
2025-07-15 08:15:10 - INFO - Usuario: carlos - Cierre de sesión
2025-07-15 08:30:22 - INFO - Usuario: juan - Inicio de sesión exitoso
2025-07-15 08:31:17 - INFO - Usuario: juan - Acceso normal a \servidor\documentos
2025-07-15 08:45:05 - ERROR - Usuario: carlos - Intento de acceso remoto desde IP desconocida: 192.168.45.22
2025-07-15 08:46:00 - CRITICAL - Usuario: carlos - Múltiples intentos fallidos de autenticación detectados

Análisis de Evidencia Digital

1. Nombre del analista:

Luis Fernando Salas

2. Fecha y hora del análisis:

04 de septiembre de 2025 – 21:00

3. Descripción general del incidente:

Se analizaron registros de seguridad de un servidor institucional. Se identificaron actividades sospechosas asociadas al usuario “carlos”, que incluyen accesos no autorizados a carpetas restringidas, intentos fallidos de lectura de archivos confidenciales y múltiples intentos de autenticación desde una IP no reconocida.

4. Tipo de evidencia analizada (log, captura de pantalla, archivo, etc.):

Archivo de log del sistema (registro de accesos de usuarios).

5. Herramienta utilizada para visualizar la evidencia:

Editor de texto avanzado (Notepad++)

6. Eventos o hallazgos relevantes (describir con hora, usuario, acción):

08:13:45 – Usuario carlos: inicio de sesión exitoso.
08:14:02 – Usuario carlos: intento de acceso a carpeta restringida \servidor\finanzas.
08:14:55 – Usuario carlos: intento fallido de lectura de archivo confidencial.
08:15:10 – Usuario carlos: cierre de sesión.
08:30:22 – Usuario juan: inicio de sesión exitoso.
08:31:17 – Usuario juan: acceso normal a \servidor\documentos.
08:45:05 – Usuario carlos: intento de acceso remoto desde IP desconocida 192.168.45.22.
08:46:00 – Usuario carlos: múltiples intentos fallidos de autenticación (actividad crítica).

7. Hipótesis sobre lo ocurrido:

- El usuario carlos podría haber sido víctima de compromiso de credenciales.
- Un atacante usó las credenciales para intentar acceder a áreas sensibles (\finanzas).
- Tras el cierre de sesión, se detectaron accesos remotos desde una IP desconocida, lo que sugiere uso indebido de su cuenta.
- Podría tratarse de un intento de escalamiento de privilegios o exfiltración de información.

8. Recomendaciones o acciones sugeridas:

- Bloquear temporalmente la cuenta carlos y forzar cambio de contraseña.
- Revisar origen de la IP 192.168.45.22 para identificar si corresponde a un dispositivo interno comprometido.
- Implementar autenticación multifactor para usuarios con acceso a recursos críticos.
- Revisar si hubo modificaciones o descargas en la carpeta \servidor\finanzas.
- Configurar alertas tempranas para accesos no autorizados y múltiples intentos de autenticación.
- Documentar el incidente y notificar al equipo de seguridad institucional.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *Autopsy. (s/f). Autopsy.com. Recuperado el 4 de septiembre de 2025, de https://www.autopsy.com/*
6. *Chapter 1. Introduction to WireShark. (s/f). Wireshark.org. Recuperado el 4 de septiembre de 2025, de https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html*
7. *Get Kali. (s/f). Kali Linux. Recuperado el 4 de septiembre de 2025, de https://www.kali.org/get-kali/*
8. *Suhartono, J. (s/f). FTK IMAGER IN DIGITAL FORENSIC. School of Information Systems. Recuperado el 4 de septiembre de 2025, de https://sis.binus.ac.id/2023/09/20/ftk-imager-in-digital-forensic/*
9. *VirtualBox. (s/f). Virtualbox.org. Recuperado el 4 de septiembre de 2025, de https://www.virtualbox.org/wiki/Downloads*