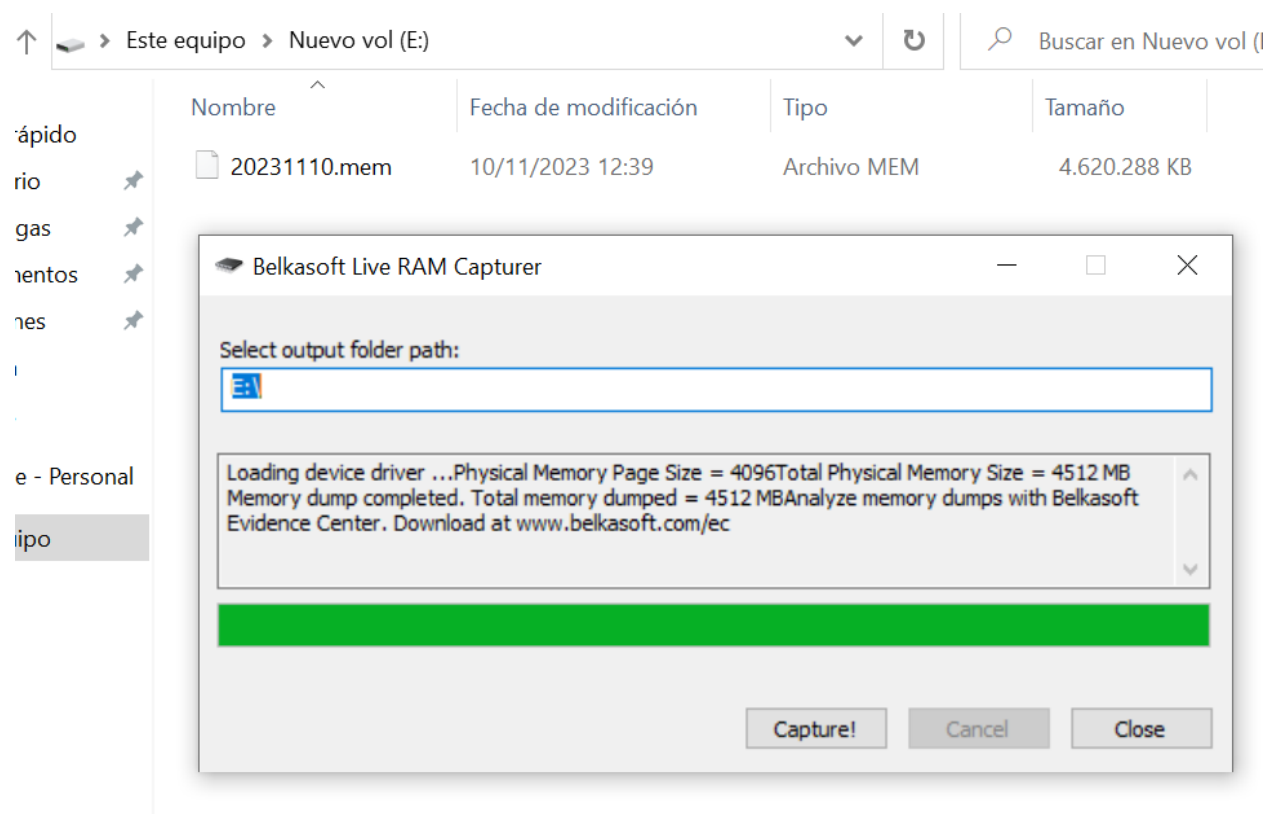


## Práctica 3

# Adquisición de evidencia en caliente

Comenzamos con una máquina virtual que ejecuta Windows 10. Le hemos incorporado un disco duro adicional destinado a almacenar la recopilación de evidencias. En este escenario particular, estamos extrayendo datos de la RAM, la cual es extremadamente susceptible a modificaciones. Por esta razón, optamos por utilizar programas portables que no necesitan instalación, como FTK Imager o, en mi caso, RAM Capture.



Posteriormente comprobamos el hash de las evidencias obtenidas

```
E:\>certutil -hashfile 20231110.mem SHA512
SHA512 hash de 20231110.mem:
de7b30c30f58a40a59a8eb2e152c42dee6f79258ad3dbcb397d0829e0c7faf95812f05cb4375bcc00660d6cc9df888882682dd353daba2c581f483d09b1db89e
CertUtil: -hashfile comando completado correctamente.
```

Para llevar a cabo la adquisición de evidencias en Linux, emplearemos la herramienta Microsoft AVML. Esto se logra fácilmente con un solo comando, invocando el ejecutable y especificando la ubicación donde se deben almacenar los datos recopilados.

```
jose@jose-almiron: ~/Descargas/avml/x86_64-unknown-linux-gnu/release
$ sudo ./avml /media/jose/Storage/imagememory.dmp
```

```
jose@jose-almiron: /media/jose/Storage$ ls -lha
total 2,0G
drwx----- 3 jose jose 4,0K nov 10 13:16 .
drwxr-x---+ 3 root root 4,0K nov 10 13:11 ..
-rw----- 1 root root 2,0G nov 10 13:17 imagememory.dmp
```

Finalmente obtenemos el hash de la evidencia

```
jose@jose-almiron: /media/jose/Storage$ sudo sha512sum imagememory.dmp
7dee3ba0bae2274c45be734bae62464320904151772c4d7b79ed441a93fbc0997361a185fce49cdd2ccd65a85f21c0f8ab401632c7eb9d37c5cf377c8c
210841  imagememory.dmp
jose@jose-almiron: /media/jose/Storage$
```