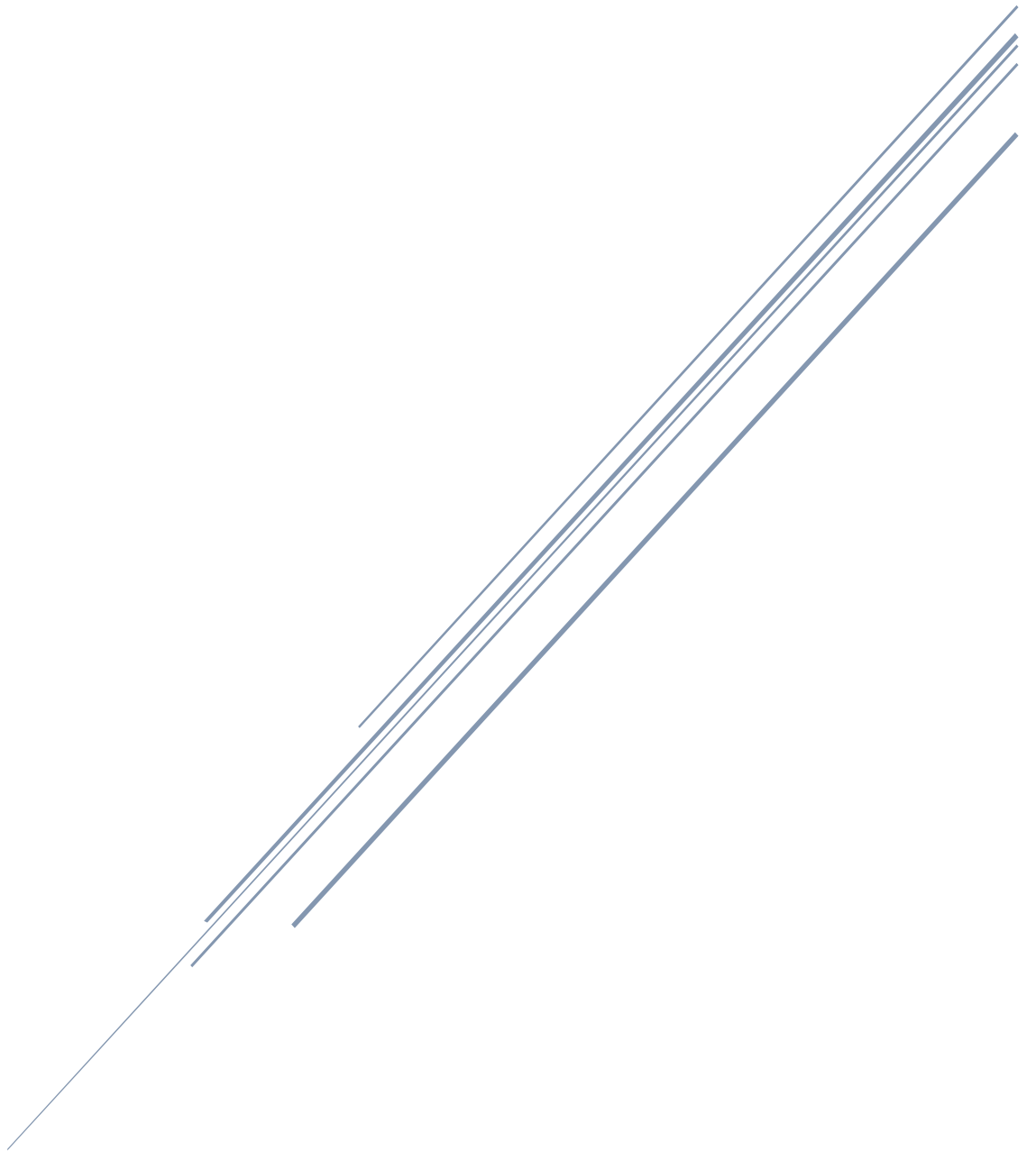


ADQUISICIÓN FORENSE DE UNA MEMORIA USB

Usando herramientas como FTK Imager, Guylmager y dd.



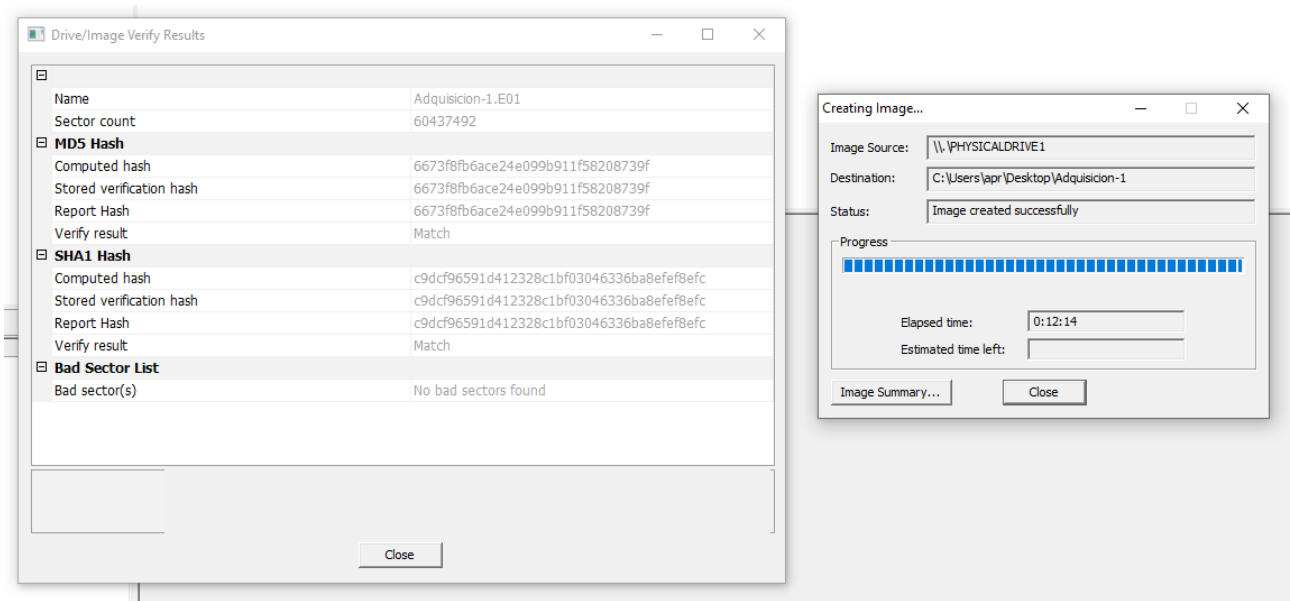
Álvaro Pérez Rey
Análisis Forense Informático

Realiza una adquisición forense de una memoria USB empleado las herramientas FTK Imager, Guylmager y dd.

Comenzaremos por la primera de las herramientas, FTK Imager. En nuestro caso hemos realizado la adquisición de una memoria USB de 32gb en un SO Windows 10 Home.

Hemos realizado una imagen del disco del dispositivo USB y para garantizar que esta imagen mantiene su integridad hemos utilizado 2 algoritmos de hashado como son MD5 y SHA1.

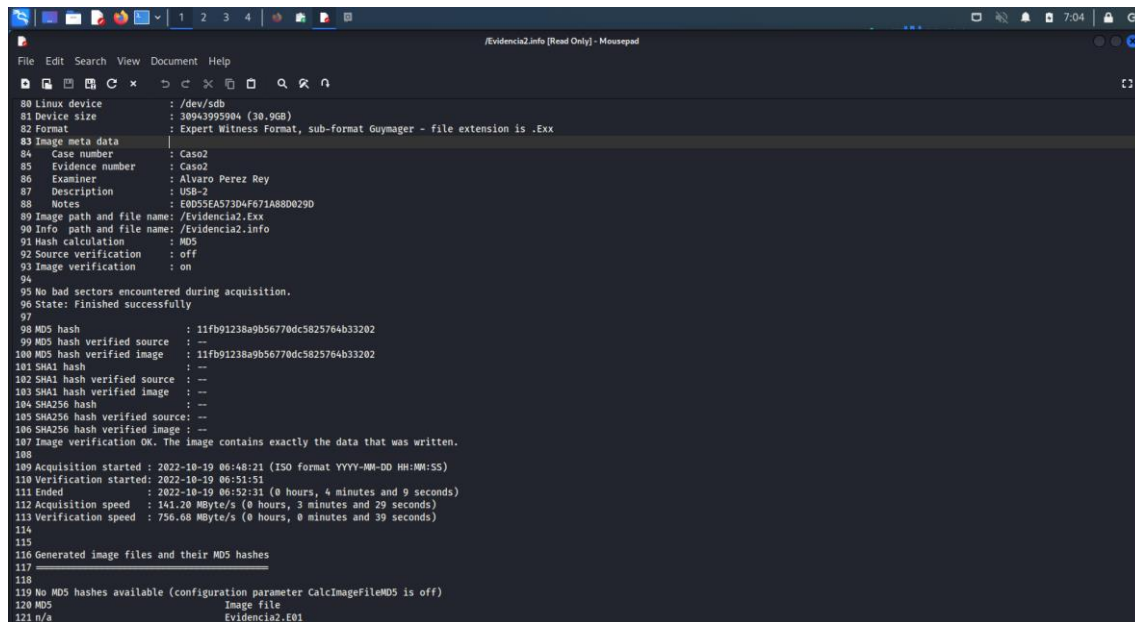
Al calcular los hashes, de los diferentes formatos, tanto en el original como en la imagen comprobamos que esta adquisición cumple con el principio de integridad, punto que debemos tener presente en todo momento.



Por otro lado, continuamos con la adquisición de otra memoria USB de 32gb en un SO Kali Linux con la herramienta Guymager, herramienta que trae por defecto este sistema.

En este caso, detectamos un problema en el programa que nos impide mover el directorio donde vamos a crear nuestros ficheros de clonación, por lo tanto, decidimos poner como directorio destino el directorio raíz.

Una vez realizado el clonado con éxito abriremos nuestro archivo.info generado para comprobar la coincidencia de hashes en formato MD5.

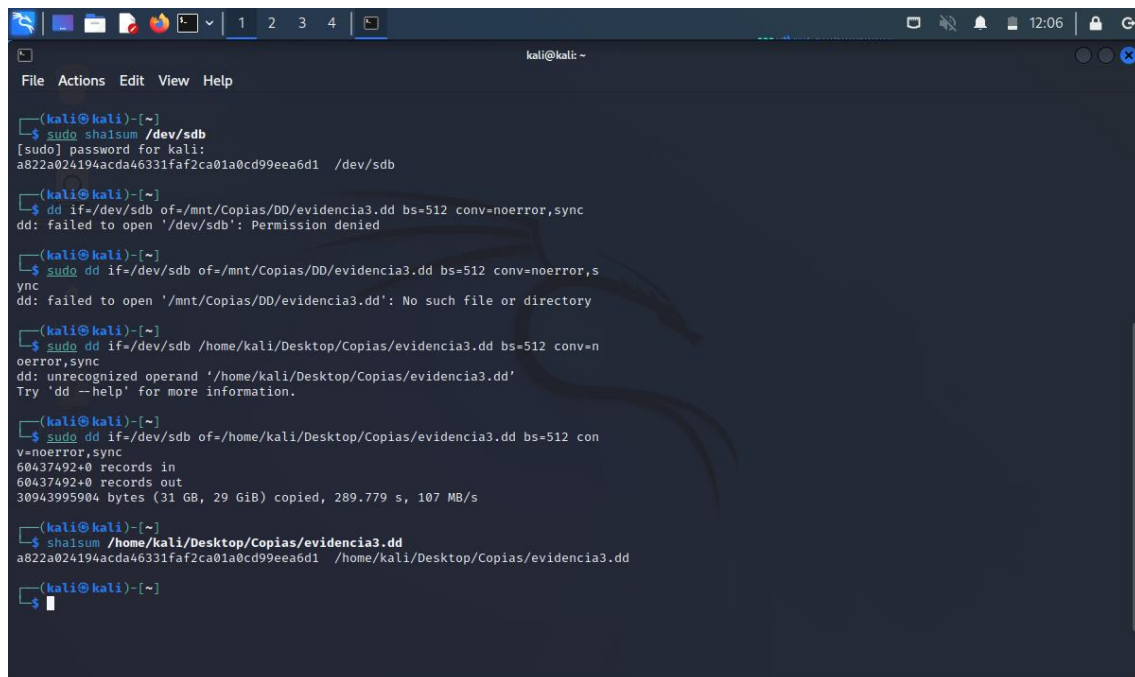


```
File Edit Search View Document Help
Evidencia2.info (Read Only) - Mousepad

80 Linux device      : /dev/sdb
81 Device size      : 30943995904 (30,9GB)
82 Format           : Expert Witness Format, sub-format Guymager - file extension is .Exx
83 Image meta data  :
84   Case number     : Caso2
85   Evidence number : Caso2
86   Examiner       : Alvaro Perez Rey
87   Description     : USB-2
88   Notes          : E0D55EA573D4F671A88D029D
89 Image path and file name: /Evidencia2.Exx
90 Info path and file name: /Evidencia2.info
91 Hash calculation  : MD5
92 Source verification : off
93 Image verification : on
94
95 No bad sectors encountered during acquisition.
96 State: Finished successfully
97
98 MD5 hash          : 11fb91238a9b56770dc5825764b33202
99 MD5 hash verified source : --
100 MD5 hash verified image  : 11fb91238a9b56770dc5825764b33202
101 SHA1 hash          : --
102 SHA1 hash verified source : --
103 SHA1 hash verified image  : --
104 SHA256 hash        : --
105 SHA256 hash verified source: --
106 SHA256 hash verified image: --
107 Image verification OK. The image contains exactly the data that was written.
108
109 Acquisition started : 2022-10-19 06:48:21 (ISO format YYYY-MM-DD HH:MM:SS)
110 Verification started: 2022-10-19 06:51:51
111 Ended              : 2022-10-19 06:52:31 (0 hours, 4 minutes and 9 seconds)
112 Acquisition speed   : 141.20 MByte/s (0 hours, 3 minutes and 29 seconds)
113 Verification speed  : 756.68 MByte/s (0 hours, 0 minutes and 39 seconds)
114
115
116 Generated image files and their MD5 hashes
117
118
119 No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
120 MD5      Image file
121 n/a      Evidencia2.E01
```

Añadir como dato que puede también añadir más algoritmos de hasheo antes del proceso de clonado.

Por último, vamos con nuestra última adquisición, está la hemos obtenido de una memoria USB de 32gb en un SO Kali Linux de nuevo. En primer lugar, hemos identificado la memoria USB dentro de nuestro sistema después hemos calculado su hash en formato SHA1 para posteriormente poder compararlo con el hash de nuestra copia.



```
(kali@kali)-[~]
└─$ sudo shasum /dev/sdb
[sudo] password for kali:
a822a024194acda46331faf2ca01a0cd99eea6d1 /dev/sdb

(kali@kali)-[~]
└─$ dd if=/dev/sdb of=/mnt/Copias/DD/evidencia3.dd bs=512 conv=noerror,sync
dd: failed to open '/dev/sdb': Permission denied

(kali@kali)-[~]
└─$ sudo dd if=/dev/sdb of=/mnt/Copias/DD/evidencia3.dd bs=512 conv=noerror,sync
dd: failed to open '/mnt/Copias/DD/evidencia3.dd': No such file or directory

(kali@kali)-[~]
└─$ sudo dd if=/dev/sdb /home/kali/Desktop/Copias/evidencia3.dd bs=512 conv=noerror,sync
dd: unrecognized operand '/home/kali/Desktop/Copias/evidencia3.dd'
Try 'dd --help' for more information.

(kali@kali)-[~]
└─$ sudo dd if=/dev/sdb of=/home/kali/Desktop/Copias/evidencia3.dd bs=512 conv=noerror,sync
60437492+0 records in
60437492+0 records out
30943995904 bytes (31 GB, 29 GiB) copied, 289.779 s, 107 MB/s

(kali@kali)-[~]
└─$ shasum /home/kali/Desktop/Copias/evidencia3.dd
a822a024194acda46331faf2ca01a0cd99eea6d1 /home/kali/Desktop/Copias/evidencia3.dd

(kali@kali)-[~]
└─$
```

Una vez realizada la copia mediante dd, por terminal, calcularemos el hash, en formato SHA1, de nuestra adquisición para poder comprobar si este y el original coincide y así cumplir el principio de integridad.