# Practica 5.4: Funciones resumen (hash)

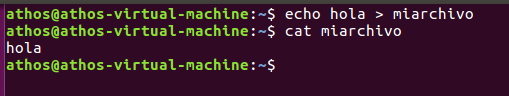
Los resúmenes (o hash) son un conjunto de bytes sacados con una función, la cual nos da siempre el mismo numero de caracteres. Siempre que utilicemos el mismo algoritmo sobre el mismo archivo, nos dará el mismo hash o resumen.

Esto es útil para comprobar si un archivo ha sido modificado desde que se “calculo” el hash correspondiente.

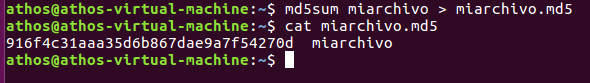
El calculo de hashes podemos hacerlo en cualquier sistema operativo. Para esto, hay muchas herramientas y diversos algoritmos. Vamos a ver como hacerlo en los sistemas operativos mas comunes, Linux y Windows.

## Linux

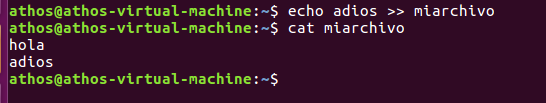
Creamos un archivo con algo de contenido



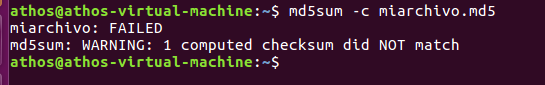
Ahora creamos el archivo md5, que nos servirá para comprobarlo posteriormente. Esto lo hacemos con la utilidad md5sum que podemos encontrar en prácticamente todas las distribuciones si no en todas.



Ahora modificamos el archivo



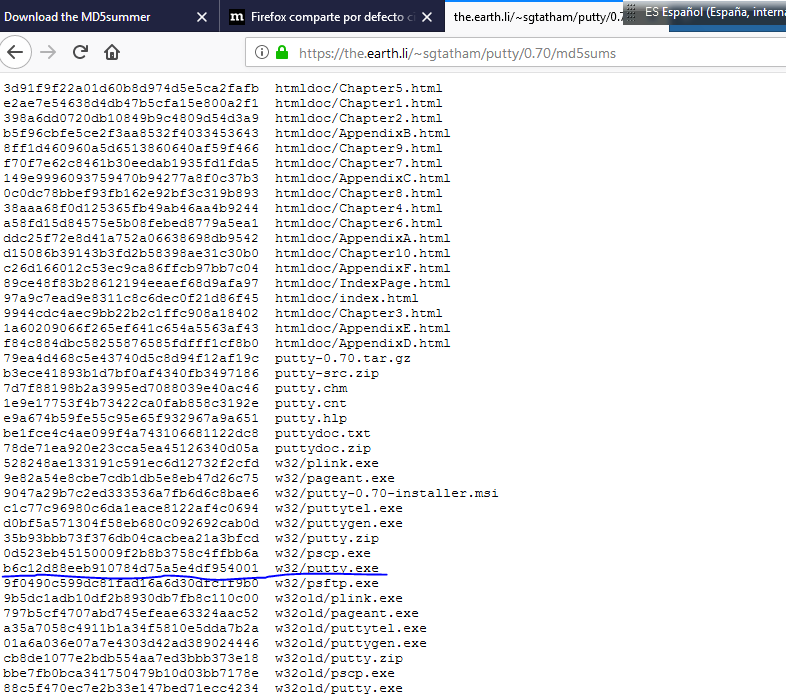
Y ahora solo queda comprobar la suma. Esto lo haremos añadiendo el parámetro –c y el archivo que se nos genero anteriormente cuando creamos el hash



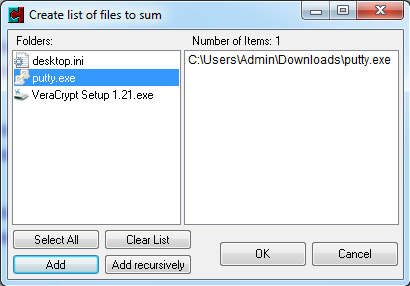
## Windows

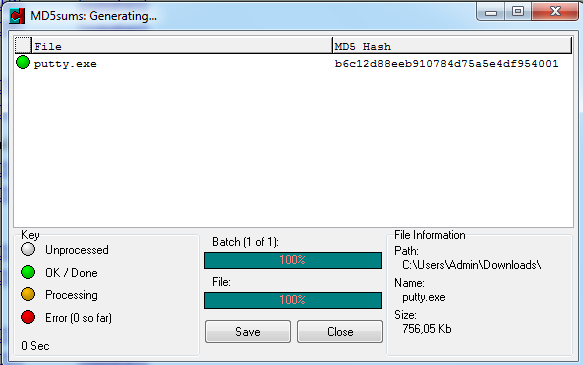
Vamos a descargarnos alguna utilidad para comprobar las firmas en md5, en este caso hemos descargado md5summer pero hay muchas mas.

Después de esto, vamos a la pagina de putty, y en la sección inferior hay un enlace a los resúmenes de todos los archivos que te puedes descargar desde su pagina. Vamos a descargar el archivo putty.exe, así que nos fijamos en su resumen



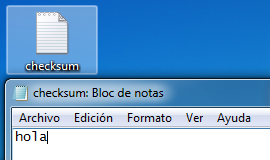
Ahora lo descargamos y lo comprobaremos con md5summer



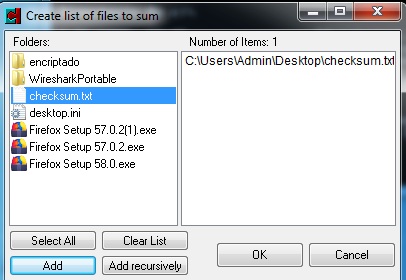


Como podemos ver, coincide. Esto quiere decir que el archivo no ha sido modificado (o que si algún atacante modifico el archivo, también modifico el hash de la web).

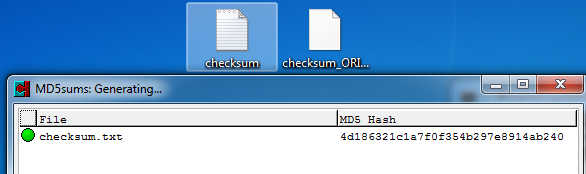
Ahora vamos a comprobarlo con un archivo nuestro. Creamos un archivo y metemos algún dato dentro.



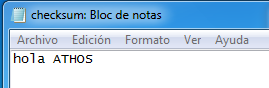
Ahora creamos el resumen.



Vemos que genera el resumen y lo guarda en un archivo.



Ahora vamos a modificar el archivo y volveremos a comprobar el checksum.



Y como vemos, md5summer nos avisa de que el checksum no coincide

