Método de Extracción:

Protocolo SCP y Túneles SSH

- **Fundamento Técnico:** Se seleccionó **SCP (Secure Copy Protocol)** debido a que opera sobre la capa de **SSH (Secure Shell)**. Esto garantiza que todos los datos transferidos desde la IP víctima `192.168.1.165` hacia la estación de análisis Kali Linux viajen a través de un túnel cifrado (normalmente utilizando el algoritmo AES-256).
- **Integridad en el Transporte:** A diferencia del FTP estándar, SCP utiliza mecanismos de verificación para asegurar que los paquetes de datos lleguen íntegros. Durante la sesión documentada en las capturas, el protocolo asegura que la estructura de los archivos `.txt` y `.ph` no sufra variaciones binarias durante el salto de red.
- **Uso Forense:** El comando ejecutado (`scp -r ...`) permitió la copia recursiva, manteniendo la organización de los directorios temporales creados en `/tmp/`, facilitando así una reconstrucción lógica del entorno atacado.

---

2. Preservación: Aplicación del Principio de Inmutabilidad

Una vez que los archivos fueron depositados en la estación de trabajo Kali Linux, el siguiente paso metodológico fue garantizar su **inmutabilidad**.

- **Implementación de Permisos:** Se ejecutó el comando `chmod 444` sobre el directorio de evidencias. En entornos Linux, esto elimina los privilegios de escritura (`-w-`) para todos los usuarios, incluido el analista.
- **Prevención de Alteraciones:** Esta medida previene cambios accidentales en el contenido de los archivos (por ejemplo, al abrir el `historial.txt` para lectura) o alteraciones en los metadatos de tiempo del sistema de archivos. Al "congelar" el estado de los archivos, se asegura que el análisis posterior sea un reflejo exacto del momento de la intrusión.

3. Cadena de Custodia mediante Verificación Hash (SHA-256)

La cadena de custodia se sustenta en la evidencia matemática. Para probar que los archivos analizados son los originales, se procedió a la generación de firmas digitales únicas.

- **Algoritmo SHA-256:** Se seleccionó el estándar **SHA-256** por su alta resistencia a colisiones. Como se observa en la captura `image_4c2b6b.png`, cada archivo posee una firma hexadecimal única.
- **Garantía de No Manipulación:** Cualquier intento de modificar el archivo (incluso añadir un espacio en blanco) invalidaría el Hash. Esta transparencia permite que el informe sea auditable por terceros, quienes pueden verificar los resultados de forma independiente.

Archivo	Hash SHA-256 (Verificación de Integridad)
historial.txt	afa029904e7ad73b43439aef0baae6d6aa51f87a274092c42021eabbdaa6ccf5
log_sistema.txt	06a125d75ec79c3e4b067d66b2dbbb5acdb400063b48eda944b761f7377de012
mariadb_config.txt	88e19ead91d927157090cb24de057f3a8f7af8edb768addb0c4f371d8d9fed9a
wp-config_audit.ph	d30e34c55db2c0652642fc235262fba55469e86af45f17acfc5b28448950f19b