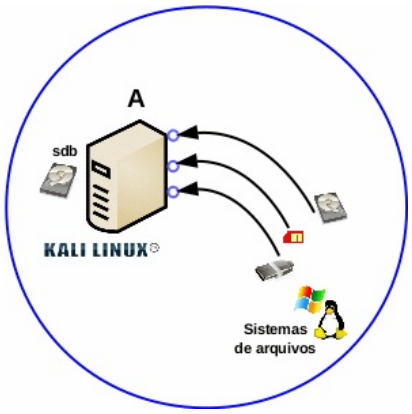
Práctica2 Seguridade Informática: Recuperación de ficheiros dunha Memoria Externa

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** **PhotoRec**

- **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.

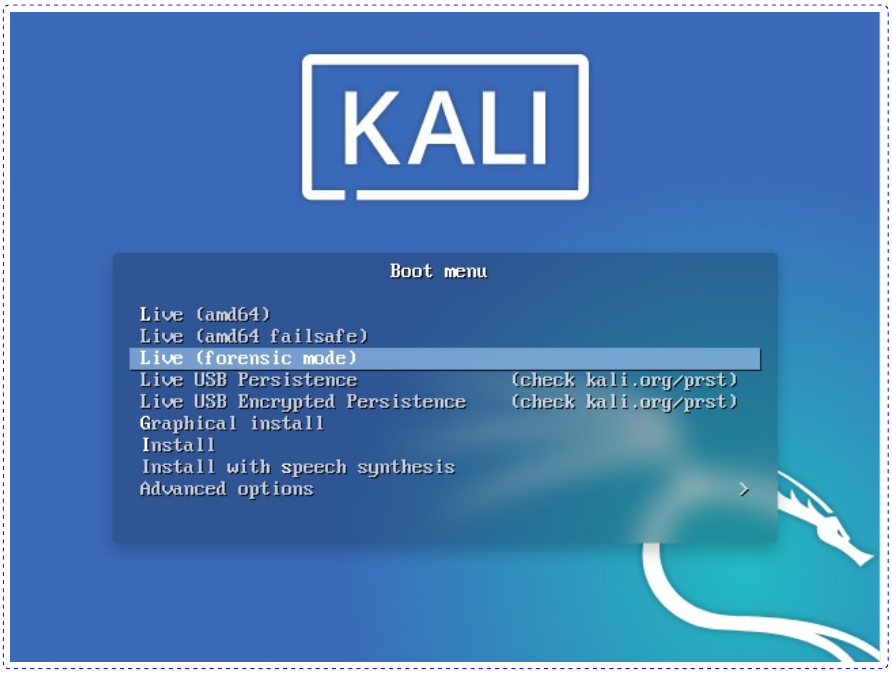
Recuperación de ficheiros dunha Memoria Externa

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 **photorec**

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 sg1 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 pasámolle 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 **photorec**

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

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

  PhotoRec 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 (RO)




>[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 an
detection, and install the latest OS patches and disk drivers.
```

A. Elixir **Proceed** para continuar.
B. Escoller a partición onde intentar recuperar datos:

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

Disk image-SD.dd - 4009 MB / 3824 MiB (RO)

     Partition                  Start        End    Size in sectors
      No partition             0   0  1   487 125 22    7831552 [Whole di
> 1 P FAT32                    0  32 33   487 125 22    7829504 [USB-PDF]




>[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                              Start file recovery
```

C. Escoller **File Opt** para seleccionar o tipo de ficheiros a recuperar

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

PhotoRec will try to locate the following files

>[X] custom Own custom signatures
 [X] 1cd  Russian Finance 1C:Enterprise 8
 [X] 3dm  Rhino / openNURBS
 [X] 7z   7zip archive file
 [X] DB
 [X] a    Unix Archive/Debian package
 [X] abr  Adobe Brush
 [X] acb  Adobe Color Book
 [X] accdb Access Data Base
 [X] ace  ACE archive
    Next
Press s to disable all file families, b to save the settings
>[  Quit  ]
                              Return to main menu
```

Unha vez seleccionados os tipos de ficheiros premer **b**, para gardar a configuración escollida, a continuación premer **Enter** para seleccionar **OK** e por último premer en **Quit** para voltar ao menú principal.

D. Escoller **Search**

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

Disk image-SD.dd - 4009 MB / 3824 MiB (RO)

     Partition                  Start        End    Size in sectors
      No partition             0   0  1   487 125 22    7831552 [Whole di
> 1 P FAT32                    0  32 33   487 125 22    7829504 [USB-PDF]




[ Search ]  [Options ]  [File Opt]  [  Quit  ]
```

E. Escoller **Other**

```
PhotoRec 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]

To recover lost files, PhotoRec needs to know the filesystem type where t
file were stored:
 [ ext2/ext3 ] ext2/ext3/ext4 filesystem
[ Other     ] FAT/NTFS/HFS+/ReiserFS/...
```

F. Elixir **Free** como o espazo a analizar:

```
PhotoRec 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]


Please choose if all space needs to be analysed:
>[   Free    ] Scan for file from FAT32 unallocated space only
 [   Whole   ] Extract files from whole partition
```

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

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

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored o
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /mnt/recuperar
>drwxr-xr-x     0     0      4096  9-Mar-2022 17:31 .
 drwxr-xr-x     0     0      4096  9-Mar-2022 17:31 ..
 -rwxrwxrwx  1000  1000 4009754624  9-Mar-2022 15:20 image-SD.dd
```

H. Recuperado e Copiado:

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

Disk image-SD.dd - 4009 MB / 3824 MiB (RO)
     Partition                  Start        End    Size in sectors
 1 P FAT32                   0  32 33   487 125 22    7829504 [USB-PDF]


1 files saved in /mnt/recuperar/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation




[ Quit ]
```

I. Saír de *photorec* premendo varias veces a tecla **q**
J. Comprobar que o ficheiro foi recuperado:

root@kali:~# ls -l /mnt/recuperar/recup_dir.1 #Listar de forma extendida amosando o contido do directorio /mnt/recuperar/recup_dir.1

```
total 20
-rw-r--r-- 1 root root 8193 mar  9 17:39 f0015304.pdf
-rw-r--r-- 1 root root 1630 mar  9 17:42 report.xml
```

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