VERIFICACIÓN DE LA INTEGRIDAD DE ARCHIVOS CON CHECKSUMS

Trabajo realizado por:

Patrice Rojas Pérez
15/10/2024
2ºASIR

Verificación de la Integridad de Archivos con Checksums

Objetivo:

En esta práctica, vas a aprender a utilizar herramientas para generar checksums y verificar la integridad de un archivo. Comprobarás cómo pequeñas modificaciones en un archivo afectan al resultado del checksum, lo que permite detectar alteraciones no deseadas o corrupciones.

Descripción:

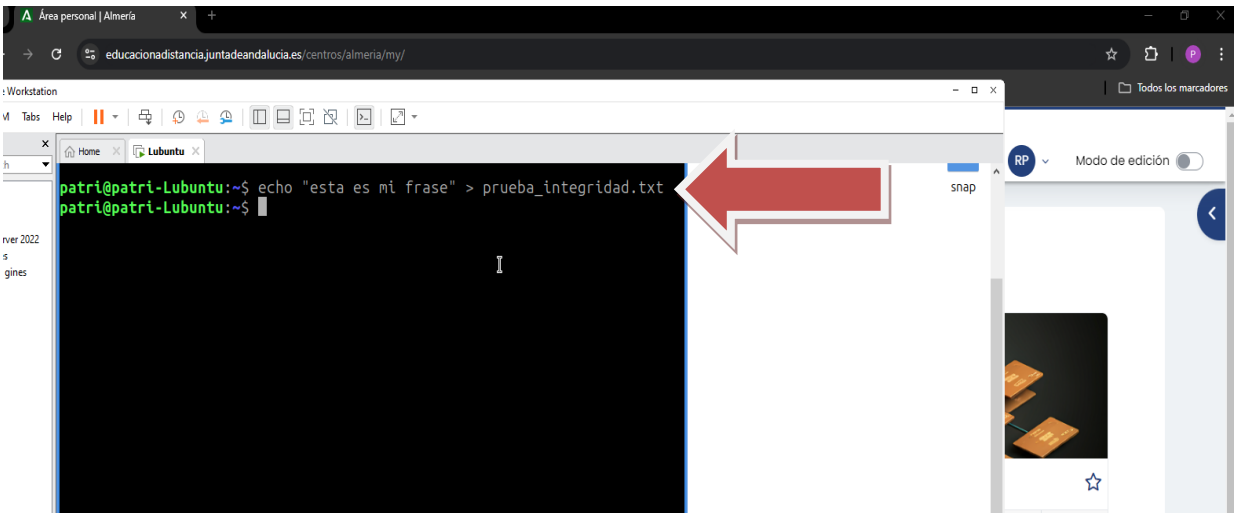
El checksum es una técnica que permite verificar si un archivo ha sido alterado o corrompido. Esto se logra generando una "huella digital" única del archivo a través de un algoritmo hash (como SHA-256 o MD5). En esta práctica, crearás un archivo, generarás su checksum, lo modificarás para corromperlo y compararás el checksum original con el nuevo.

Pasos a Seguir:

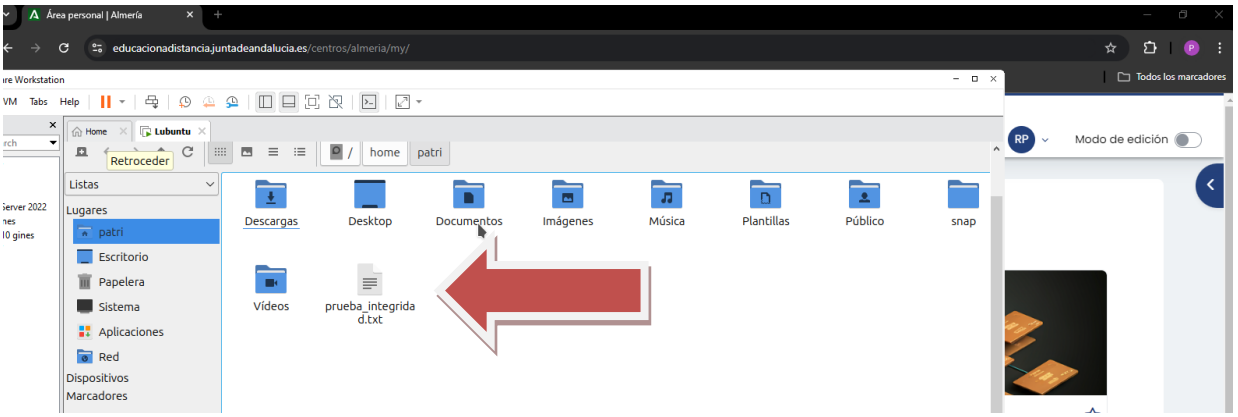
1. **Creación de un archivo de texto**:
   Crea un archivo de texto llamado prueba_integridad.txt que contenga una breve frase. Este archivo se utilizará para generar un checksum inicial.

   Para realizar este ejercicio, usaremos la maquina virtual de lubuntu y crearemos el archivo con el comando siguiente:

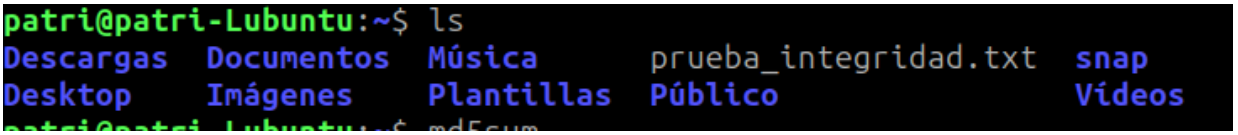
   echo "Esta es mi frase" > mi_archivo.txt



Una vez realizado el comando, nos aparece el archivo en nuestra carpeta.



Y si lo hacemos por la terminal, con el comando ls.

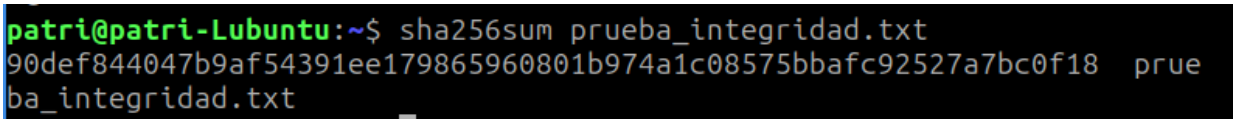


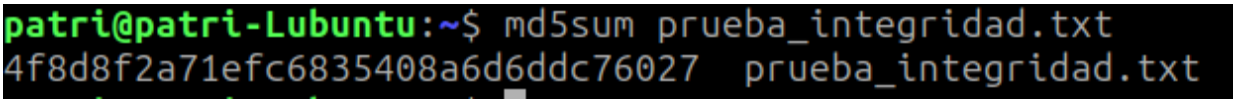
2. **Generación del checksum**:

- **En Windows, utiliza la herramienta CertUtil para generar el checksum del archivo.**
- **En Linux, utiliza el comando sha256sum o md5sum para generar el checksum. Anota el resultado del checksum en un documento.**

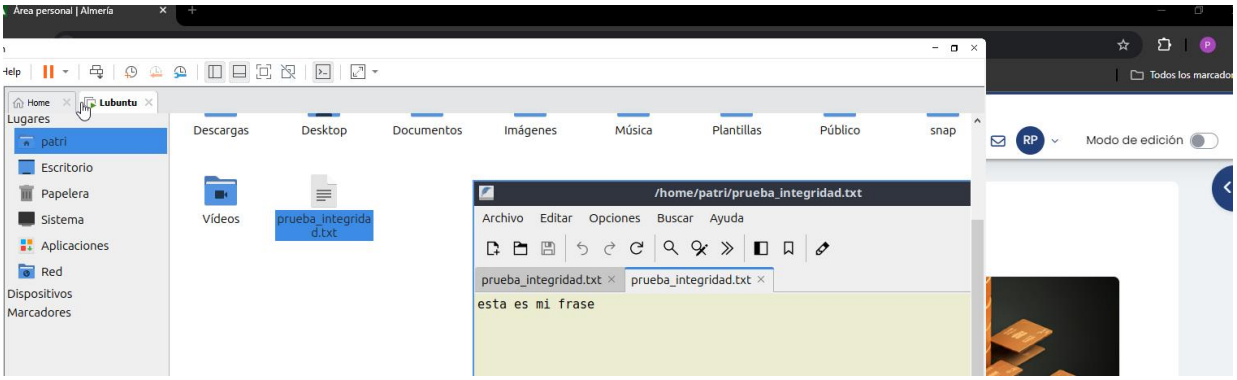
  Primero realizamos con el comando sha256sum y el nombre del archivo. Y luego con md5sum

  .

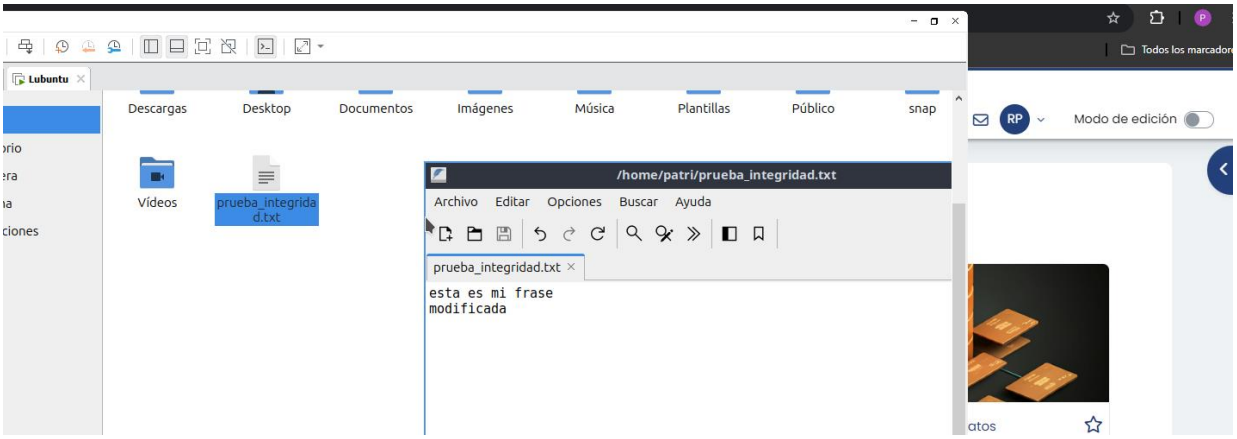




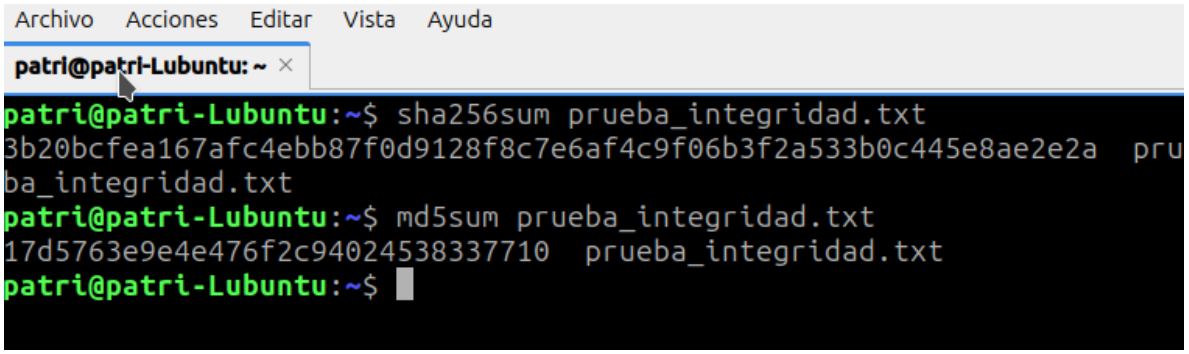
3. **Modificación del archivo:**
   Realiza una pequeña modificación en el archivo de texto, como agregar una nueva línea o modificar una palabra.
   Esta es mi archivo y frase original



Este es el archivo con la frase modificada



4. **Generación del nuevo checksum:**
   Después de modificar el archivo, genera nuevamente el checksum. Compara este nuevo valor con el checksum original y observa las diferencias.
   Realizamos de nuevo el checksum con el archivo modificado.



Los números han cambiado en las 2 pruebas y a que hemos modificado el archivo.

5. **Análisis:**
   Responde a las siguientes preguntas:

   - **¿Por qué crees que el checksum cambia cuando modificas el archivo?**
     Porque cada archivo es único y si se modifica o manipulan en archivo, cambia el número del checksum, y así sabemos si se ha modificado.

   - **¿Qué pasaría si solo cambias una letra del archivo?¿El cambio sería igualmente notable en el checksum?**
     Si modificas una sola letra del archivo, el checksum cambia también, y .así sabemos si han manipulado el documento.
     Si. Si el checksum calculado para un archivo descargado no coincide con el checksum proporcionado por la fuente original, significa que el archivo ha sido alterado en algún momento.

   - **¿Cómo podrías utilizar los checksums para garantizar que un archivo no ha sido alterado después de su transferencia en una red?**

     Si cambia el numero de checksum, podremos saber si se ha modificado o no.