Cómo hallar la huella digital de un documento en formato electrónico

1.- Introducción

Debido a la gran cantidad de información que se necesita evaluar en la licitación de los servicios de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía para poder comparar y evaluar las distintas ofertas, se hace necesario disponer de los documentos de las ofertas en formato electrónico. Pero además, hay que poder garantizar en cada momento que la documentación entregada por la empresa licitadora permanece inalterada, es decir, garantizar la integridad y la autenticidad de los documentos en formato electrónico que componen la oferta.

En tanto se generaliza el uso de la *firma electrónica reconocida* por parte de las empresas licitadoras, se debe contar con una alternativa para conseguir el objetivo de disponer de los documentos de las ofertas en formato electrónico y que cumpla con los requisitos de integridad y autenticidad citados.

El proceso de firma electrónica de un documento en formato electrónico consiste en firmar electrónicamente la **huella digital (obtenida según una determinada función hash)** del fichero que contiene a dicho documento electrónico.

La **huella digital** del fichero que contiene un documento en formato electrónico es la secuencia de dígitos que se obtiene al aplicar una función 'hash' sobre aquel. Ésta tiene la propiedad de que a ficheros idénticos les corresponde una misma huella digital y a ficheros distintos les corresponden huellas digitales distintas.

Por lo tanto, si se dispone de una declaración, firmada de forma manuscrita, de las huellas digitales de todos los ficheros que contienen los documentos que componen la proposición de un licitador, se puede asegurar que los documentos en formato electrónico cumplen con el requisito de integridad siempre que mantengan la misma huella digital. El requisito de autenticidad vendrá garantizado de la misma forma que en los casos donde se cuenta con ofertas realizadas en documentos en papel.

2.- Entrega de proposiciones

Para la entrega de la documentación en formato electrónico, el algoritmo que se usará para la generación de la huella digital es (Secure Hash Algorithm, Algoritmo de Hash Seguro - 256). Existen herramientas de generación de la huella digital tanto en modo comando como en modo interfaz gráfica de usuario (GUI) para los distintos entornos (Windows, Mac y Linux entre otros). En esta guía se muestra cómo se calculan las huellas digitales según el algoritmo SHA-256 en estos tres entornos de usuario.

A la hora de obtener la huella digital de un fichero, es muy importante tener en cuenta lo que se indica más arriba: **siempre que se modifique el contenido del mismo se obtendrá una huella digital distinta**. Incluso si no se cambia el contenido pero se graba de nuevo el documento, el fichero que lo contiene puede sufrir modificaciones debido a la actualización de los metadatos propios del documento (fecha de última modificación, path del documento si éste se graba en otra carpeta,...) aunque el documento en si no haya cambiado.

Por esto, se recomienda que la obtención de la huella digital sea la última operación que se haga sobre los ficheros que contienen la documentación en formato electrónico de la oferta.

La propuesta de los licitadores, aparte de los documentos en formato electrónico que irían almacenados en un soporte de memoria (dispositivo de almacenamiento óptico o de memoria USB), se completaría con el documento declarativo (anexos correspondientes del PCAP), firmado de forma manuscrita, de las huellas

digitales según el algoritmo SHA-256 de cada uno de los ficheros que contienen los documentos en formato electrónico que componen la propuesta.

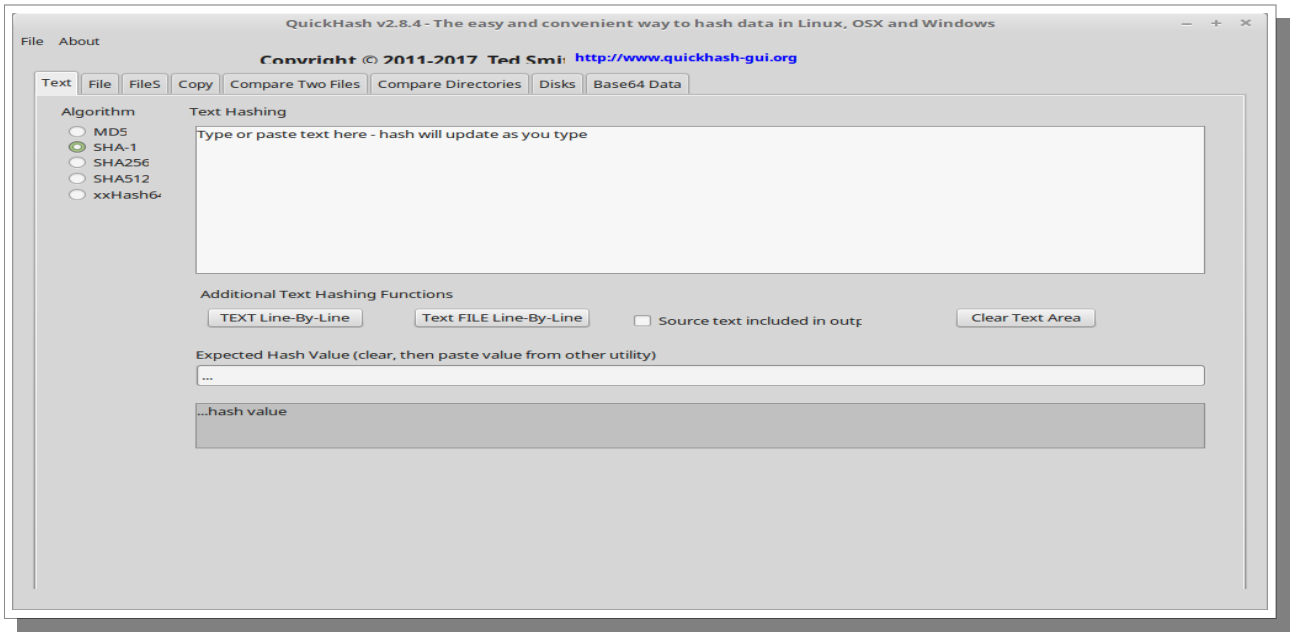
En resumen, todos los documentos que se presenten en los sobres 2 (y 3 si lo hubiera) estarán sólo en formato electrónico e irán acompañados por la declaración de huella digital de los ficheros que contienen estos documentos en formato electrónico, tal como se indica en el párrafo anterior.

En los siguientes apartados se muestra cómo calcular las huellas digitales de un conjunto de ficheros, tanto para aplicaciones con interfaz gráfico de usuario como en modo línea de comando, para los sistemas operativos Linux, Windows 10 o Mac

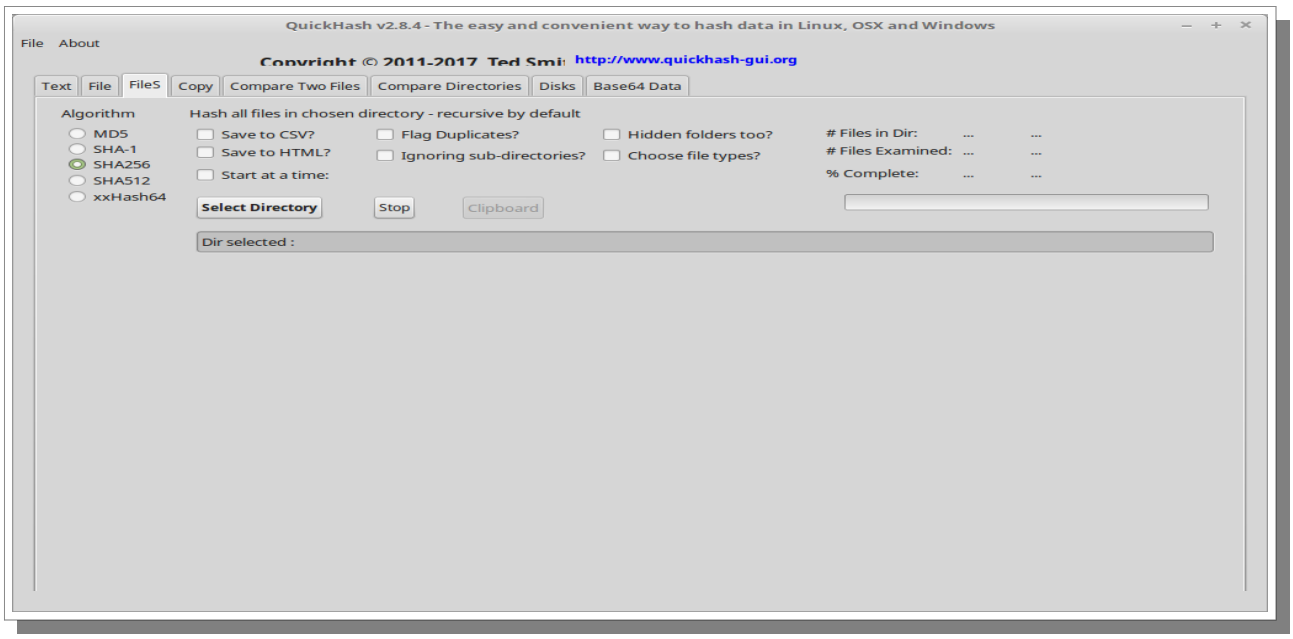
3.- Modo Interfaz Gráfica: QuickHash

Para el modo GUI se usará la herramienta QuickHash en su versión 2.6.0 o superior (http://sourceforge.net/projects/quickhash/). Esta herramienta está disponible para los S.O. Windows, Mac y Linux.

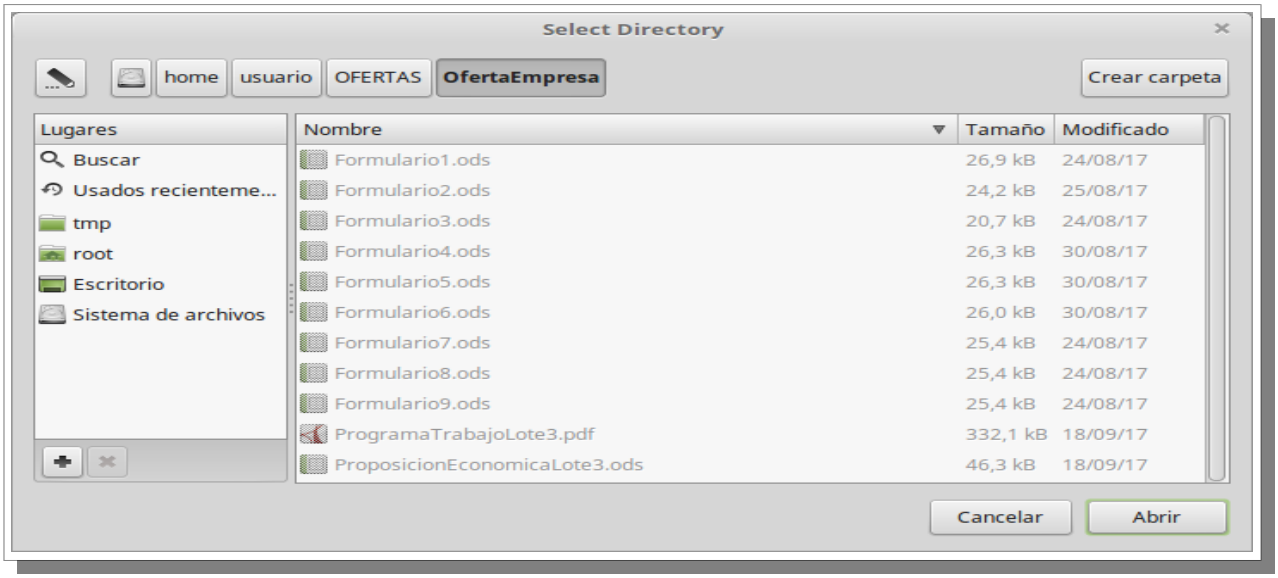
Una vez iniciada la herramienta se mostrará tal como aparece en la siguiente figura:



A continuación se selecciona la pestaña (ficha) **FileS** y aparecerá la siguiente pantalla:

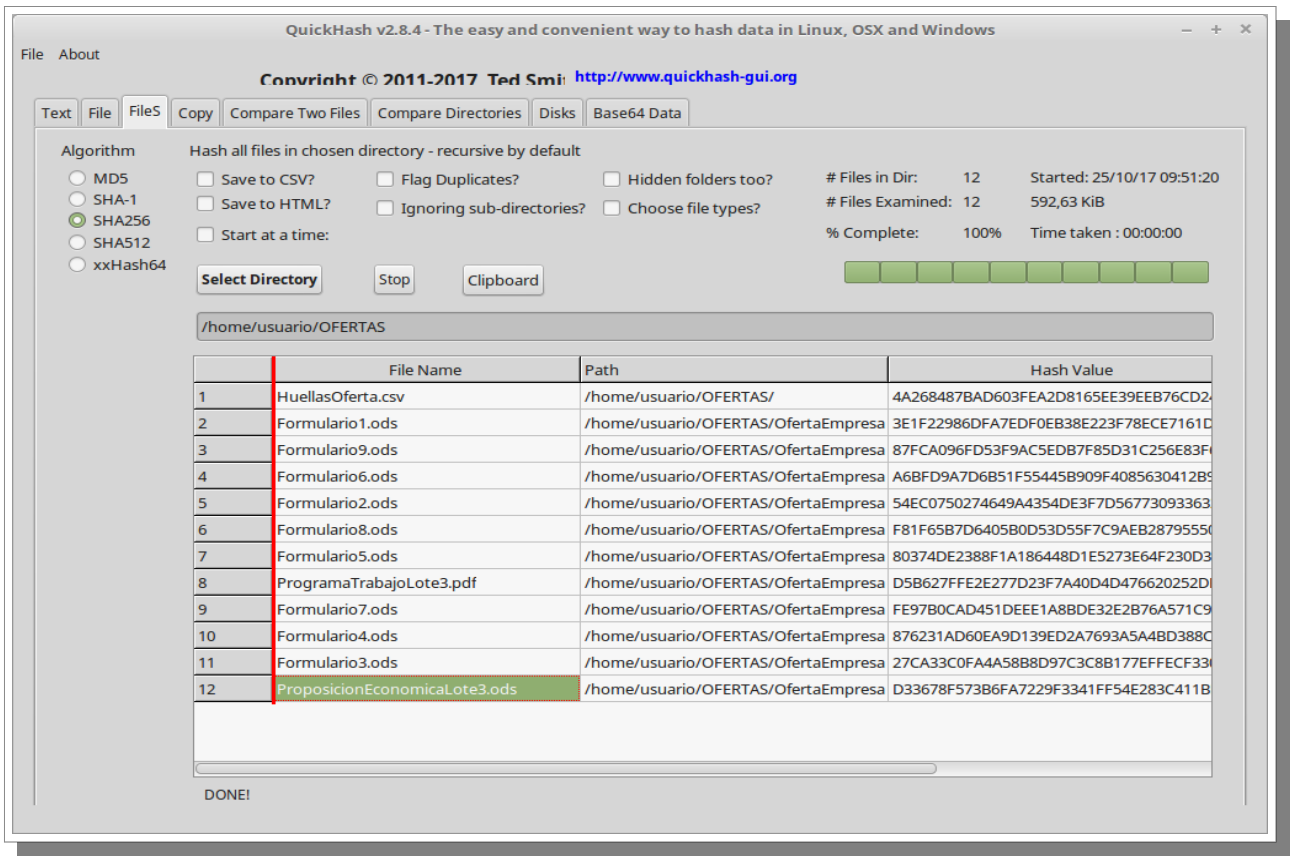


En esta pantalla se selecciona el algoritmo de generación de Huella digital SHA256, se des-selecciona la creación de un fichero en formato CSV y se pulsa sobre el botón "Select Directory" mostrándose la ventana de selección de la figura siguiente:

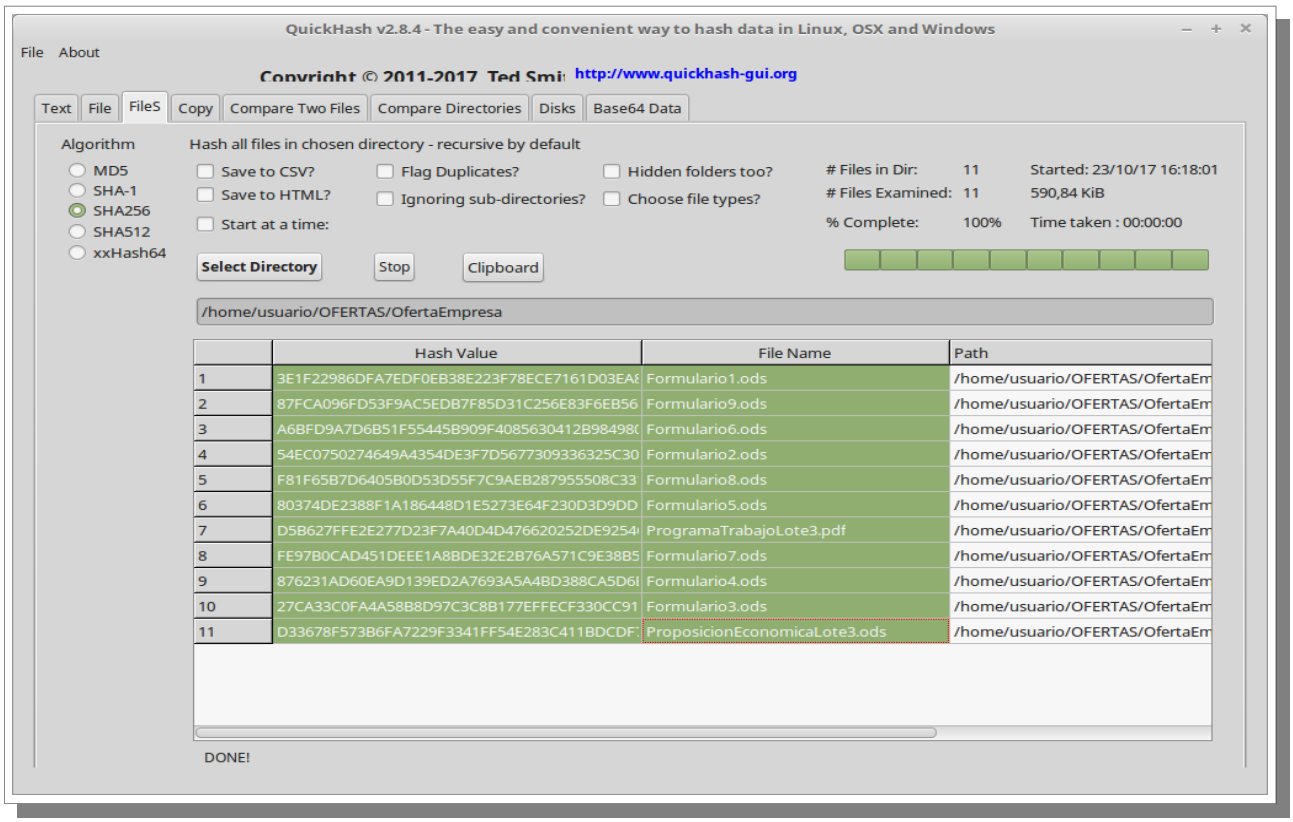


Una vez elegido el directorio donde se encuentra los ficheros de los documentos de los que se necesita calcular su huella digital se mostrará la ventana donde se puede ver, entre otros datos, las huellas digitales obtenidas.

Seleccionado la columna "Hash Value", se "arrastra" hasta que ocupe la primera columna de la tabla.



Después se seleccionan y copian las filas correspondientes a los valores de los ficheros y huella digital para incluirlos en los anexos de las declaraciones de huella digital indicados en el PCAP.



4.- Modo Línea Comando

La forma más sencilla de calcular la huella digital de un conjunto de ficheros es utilizando aplicaciones en modo gráfico, como la presentada en el apartado anterior, debido a que el entorno de trabajo es mucho más intuitivo que las equivalentes en modo línea de comando.

No obstante, a modo de demostración, se incluyen a continuación la forma de generar las huellas digitales en modo comando para las distintas plataformas.

4.1.- Linux

```
usuario@indalo ~/PROPUESTA
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
-rwxr-xr-x 1 usuario usuario  24188 ago 25 09:32 Formulario2.ods
-rwxr-xr-x 1 usuario usuario  20653 ago 24 11:13 Formulario3.ods
-rwxr-xr-x 1 usuario usuario  26342 ago 30 09:18 Formulario4.ods
-rwxr-xr-x 1 usuario usuario  26313 ago 30 09:13 Formulario5.ods
-rwxr-xr-x 1 usuario usuario  26017 ago 30 09:03 Formulario6.ods
-rwxr-xr-x 1 usuario usuario  25408 ago 24 12:48 Formulario7.ods
-rwxr-xr-x 1 usuario usuario  25399 ago 24 10:13 Formulario8.ods
-rwxr-xr-x 1 usuario usuario  25398 ago 24 10:10 Formulario9.ods
-rwxr-xr-x 1 usuario usuario 332087 sep 18 13:17 ProgramaTrabajoLote3.pdf
-rwxr-xr-x 1 usuario usuario  46302 sep 18 13:17 ProposicionEconomicaLote3.ods
usuario@indalo ~/PROPUESTA $ sha256sum * > /tmp/Huellas.txt
usuario@indalo ~/PROPUESTA $ cat /tmp/Huellas.txt
3e1f22986dfa7edf0eb38e223f78ece7161d03ea8c6a6f3ad4bb2a0118d11b1e  Formulario1.ods
54ec0750274649a4354de3f7d5677309336325c303721fbef04f685340d938f3  Formulario2.ods
27ca33c0fa4a58b8d97c3c8b177effecf330cc919127642e0803a448678cf8b0  Formulario3.ods
876231ad60ea9d139ed2a7693a5a4bd388ca5d6e4095cb1a227c37f3f0889df0  Formulario4.ods
80374de2388f1a186448d1e5273e64f230d3d9ddfdbf66f3e461b129d7c2a9de  Formulario5.ods
a6bfd9a7d6b51f55445b909f4085630412b98498017f75540308fe5bf001a150  Formulario6.ods
fe97b0cad451deee1a8bde32e2b76a571c9e38b5f5a1a6baf2ebd13773badc4d  Formulario7.ods
f81f65b7d6405b0d53d55f7c9aeb287955508c331be598cec5b9f6de1b0bbf2c  Formulario8.ods
87fca096fd53f9ac5edb7f85d31c256e83f6eb56f40687497d411cfc9f62708e  Formulario9.ods
d5b627ffe2e277d23f7a40d4d476620252de9254cdc0cb0c9b0c515ca7d2e7da  ProgramaTrabajoLote3.pdf
d33678f573b6fa7229f3341ff54e283c411bdcdf7d39a39716e2f636bf7b57d1  ProposicionEconomicaLote3.ods
usuario@indalo ~/PROPUESTA $ ls
```

Se muestra cómo se calculan las huellas digitales, según el algoritmo SHA256, para todos los ficheros del directorio actual en un sistema Linux. El comando que se usa es el sha256sum. En distribuciones derivadas de Debian (Ubuntu, Guadalinex, LinuxMint,...) se encuentra incluido en el paquete coreutils.

4.2.- Windows 10

```
Símbolo del sistema
24/10/2017  12:53    <DIR>          .
24/10/2017  12:53    <DIR>          ..
24/08/2017  09:59            26.914 Formulario1.ods
25/08/2017  09:32            24.188 Formulario2.ods
24/08/2017  11:13            20.653 Formulario3.ods
30/08/2017  09:18            26.342 Formulario4.ods
30/08/2017  09:13            26.313 Formulario5.ods
30/08/2017  09:03            26.017 Formulario6.ods
24/08/2017  12:48            25.408 Formulario7.ods
24/08/2017  10:13            25.399 Formulario8.ods
24/08/2017  10:10            25.398 Formulario9.ods
19/01/2017  14:30           332.087 ProgramaTrabajoLote2.pdf
15/09/2016  09:45            46.302 ProposicionEconomicaLote2.ods
              11 archivos        605.021 bytes
               2 dirs  59.127.664.640 bytes libres

C:\md5deep-4.4>sha256deep ..\Propuesta\*
3e1f22986dfa7edf0eb38e223f78ece7161d03ea8c6a6f3ad4bb2a0118d11b1e  C:\Propuesta\Formulario1.ods
54ec0750274649a4354de3f7d5677309336325c303721fbef04f685340d938f3  C:\Propuesta\Formulario2.ods
27ca33c0fa4a58b8d97c3c8b177effecf330cc919127642e0803a448678cf8b0  C:\Propuesta\Formulario3.ods
876231ad60ea9d139ed2a7693a5a4bd388ca5d6e4095cb1a227c37f3f0889df0  C:\Propuesta\Formulario4.ods
80374de2388f1a186448d1e5273e64f230d3d9ddfdbf66f3e461b129d7c2a9de  C:\Propuesta\Formulario5.ods
a6bfd9a7d6b51f55445b909f4085630412b98498017f75540308fe5bf001a150  C:\Propuesta\Formulario6.ods
fe97b0cad451deee1a8bde32e2b76a571c9e38b5f5a1a6baf2ebd13773badc4d  C:\Propuesta\Formulario7.ods
f81f65b7d6405b0d53d55f7c9aeb287955508c331be598cec5b9f6de1b0bbf2c  C:\Propuesta\Formulario8.ods
87fca096fd53f9ac5edb7f85d31c256e83f6eb56f40687497d411cfc9f62708e  C:\Propuesta\Formulario9.ods
d33678f573b6fa7229f3341ff54e283c411bdcdf7d39a39716e2f636bf7b57d1  C:\Propuesta\ProposicionEconomicaLote2.ods
d5b627ffe2e277d23f7a40d4d476620252de9254cdc0cb0c9b0c515ca7d2e7da  C:\Propuesta\ProgramaTrabajoLote2.pdf

C:\md5deep-4.4>_
```

En la figura anterior se muestra como se calculan las huellas digitales, según el algoritmo SHA256, para todos los ficheros del directorio actual en un sistema Windows 10. El comando que se usa (para arquitectura de 64 bits) es el que se incluye en el paquete hashdeep en su versión 4.4 (http://md5deep.sourceforge.net/ → https://github.com/jessek/hashdeep/releases/tag/release-4.4).

4.3.- Mac OS

```
OfertaDemo — -bash — 97×24
usuario@indalo ~PROPUESTA $
usuario@indalo ~PROPUESTA $
usuario@indalo ~PROPUESTA $
usuario@indalo ~PROPUESTA $ ls
Formulario1.ods          Formulario5.ods          Formulario9.ods
Formulario2.ods          Formulario6.ods          ProgramaTrabajoLote3.pdf
Formulario3.ods          Formulario7.ods          ProposicionEconomicaLote3.ods
Formulario4.ods          Formulario8.ods
usuario@indalo ~PROPUESTA $ shasum -a 256 *
3e1f22986dfa7edf0eb38e223f78ece7161d03ea8c6a6f3ad4bb2a0118d11b1e  Formulario1.ods
54ec0750274649a4354de3f7d5677309336325c303721fbef04f685340d938f3  Formulario2.ods
27ca33c0fa4a58b8d97c3c8b177effecf330cc919127642e0803a448678cf8b0  Formulario3.ods
876231ad60ea9d139ed2a7693a5a4bd388ca5d6e4095cb1a227c37f3f0889df0  Formulario4.ods
80374de2388f1a186448d1e5273e64f230d3d9ddfdbf66f3e461b129d7c2a9de  Formulario5.ods
a6bfd9a7d6b51f55445b909f4085630412b98498017f75540308fe5bf001a150  Formulario6.ods
fe97b0cad451deee1a8bde32e2b76a571c9e38b5f5a1a6baf2ebd13773badc4d  Formulario7.ods
f81f65b7d6405b0d53d55f7c9aeb287955508c331be598cec5b9f6de1b0bbf2c  Formulario8.ods
87fca096fd53f9ac5edb7f85d31c256e83f6eb56f40687497d411cfc9f62708e  Formulario9.ods
d5b627ffe2e277d23f7a40d4d476620252de9254cdc0cb0c9b0c515ca7d2e7da  ProgramaTrabajoLote3.pdf
d33678f573b6fa7229f3341ff54e283c411bdcdf7d39a39716e2f636bf7b57d1  ProposicionEconomicaLote3.ods
usuario@indalo ~PROPUESTA $
```

En esta ocasión se muestra como se calculan las huellas digitales, según el algoritmo SHA256, para todos los ficheros del directorio actual en un sistema Mac OS. El comando que se usa es el que se incluye en propio sistema operativo.