Práctica Seguridade Informática: Volcados de memoria RAM

ESCENARIO:

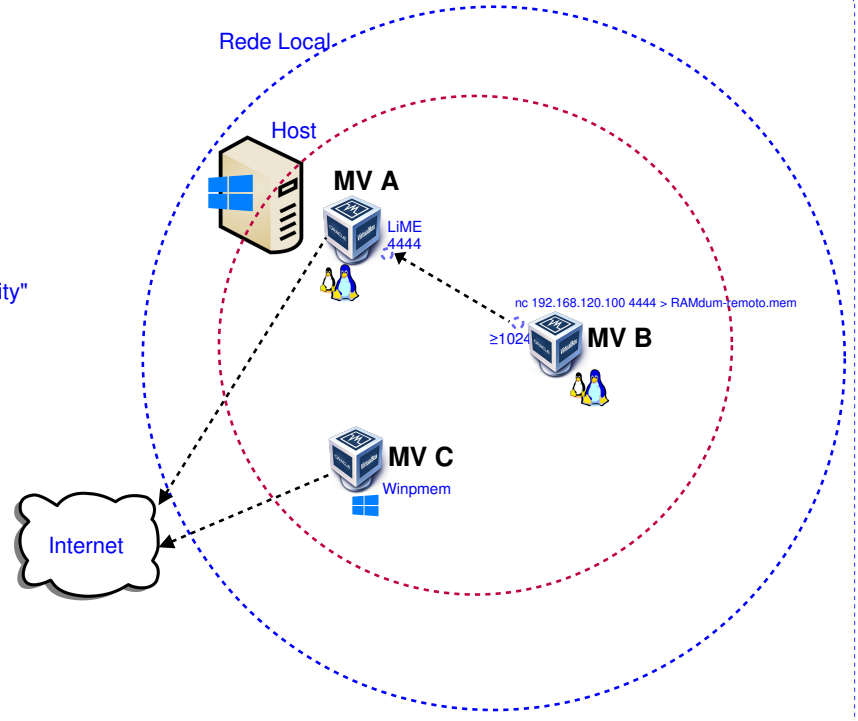
Host anfitrión:
Oracle VirtualBox
Conexión a Internet

Máquinas virtuais:
RAM ≤ 2048MBCPU ≤ 2PAE/NX habilitado
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
"KALI LINUX ™ é unha marca comercial de Offensive Security"

Máquina virtual A:
ISO: Kali Live amd64
Rede1: NAT
Rede2: Interna → 192.168.120.100/24
Disco duro onde volcar datos: /dev/sdb
LiME: Volcado memoria RAM en local e remoto

Máquina virtual B:
ISO: Kali Live amd64
Rede1: Interna → 192.168.120.101/24
Disco duro onde volcar datos: /dev/sdb

Máquina virtual HostC:
Rede1: NAT
Disco duro: Windows amd64
BIOS: Permite arranque disco duro
Winpmem: Volcado memoria RAM en local



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:

  [1] LiME

  [2] winpmem **[3] winpmem download release**

  [4] Extracción y análisis de malware desde volcados de memoria - Ricardo J. Rodríguez (UNIZAR)

  [5] Volatility **[6] Volatility2 GitHub** **[7] Volatility3 GitHub**

IMPORTANTE!:

- **En sistemas operativos non virtualizados o volcado de memoria RAM é unha técnica invasiva**, é dicir, nos datos volcados tamén apareceran os do propio programa de volcado. Isto é debido a que calquera programa debe ser executado en RAM, polo tanto, se queremos facer un volcado da RAM debemos executar un programa que á súa vez debe estar executándose na RAM.
- **LiME [1]** → Permite volcados RAM de sistemas operativos GNU/Linux e Android. Podemos facer o volcado dos datos no sistema de arquivos do dispositivo, nun dispositivo externo conectado ou directamente por rede.
- **winpmem [2]** → Permite volcados RAM de sistemas operativos MS Windows.
- **Máquinas virtuais** → O xestor de máquinas virtuais (VirtualBox, VMWare, etc) xa permiten de por si, coas súas propias ferramentas(comandos) facer un volcado da memoria RAM, sendo **o volcado de memoria RAM unha técnica non invasiva**, posto que no sistema operativo virtualizado non executamos o programa de volcado de memoria. Esta faise dendo o equipo anfitrión (onde está instalado o programa de virtualización).

Volcados de memoria RAM

Imos realizar volcados de memoria RAM en:

1. Sistemas operativos GNU/Linux
2. Sistemas operativos MS Windows
3. Máquinas virtuais Oracle VirtualBox

Volcado de memoria RAM en sistemas GNU/Linux

Imos facer un volcado da memoria RAM dunha distro GNU/Linux de 2 xeitos: a través dun disco duro (externo) que non contén o propio sistema operativo e a través da rede dende outra máquina conectada no mesmo segmento de rede. Basicamente:

1. Instalar o programa para volcar a memoria RAM no equipo do cal queremos volcar a memoria.
2. Realizar o volcado en local ou remoto.

Máquina virtual B: Kali amd64

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

2. Cambiar hostname da máquina virtual B. Por kaliB como hostname:
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   Opción A:
   root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
   root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
   root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.
   Opción B:
   root@kali:~# hostnamectl hostname kaliB #Modificar o valor do hostname a kaliB.
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

3. Configurar a rede:
   Na contorna gráfica abrir un terminal e executar:
   kali@kaliB:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kaliB:~# /etc/init.d/avahi-daemon stop || systemctl stop avahi-daemon #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
   root@kaliB:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
   root@kaliB:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B, as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kaliB:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
   root@kaliB:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B, as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kaliB:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0

4. Montar o disco onde gardar os volcados de memoria RAM:

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

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

```
Disk /dev/sdb: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xa944796c

Device     Boot Start       End   Sectors Size Id Type
/dev/sdb1        2048 167772159 167770112  80G  7 HPFS/NTFS/exFAT
```

root@kaliB:~# mkdir /mnt/remoto #Crear o directorio /mnt/volcar.

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

root@kaliB:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.

kali@kaliB:~$

Máquina virtual A: Kali amd64

Procedemento:

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ passwd kali || (echo -e 'kali\nabc123.\nabc123.' | passwd) #Cambiar o contrasinal do usuario kali. Por como contrasinal **abc123.**(Ollo que o contrasinal ten un caracter punto final)

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   Opción A:
   root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
   root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
   root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.
   Opción B:
   root@kali:~# hostnamectl hostname kaliA #Modificar o valor do hostname a kaliA.
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

3. Configurar a rede:
   Na contorna gráfica abrir un terminal e executar:
   kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kaliA:~# /etc/init.d/avahi-daemon stop || systemctl stop avahi-daemon #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
   root@kaliA:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
   root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(eth0) e interna(eth1).
   root@kaliA:~# ip addr add 192.168.120.100/24 dev eth1 #Configurar a tarxeta de rede interna eth1, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
   root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(eth0) e interna(eth1).
   root@kaliA:~# ip route #Amosar a táboa de rutas do sistema.
   root@kaliA:~# cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.
   root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth1
   root@kaliA:~# ping -c4 www.google.es #Comprobar mediante o comando ping a conectividade co dominio www.google.es
   root@kaliA:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade con kaliB

4. Montar o disco onde gardar os volcados de memoria RAM:
   root@kaliA:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
   root@kaliA:~# fdisk -l /dev/sdb #Lista a táboa de particións do disco /dev/sdb e logo remata.

   ```
   Disk /dev/sdb: 80 GiB, 85899345920 bytes, 167772160 sectors
   Disk model: VBOX HARDDISK
   Units: sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disklabel type: dos
   Disk identifier: 0xa944796c

   Device     Boot Start       End   Sectors Size Id Type
   /dev/sdb1        2048 167772159 167770112  80G  7 HPFS/NTFS/exFAT
   ```

   root@kaliA:~# mkdir /mnt/volcar #Crear o directorio /mnt/volcar.
   root@kaliA:~# mount -t auto /dev/sdb1 /mnt/volcar #Montar a partición 1 do disco duro /dev/sdb no directorio da live /mnt/volcar. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe..
   root@kaliA:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kaliA:~$

5. Programa de volcado (LiME [1]):

   kali@kaliA:~$ git clone https://github.com/504ensicsLabs/LiME.git #Descargar o repositorio LiME de git de 504ensicsLabs

   kali@kaliA:~$ cd LiME/src #Acceder ao directorio LiME/src

   kali@kaliA:~/LiME/src$ make #Compilar para crear o modulo lime.ko

6. Realizar volcado en local (LiME [1]):

   kali@kaliA:~/LiME/src$ sudo insmod ./lime*.ko "path=/mnt/volcar/RAMdump-local.mem format=lime timeout=0" #Facer o volcado de memoria RAM e gardalo no ficheiro /mnt/volcar/RAMdump-local.mem. A opción lime indica ese formato de copia, o cal e totalmente compatible co programa *volatility* [5][6][7]. A opción timeout=0 permite deshabilitar o "timeout" permitindo realizar unha copia máis fiable das páxinas de memoria.

   - O comando *sudo* é necesario porque precisamos permisos de *root* para poder cargar un módulo no kernel.
   - Non debemos facer nada no equipo ata que o comando remate, xa que senón estariamos "modificando" a estática da memoria RAM que pretendemos volcar.
   - Agora xa dispoñemos dunha copia do que está a acontecer no volcado na memoria RAM no instante do volcado.

7. Realizar volcado en remoto (LiME [1]):

   En kaliA(máquina local)

   kali@kaliA:~/LiME/src$ sudo rmmod lime Eliminar o módulo lime do kernel. Necesario para poder executar de nome un volcado de memoria, xa que temos que insertar de novo o módulo lime no kernel.

   kali@kaliA:~/LiME/src$ sudo insmod ./lime*.ko "path=tcp:4444 format=lime timeout=0" #Neste volcado de memoria RAM ábrese unha conexión en kaliA no porto TCP 4444 para que de forma remota establecendo conexión con ese porto gárdese o volcado nun ficheiro na máquina remota. A opción lime indica ese formato de copia, o cal e totalmente compatible co programa *volatility* [5][6][7]. A opción timeout=0 permite deshabilitar o "timeout" permitindo realizar unha copia máis fiable das páxinas de memoria.

   - O comando *sudo* é necesario porque precisamos permisos de *root* para poder cargar un módulo no kernel.
   - Non debemos facer nada no equipo ata que o comando remate, xa que senón estariamos "modificando" a estática da memoria RAM que pretendemos volcar.

   En kaliB(máquina remota)

   kali@kaliB:~$ nc 192.168.120.100 4444 > /mnt/remoto/RAMdump-remoto.mem #Facer o volcado de memoria RAM de forma remota e gardalo no ficheiro /mnt/remoto/RAMdump-remoto.mem. A opción lime indica ese formato de copia, o cal e totalmente compatible co programa *volatility* [5][6][7]. A opción timeout=0 permite deshabilitar o "timeout" permitindo realizar unha copia máis fiable das páxinas de memoria.

   - Agora xa dispoñemos dunha copia do que está a acontecer no volcado na memoria RAM no instante do volcado.

8. Tamaño dos ficheiros volcados (LiME [1]):

   En kaliA(máquina local)

   kali@kaliA:~$ free -m # Indicar a memoria RAM que dispón o sistema (neste caso 2GB)

```
               total        used        free      shared  buff/cache   available
Mem:            1967         795          92         128        1373        1171
Swap:              0           0           0
```

   kali@kaliA:~$ ls -lh /mnt/volcar/RAMdump-local.mem Listar en formato extendido o ficheiro que contén o volcado de memoria realizado. Podemos comprobar que ocupa 2.0G de espazo, que é o tamaño da mamoria RAM que posúe kaliA.

```
-rwxrwxrwx 1 root root 2.0G Jan 18 20:34 /mnt/volcar/RAMdump-local.mem
```

   kali@kaliA:~$ file /mnt/volcar/RAMdump-local.mem #Ver o tipo de ficheiro para RAMdump-local.mem (neste caso data=binario)

```
/mnt/volcar/RAMdump-local.mem: data
```

   En kaliB(máquina remota)

   kali@kaliB:~$ ls -lh /mnt/remoto/RAMdump-remoto.mem Listar en formato extendido o ficheiro que contén o volcado de memoria realizado. Podemos comprobar que ocupa 2.0G de espazo, que é o tamaño da mamoria RAM que posúe kaliA.

```
-rwxrwxrwx 1 root root 2.0G Jan 18 20:44 /mnt/remoto/RAMdump-remoto.mem
```

   kali@kaliB:~$ file /mnt/volcar/RAMdump-remoto.mem #Ver o tipo de ficheiro para RAMdump-remoto.mem (neste caso data=binario)

```
/mnt/remoto/RAMdump-remoto.mem: data
```

9. Desmontar os discos empregados para gardar o volcado de memoria RAM:

   En kaliA(máquina local)

   kali@kaliA:~$ sudo umount /mnt/volcar #Desmontar (deixar de facer uso) a partición primaria /dev/sdb1 que estaba montada en /mnt/volcar

   En kaliB(máquina remota)

   kali@kaliB:~$ sudo umount /mnt/remoto #Desmontar (deixar de facer uso) a partición primaria /dev/sdb1 que estaba montada en /mnt/remoto

Volcado de memoria RAM en sistemas MS Windows

Imos facer un volcado da memoria RAM dun sistema operativo MS Windows no propio disco que contén o sistema operativo. Tamén podería facerse a través dun disco duro (externo) que non contén o propio sistema operativo. Basicamente:

1. Instalar o programa para volcar a memoria RAM no equipo do cal queremos volcar a memoria.
2. Realizar o volcado en local.

Máquina virtual C: MS Windows 1X x64

1. Dirixirse á url [3] e descargar o ficheiro winpmem 64bits:

2. Executar unha consola con permisos de administrador e executar o ficheiro descargado para obter un volcado de memoria RAM:

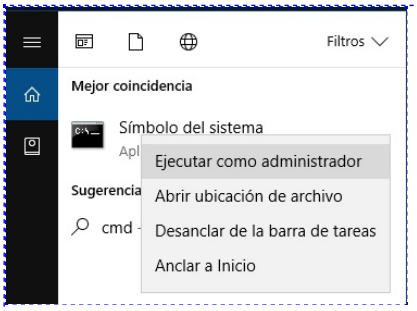


Fig. 1: cmd → Abrir como administrador

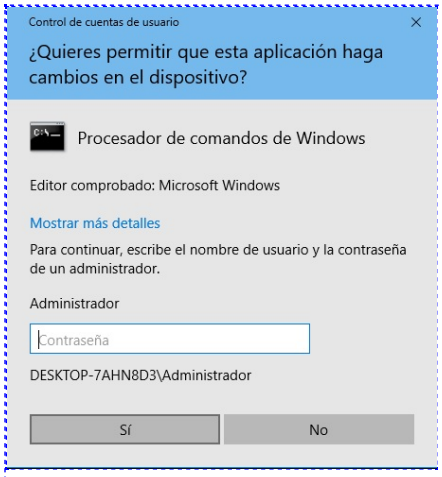


Fig. 2: Permitir abrir como administrador

```
c:\Users\usuario\Downloads>winpmem_mini_x64_rc2.exe
WinPmem64
Winpmem - A memory imager for windows.
Copyright Michael Cohen (scudette@gmail.com) 2012-2014.

Version 2.0.1 Oct 13 2020
Usage:
  winpmem_mini_x64_rc2.exe [option] [output path]

Option:
  -l    Load the driver and exit.
  -u    Unload the driver and exit.
  -d [filename]
        Extract driver to this file (Default use random name).
  -h    Display this help.
  -w    Turn on write mode.
  -0    Use MmMapIoSpace method.
  -1    Use \\Device\PhysicalMemory method (Default for 32bit OS).
  -2    Use PTE remapping (AMD64 only - Default for 64bit OS).

NOTE: an output filename of - will write the image to STDOUT.

Examples:
winpmem_mini_x64_rc2.exe physmem.raw
Writes an image to physmem.raw
```

Fig. 3: Ver axuda do comando

```
c:\Users\usuario\Downloads>winpmem_mini_x64_rc2.exe RAMdump-windows.raw
WinPmem64
Extracting driver to C:\Users\ADMINI~1\AppData\Local\Temp\pme1148.tmp
Driver Unloaded.
Loaded Driver C:\Users\ADMINI~1\AppData\Local\Temp\pme1148.tmp.
Deleting C:\Users\ADMINI~1\AppData\Local\Temp\pme1148.tmp
The system time is: 20:27:49
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AA000
 3 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0x7FEED000
max_physical_memory_ 0x7fff0000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000

00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x9f000

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
 - length: 0x61000

00% 0x0009F000 .
copy_memory
 - start: 0x100000
 - end: 0x102000
```

Fig. 4: Crear volcado da RAM no ficheiro RAMdump-windows.raw

```
Seleccionar Administrador: Símbolo del sistema
 - start: 0x100000
 - end: 0x102000

00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
 - length: 0x1000

00% 0x00102000 .
copy_memory
 - start: 0x103000
 - end: 0x7fff0000

00% 0x00103000 ..............................................
39% 0x32103000 ..............................................
78% 0x64103000 ..........................
The system time is: 20:28:13
Driver Unloaded.
```

Fig. 5: Proceso de volcado

```
c:\Users\usuario\Downloads>dir RAMdump-windows.raw
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1AC4-C86A

 Directorio de c:\Users\usuario\Downloads

20/01/2024  21:28     2.147.418.112 RAMdump-windows.raw
               1 archivos  2.147.418.112 bytes
               0 dirs  32.623.800.320 bytes libres

c:\Users\usuario\Downloads>
```

Fig. 6: Proceso rematado. Listado do ficheiro xerado

Volcado de memoria RAM en Máquinas virtuais Oracle VirtualBox

Basicamente dende a máquina anfitrión(neste caso unha distro GNU/Linux) executamos o comando *VboxManage* coa opción *debugvm* indicando o nome da máquina virtual da cal imos facer o volcado de memoria RAM e o nome do ficheiro onde imos gardar o volcado xerado:

```
$ VBoxManage debugvm  dumpvmcore [--filename=name]
```

Imos facer 2 volcados de memoria RAM:

1. Un volcado dunha máquina virtual cunha distro GNU/Linux arrancada: KaliA-XY

   ```
   $ VBoxManage debugvm KaliA-XY dumpvmcore --filename=RAMdump-MV.elf

   $ ls -lh RAMdump-MV.elf
   -rwxrwxrwx 1 usuario usuario 2,1G ene 18 22:23 RAMdump-MV.elf
   ```

2. Un volcado dunha máquina virtual cun sistema operativo MS Windows arrancado: Windows64

   ```
   $ VBoxManage debugvm Windows64 dumpvmcore --filename=RAMdump-MV-Windows64.elf

   $ ls -lh RAMdump-MV-Windows64.elf
   -rwxrwxrwx 1 usuario usuario 2,2G ene 18 22:26 RAMdump-MV-Windows64.elf
   ```

Ricardo Feijoo Costa