

Práctica Seguridade Informática: Recuperación de ficheiros dunha Memoria Externa



ESCENARIO

Máquina A:

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

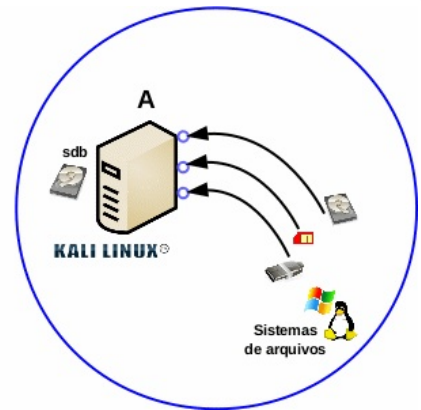
ISO: Kali Live amd64

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

sdb: Disco externo USB empregado para recuperación de datos

Tamaño sdb = ((Tamaño Memoria externa a recuperar) + (espazo recuperación datos))

"KALI LINUX™ é unha marca comercial de Offensive Security"



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTA:

- Documentación de interese:

Sistemas de arquivos



TestDisk



- Comando dd**

\$ man dd

dd if=/dev/sdX of=/mnt/image-SD.dd bs=1024K status=progress

Volcar todos os sectores/bloques do disco sdX en /mnt/image-SD.dd, onde:

- if=/dev/sdX → input file (Orixe da copia): Ficheiro/dispositivo que se quere copiar. Neste caso, o dispositivo /dev/sdX
- of=/mnt/image-SD.dd → output file (Destino da): Ficheiro/dispositivo a onde se quere volcar/copiar a orixe indicada. Neste caso, o destino é o ficheiro /mnt/image-SD.dd
- bs=1024K → Tamaño de lectura/escritura en bloques para realizar o volcado de if a of
- status=progress → amosar o progreso da copia durante a transferencia.

IMPORTANTE!:

- Nunca tratar de recuperar os datos no propio dispositivo(memoria externa) do que queremos recuperar os datos.
- Facer un volcado(copia por sectores/bloques co comando **dd**) do dispositivo que posúe os datos a recuperar.
- Se un dase conta que eliminou datos por erro nun dispositivo, deixar inmediatamente de traballar co dispositivo, para non corromper máis o dispositivo, sobreescribindo sectores, e impedindo un bo resultado no procedemento de recuperación de datos.
- Non montar a memoria externa para recuperar datos, é dicir, non montar o propio dispositivo do cal queremos recuperar datos.

Recuperación de ficheiros dunha Memoria Externa

Imos recuperar datos dunha memoria externa (pendrive, tarxeta SD (microSD ou similar), disco duro externo, etc. mediante o mesmo procedemento. Basicamente:

1. Arrancar en modo forense Kali Linux.
2. Montar o disco duro **sdb** (particións/volumes sdaX) que posúe o espazo suficiente para volcar a memoria externa e tamén poder recuperar os datos.
3. Conectar a memoria externa.
4. **IMPORTANTE: Non montar a memoria externa.**
5. Facer un volcado do sistema de arquivos da memoria externa mediante o comando **dd**
6. Recuperar a información desexada mediante o comando **testdisk**

Procedemento:

1. Arrancar en modo forense en Kali Linux.



2. Montar o disco duro **sdb** (particións/volumes sdaX) que posúe o espazo suficiente para volcar a memoria externa e tamén poder recuperar os datos.

Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
```

```
root@kali:~# fdisk -l /dev/sdb #Lista a táboa de particións do disco /dev/sdb e logo remata.
```

```
Disco /dev/sdb: 1,8 TiB, 2000398931968 bytes, 3907029164 sectores
Modelo de disco: External USB 3.0
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0xabc123ab
```

Disposit.	Inicio	Comienzo	Final	Sectores	Tamaño	Id	Tipo
/dev/sdb1	2048	3907028991	3907026944	1,8T	7		HPFS/NTFS/exFAT

```
root@kali:~# mkdir /mnt/recuperar #Crear o directorio /mnt/recuperar.
```

```
root@kali:~# mount -t auto /dev/sdb1 /mnt/recuperar #Montar a partición 1 do disco duro /dev/sdb no directorio da live /mnt/recuperar. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe..
```

3. Conectar/identificar a memoria externa (pendrive, SD, disco duro, etc)

Antes de conectar a memoria externa, executar:

```
root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
```

```
root@kali:~# dmesg -w #Amosar as mensaxes do kernel acontecidas e espera a próximas conexións en tempo real sen devolver o
```

prompt. A opción -w é válida dende a versión do kernel 3.5.0

Conectar a memoria externa e revisar a consola onde executamos o comando anterior *dmesg -w*. Agora debería aparecer identificado o dispositivo conectado.

```
[217321.291034] usb 1-6: USB disconnect, device number 9
[217459.947432] usb 1-3: new high-speed USB device number 10 using xhci_hcd
[217460.100498] usb 1-3: New USB device found, idVendor=0951, idProduct=162d, bcdDevice= 1.00
[217460.100506] usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[217460.100511] usb 1-3: Product: DataTraveler 102
[217460.100515] usb 1-3: Manufacturer: Kingston
[217460.100519] usb 1-3: SerialNumber: AA1CC0BB34EAAAC0ACCCCCC9
[217460.102232] usb-storage 1-3:1.0: USB Mass Storage device detected
[217460.102624] scsi host2: usb-storage 1-3:1.0
[217461.127002] scsi 2:0:0:0: Direct-Access Kingston DataTraveler 102 PMAP PQ: 0 ANSI: 0 CCS
[217461.128726] sd 2:0:0:0: Attached scsi generic sgl type 0
[217462.119994] sd 2:0:0:0: [sdc] 7831552 512-byte logical blocks: (4.01 GB/3.73 GiB)
[217462.121398] sd 2:0:0:0: [sdc] Write Protect is off
[217462.121404] sd 2:0:0:0: [sdc] Mode Sense: 03 41 00 00
[217462.122766] sd 2:0:0:0: [sdc] No Caching mode page found
[217462.122778] sd 2:0:0:0: [sdc] Assuming drive cache: write through
[217462.143673] sdc: sdc1
[217462.148693] sd 2:0:0:0: [sdc] Attached SCSI removable disk
```

Executar:

root@kali:~# ^C #Abortar execución do comando anterior, é dicir, abortar o comando *dmesg -w*, enviando o sinal 2 (SIGNINT 2)(kill -l) ao sistema.

root@kali:~# fdisk -l /dev/sdc #Lista a táboa de particións do disco /dev/sdc e logo remata.

```
Disco /dev/sdc: 3,8 GiB, 4009754624 bytes, 7831552 sectores
Modelo de disco: DataTraveler 102
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0x4a423dc7
```

Disposit.	Inicio	Comienzo	Final	Sectores	Tamaño	Id	Tipo
/dev/sdc1	2048	7831551	7829504	3,8G	b W95	FAT32	

4. IMPORTANTE: Non montar a memoria externa.

Revisar antes de proceder que o dispositivo memoria externa non está montado:

root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.

5. Facer un volcado do sistema de arquivos da memoria externa mediante o comando **dd**

root@kali:~# dd if=/dev/sdc of=/mnt/recuperar/image-SD.dd bs=1024K status=progress #Facer un volcado da memoria externa (/dev/sdc) no ficheiro image-SD.dd. Para iso ao comando dd pásámolle como argumento o tamaño de lectura/escritura en bloques que emprega para realizar a copia (bs=1024K).

```
3997171712 bytes (4,0 GB, 3,7 GiB) copied, 239 s, 16,7 MB/s
3824+0 registros leídos
3824+0 registros escritos
4009754624 bytes (4,0 GB, 3,7 GiB) copied, 239,97 s, 16,7 MB/s
```

6. Recuperar a información desexada mediante o comando **testdisk**

root@kali:~# testdisk /mnt/recuperar/image-SD.dd #Abrir mediante o comando *testdisk* a imaxe copiada da memoria externa para proceder á recuperación de datos.

```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk image-SD.dd - 4009 MB / 3824 MiB

>[Proceed ] [ Quit ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

A. Elixir **Proceed** para continuar:

```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org

Disk image-SD.dd - 4009 MB / 3824 MiB

Please select the partition table type, press Enter when done.
>[Intel ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Humax ] Humax partition table
[Mac ] Apple partition map (legacy)
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return] Return to disk selection

Hint: Intel partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

B. Escoller o tipo de táboa de particionamento que posúa a memoria externa, neste caso **Intel**:

```

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org

Disk image-SD.dd - 4009 MB / 3824 MiB
CHS 488 255 63 - sector size=512

[ Analyse ] Analyse current partition structure and search for lost partitions
>[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ MBR Code ] Write TestDisk MBR code to first sector
[ Delete ] Delete all data in the partition table
[ Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.

```

C. Escoller Advanced

```

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org

Disk image-SD.dd - 4009 MB / 3824 MiB - CHS 488 255 63

Partition              Start      End      Size in sectors
> 1 P FAT32             0 32 33   487 125 22   7829504 [USB-PDF]

[ Type ] [ Boot ] >[Undelete] [Image Creation] [ Quit ]
                        File undelete

```

D. Escoller Undelete

```

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org
 1 P FAT32             0 32 33   487 125 22   7829504 [USB-PDF]
Directory /

Previous
...
>-rwxr-xr-x    0    0   40988 26-Jan-2020 12:01 Sin título 1.pdf
...
Next

Use Right to change directory, h to hide deleted files
q to quit, : to select the current file, a to select all files
C to copy the selected files, c to copy the current file

```

- E. Move-se pelos directorios e atopar os dados(ficheiros/cartafol) a recuperar.
- F. Premir **c** para copiar o ficheiro onde temos o cursor.

G. Elixir onde copiar. Imos premer **C** para indicar que **/mnt** é o destino de copia:

```
TestDisk 7.1, Data Recovery Utility, July 2019

Please select a destination where /Sin título 1.pdf will be copied.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /mnt
>drwxrwxrwx 1000 1000 0 8-Feb-2021 01:16 .
drwxr-xr-x 0 0 160 8-Feb-2021 01:38 ..
-rwxrwxrwx 1000 1000 4009754624 8-Feb-2021 01:20 image-SD.dd
```

H. Copiado:

```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER
https://www.cgsecurity.org
1 P FAT32 0 32 33 487 125 22 7829504 [USB-PDF]
Directory /Sin título 1.pdf
Copy done! 1 ok, 0 failed Previous
...
>-rwxr-xr-x 0 0 40988 26-Jan-2020 12:01 Sin título 1.pdf
...
Next
Use Right to change directory, h to hide deleted files
q to quit, : to select the current file, a to select all files
C to copy the selected files, c to copy the current file
```

I. Saír de *testdisk* premendo varias veces a tecla **q**

J. Comprobar que o ficheiro foi recuperado:

```
root@kali:~# ls -l #Listar de forma extendida amosando o contido do directorio onde se executa o comando (neste caso /mnt)
```

```
total 3915820
-rwxrwxrwx 1 kali kali 4009754624 feb 8 01:20 image-SD.dd
-rwxrwxrwx 1 kali kali 40988 ene 26 2020 'Sin título 1.pdf'
```

Os datos foron recuperados

K. Unha vez recuperados os datos desmontar o disco externo onde foron recuperados:

```
root@kali:~# cd #Cambiar ao directorio $HOME do usuario que executa o comando, é dicir, se $HOME=/home/usuario, cambiarase ao
directorio /home/usuario, se $HOME=/root, cambiarase ao directorio /root
root@kali:~# umount /mnt/recuperar #Desmontar (deixar de facer uso) a partición primaria /dev/sdb1 que estaba montada en
/mnt/recuperar
```

Ricardo Feijoo Costa



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**