Universidad Carlos III de Madrid

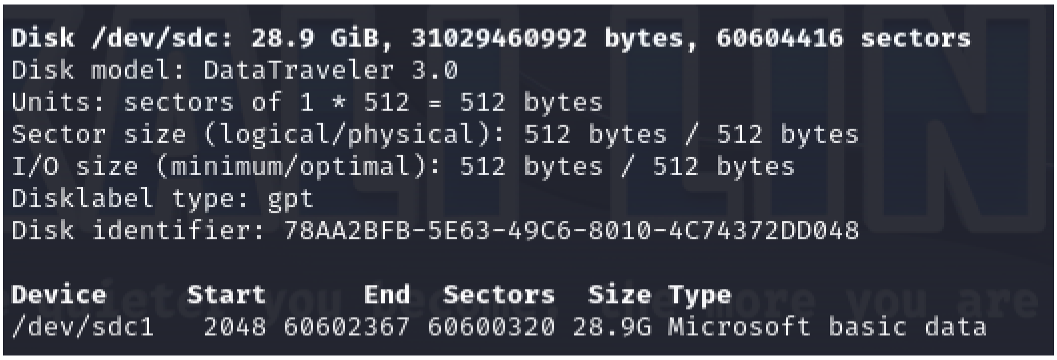
Reporte de Data carving - USB

Juan Diego Llano Miraval

Fecha: 16/05/2024

procedure

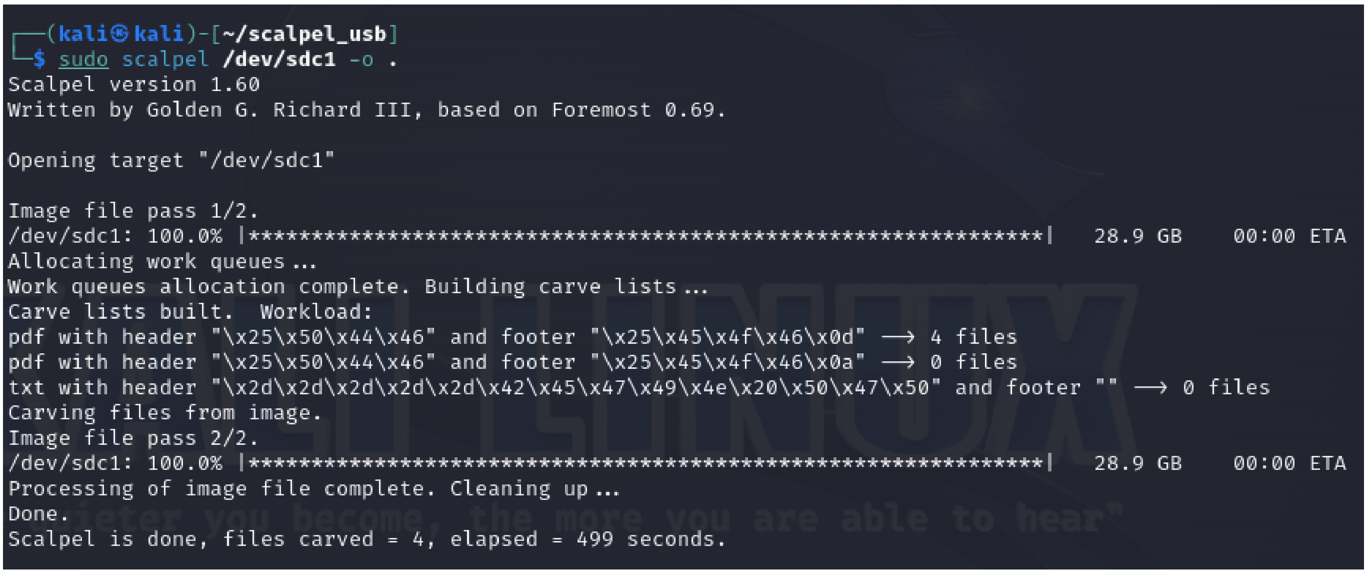
The first after deleting some files, is connecting the usb into our linux machine and check for the disk:



```
Disk /dev/sdc: 28.9 GiB, 31029460992 bytes, 60604416 sectors
Disk model: DataTraveler 3.0
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: gpt
Disk identifier: 78AA2BFB-5E63-49C6-8010-4C74372DD048

Device      Start      End  Sectors  Size Type
/dev/sdc1    2048 60602367 60600320 28.9G Microsoft basic data
```

after this we use Scalpel to check for deleted files into the USB disk.

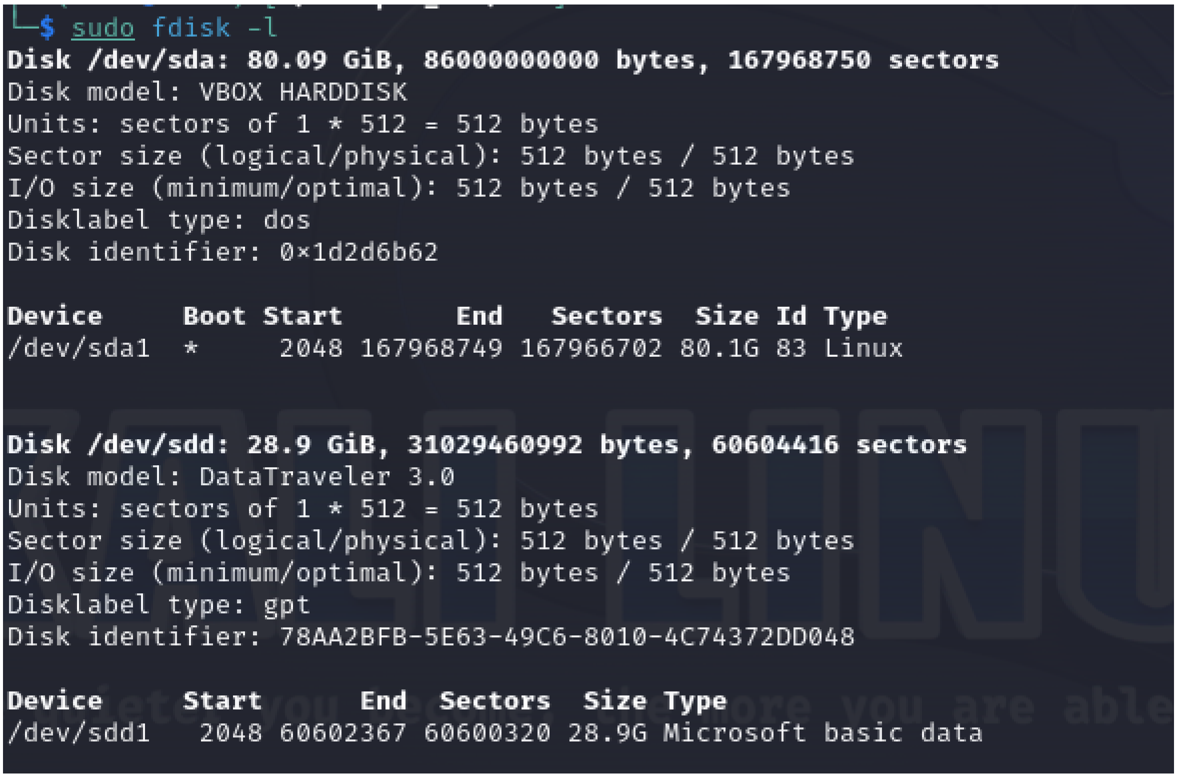


```
┌──(kali㉿kali)-[~/scalpel_usb]
└─$ sudo scalpel /dev/sdc1 -o .
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sdc1"

Image file pass 1/2.
/dev/sdc1: 100.0% |***************************************************************|   28.9 GB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" ⟶ 4 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" ⟶ 0 files
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" ⟶ 0 files
Carving files from image.
Image file pass 2/2.
/dev/sdc1: 100.0% |***************************************************************|   28.9 GB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 4, elapsed = 499 seconds.
```

After this, we return the USB to the windows environment and run a quick format on the USB. Then we plug it into the Linux and check the disk once again:



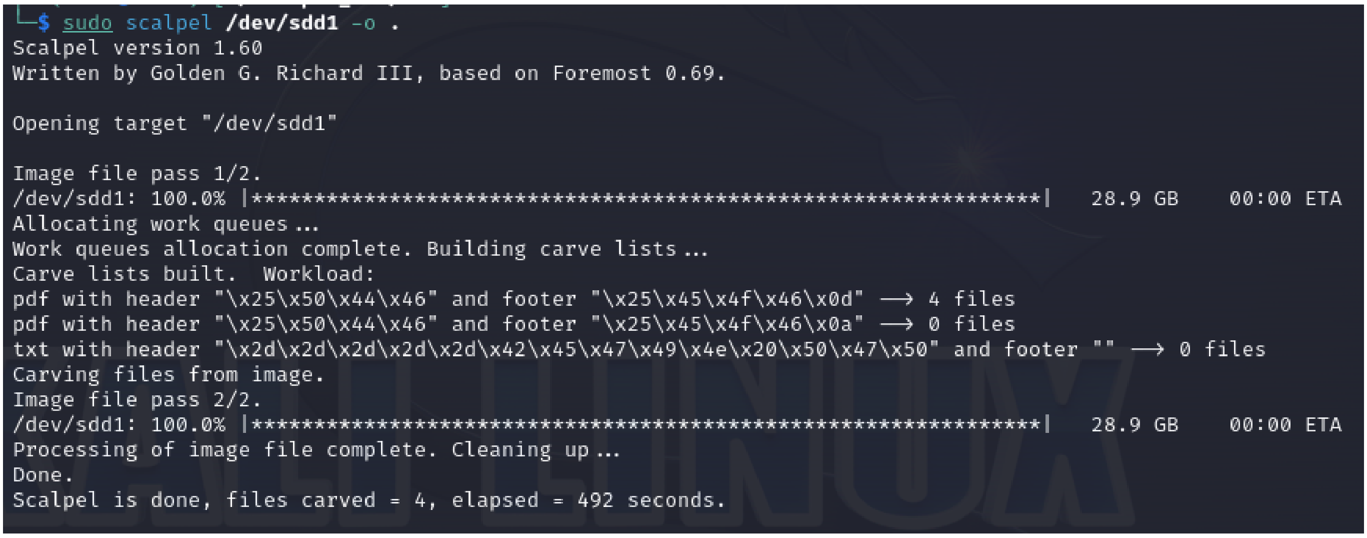
```
└─$ sudo fdisk -l
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×1d2d6b62

Device     Boot Start       End   Sectors  Size Id Type
/dev/sda1  *     2048 167968749 167966702 80.1G 83 Linux


Disk /dev/sdd: 28.9 GiB, 31029460992 bytes, 60604416 sectors
Disk model: DataTraveler 3.0
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: gpt
Disk identifier: 78AA2BFB-5E63-49C6-8010-4C74372DD048

Device     Start      End  Sectors  Size Type
/dev/sdd1   2048 60602367 60600320 28.9G Microsoft basic data
```

after this we perform another scan with scalpel:

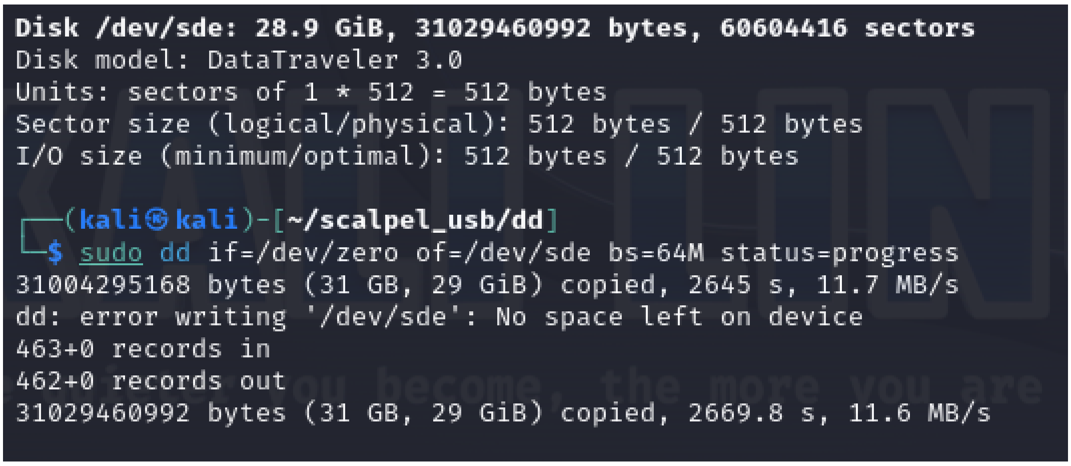


```
└─$ sudo scalpel /dev/sdd1 -o .
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sdd1"

Image file pass 1/2.
/dev/sdd1: 100.0% |****************************************************************|   28.9 GB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" ⟶ 4 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" ⟶ 0 files
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" ⟶ 0 files
Carving files from image.
Image file pass 2/2.
/dev/sdd1: 100.0% |****************************************************************|   28.9 GB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 4, elapsed = 492 seconds.
```

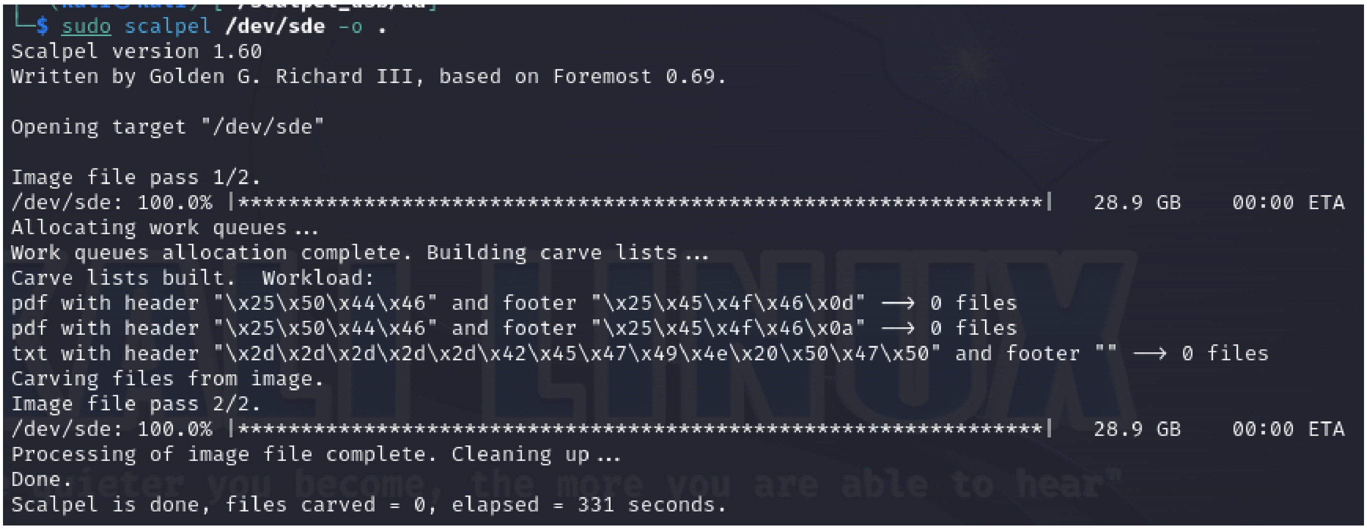
After this step, we put some PDFs into the USB and run a dd command to clear the information in the USB:



```
Disk /dev/sde: 28.9 GiB, 31029460992 bytes, 60604416 sectors
Disk model: DataTraveler 3.0
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

┌──(kali㉿kali)-[~/scalpel_usb/dd]
└─$ sudo dd if=/dev/zero of=/dev/sde bs=64M status=progress
31004295168 bytes (31 GB, 29 GiB) copied, 2645 s, 11.7 MB/s
dd: error writing '/dev/sde': No space left on device
463+0 records in
462+0 records out
31029460992 bytes (31 GB, 29 GiB) copied, 2669.8 s, 11.6 MB/s
```

and finally we run a final scalpel:



```
┌──(kali㉿kali)-[~/scalpel_usb/dd]
└─$ sudo scalpel /dev/sde -o .
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sde"

Image file pass 1/2.
/dev/sde: 100.0% |*****************************************************************|   28.9 GB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
/dev/sde: 100.0% |*****************************************************************|   28.9 GB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 0, elapsed = 331 seconds.
```

There were no files inside the drive after the dd format. This is because dd is writing the data of the drive into zeros, and when we usually delete or quick formate a drive, it doesn't errase the data, the space is free, but it contains the information. This is why before we could recover the files.