Aquisição física feita com duas ferramentas diferentes para determinar se a montagem do disco foi feita automaticamente e se os hash são iguais.

Laboratório para comparar uma aquisição física feita com o EnCase Acquisition e o Guymager.

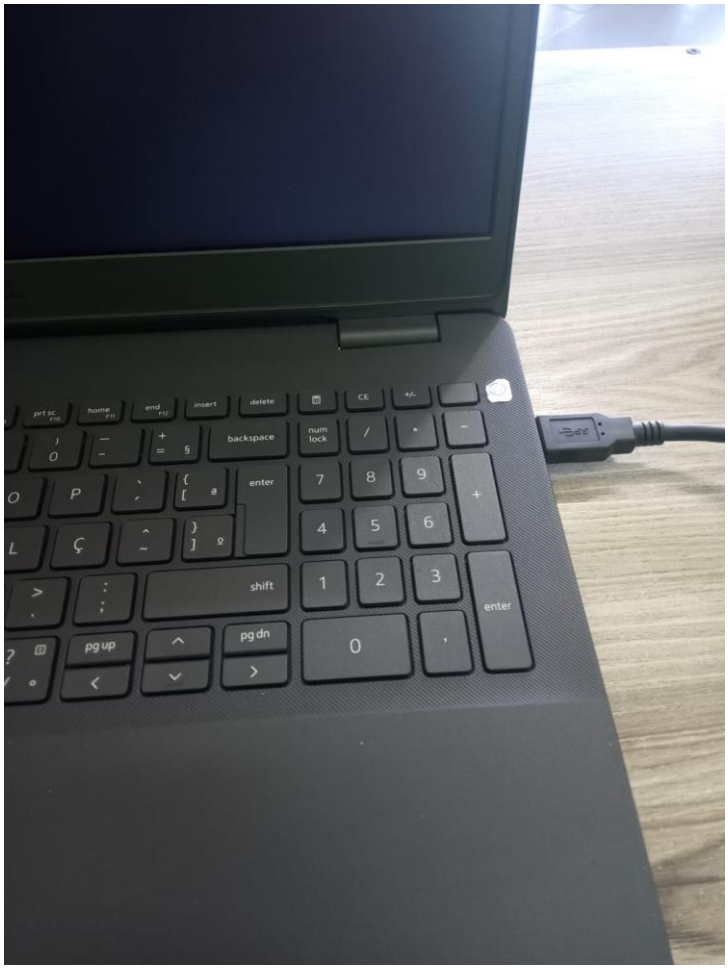
Para esse teste foi usado um notebook Dell Vostro 3500 i7 8gb SSD 256 com placa de vídeo iris com dual boot Windows 10 e Ubuntu 4:5.18.7-0ubuntu0.1.

Em toda aquisição forense cuidados com a montagem automática do disco e bloqueio de escrita são necessários para que as possíveis provas ali recuperadas tenham validade nos tribunais.

Nesse teste foi usado um HD 160GB como dispositivo questionado e um adaptador sata USB 3.0 com fonte.

Agora no sistema Ubuntu antes de conectar o disco, a montagem automática está desabilitada. Caso você não saiba desabilitar a montagem no Ubuntu, segue o link de um artigo que eu explico como desabilitar a montagem automática de disco no Linux; https://www.linkedin.com/pulse/uma-abordagem-gr%C3%A1fica-sobre-como-desabilitar-montagem-jonatas-costa/


WHERE "Someone"
LIKE '%You%'
...
/> no results !
LG
160GB

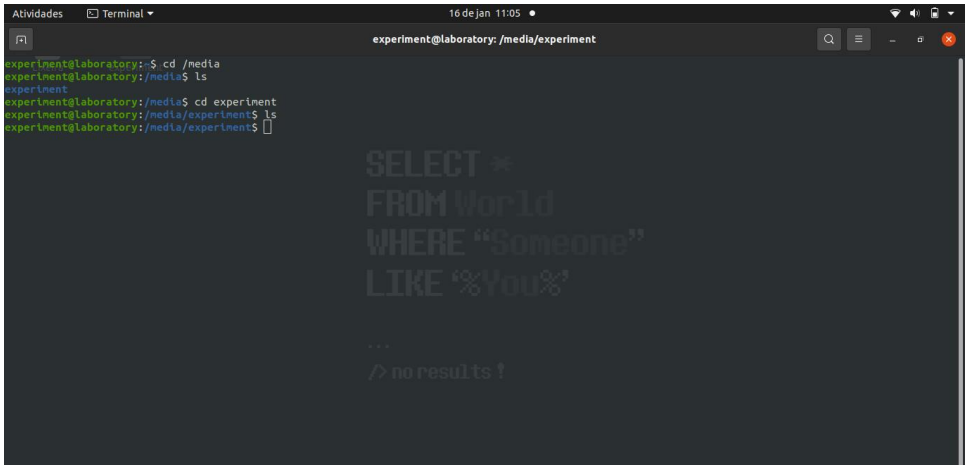


Com o disco conectado o comando sudo fdisk - l lista todos os discos conectados que estão em /dev.

```
Disco /dev/sda: 149,5 GiB, 160040803840 bytes, 312579695 setores
Disk model: 00AAJS-00M0A0
Unidades: setor de 1 * 512 = 512 bytes
Tamanho de setor (lógico/físico): 512 bytes / 4096 bytes
Tamanho E/S (mínimo/ótimo): 4096 bytes / 4096 bytes
Tipo de rótulo do disco: dos
Identificador do disco: 0x08881bfd

Dispositivo Inicializar Início       Fim   Setores Tamanho Id Tipo
/dev/sda1                2048 312575999 312573952    149G  7 HPFS/NTFS/exFAT
experiment@laboratory:~$
```

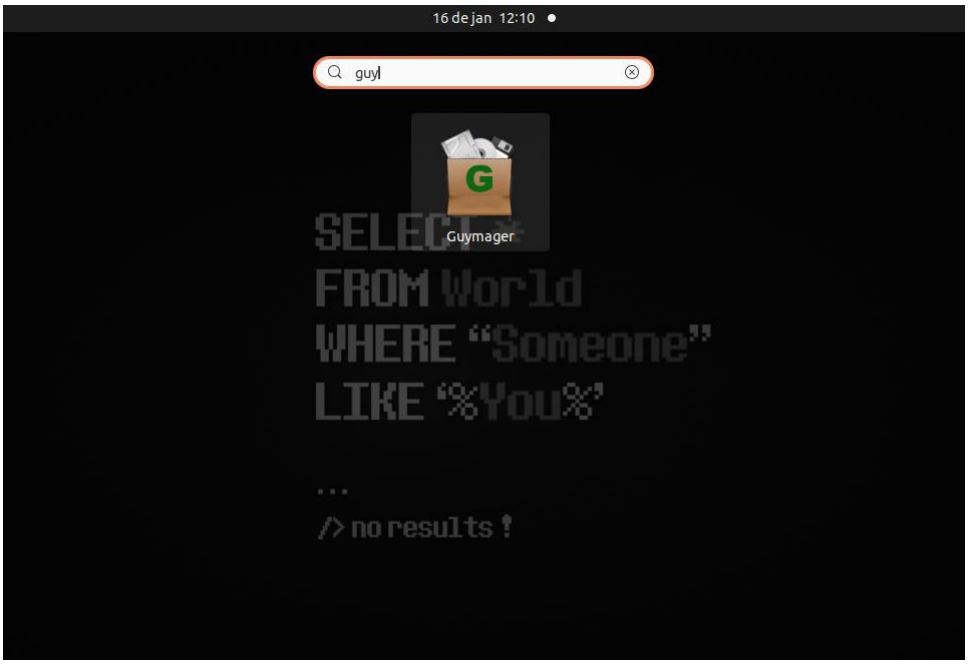
Digitando o comando: cd /media

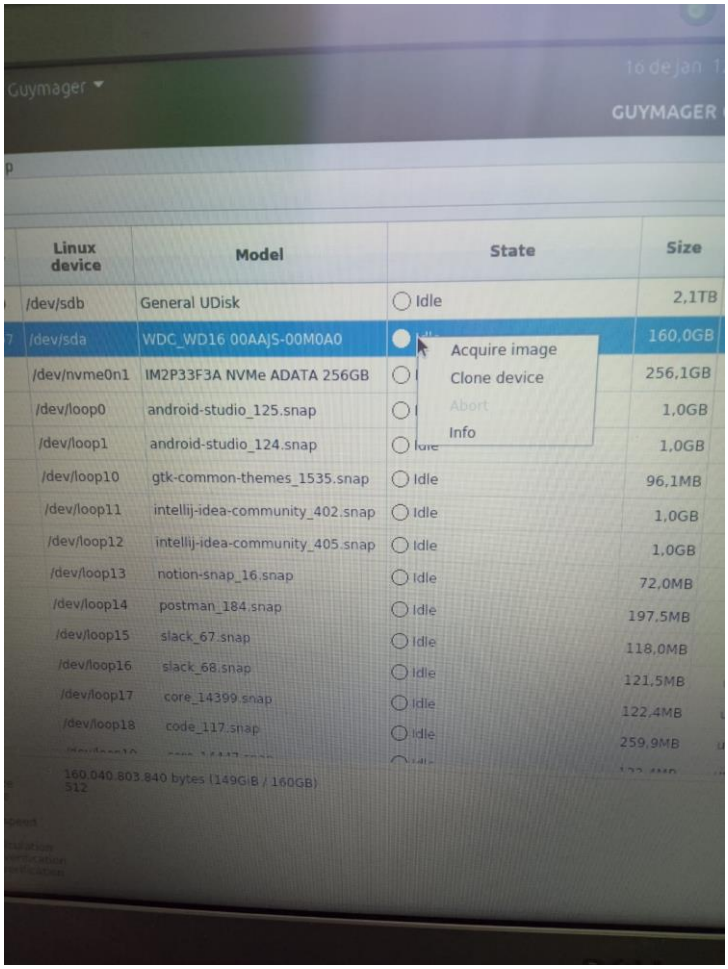
Esse comando lista todos os discos montados no sistema.



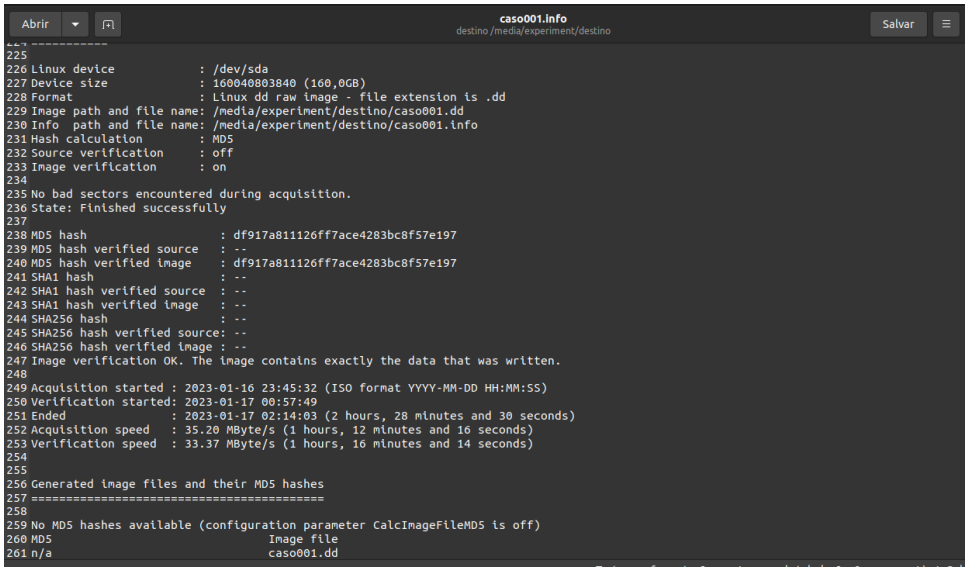
Na imagem acima fica claro que nem um disco foi montado.

Agora com o Guymager aberto a aquisição física será executada.

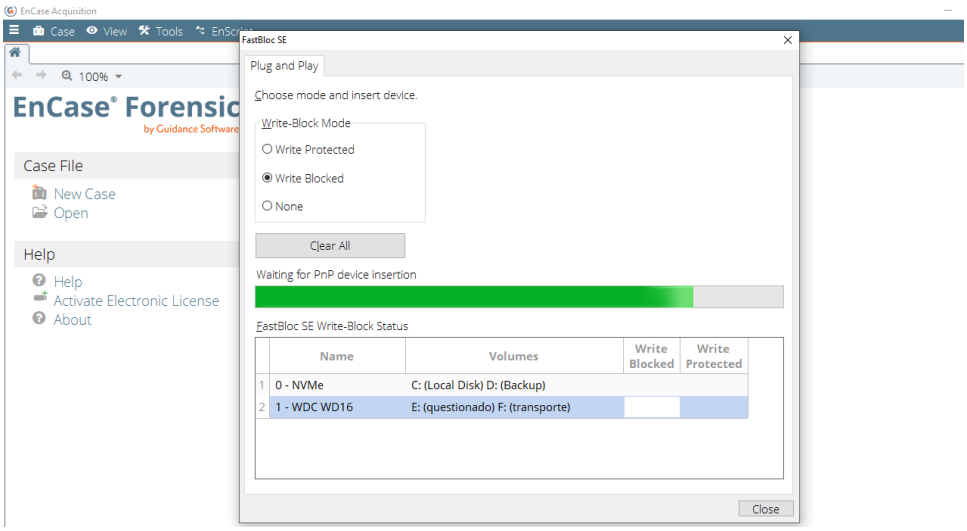




Após a aquisição pelo Guymager, podemos ver que o hash é df917a811126ff7ace4283bc8f57e197.



Agora com o sistema Windows 10 o disco questionado será inserido, mas antes com o uso da ferramenta EnCase Acquisition será ativado o bloqueio de escrita.

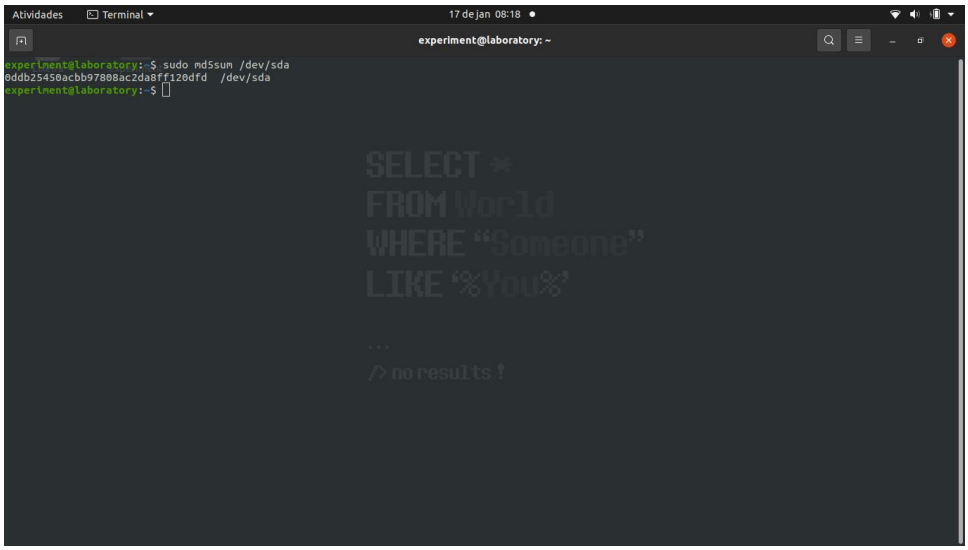


Como é possível observar o bloqueio de escrita é ineficaz com o uso de adaptador do tipo sata 3.0 com disco conectado a ele.

Para melhor compreensão, o disco será conectado novamente ao sistema Ubuntu que tem a montagem automática de discos desabilitada e o cálculo de hash será calculado novamente.

Com o comando md5sum /endereço do disco o hash foi recalculado.

Como foi possível determinar o hash do disco foi modificado devido a ferramenta EnCase Acquisition não bloquear a escrita do dico via adaptador usb sata 3.0.

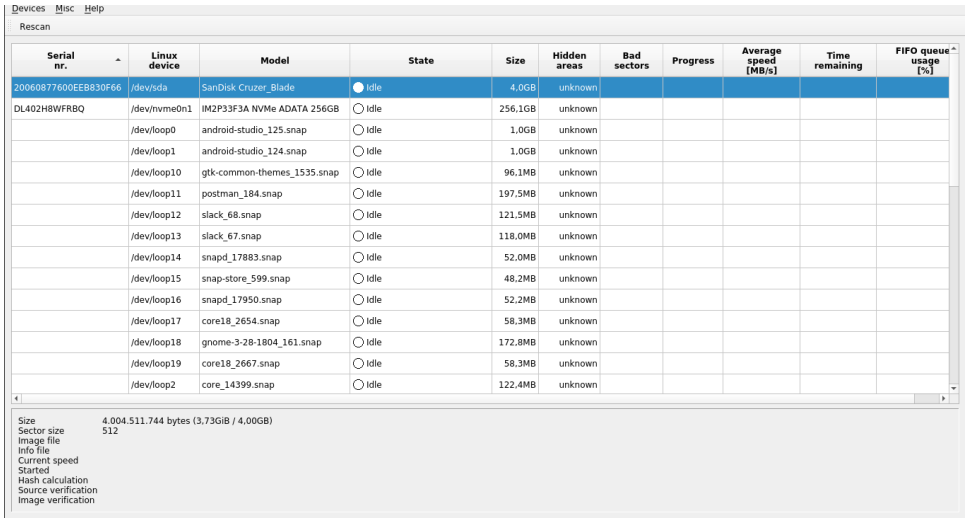


Como segundo experimento, o mesmo teste será corrido com um pen-drive de 4GB.

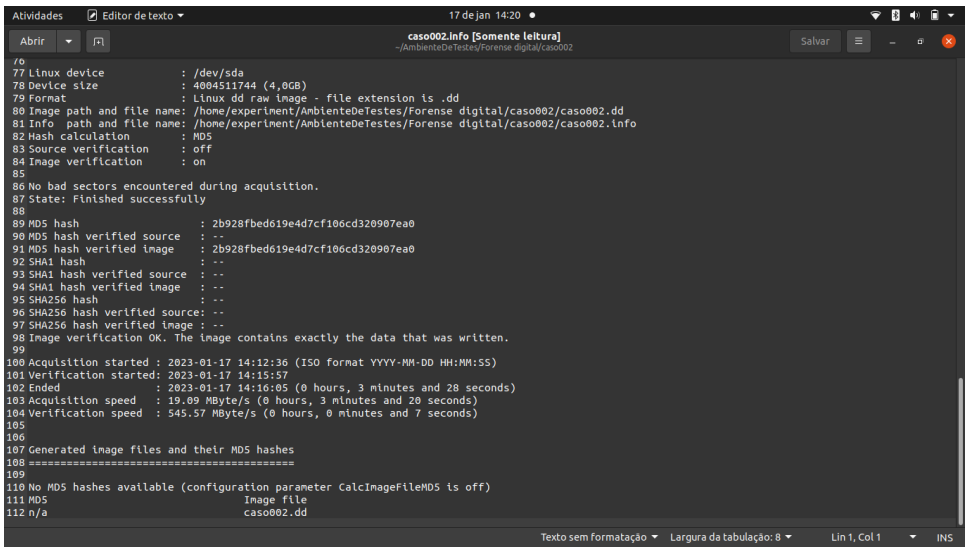
Localização do pen-drive:

```
Disco /dev/sda: 3,75 GiB, 4004511744 bytes, 7821312 setores
Disk model: Cruzer Blade
Unidades: setor de 1 * 512 = 512 bytes
Tamanho de setor (lógico/físico): 512 bytes / 512 bytes
Tamanho E/S (mínimo/ótimo): 512 bytes / 512 bytes
Tipo de rótulo do disco: dos
Identificador do disco: 0x500a0dff

Dispositivo Inicializar     Início        Fim    Setores Tamanho Id Tipo
/dev/sda1               1634493285 3550204804 1915711520  913,5G 6e desconhecida
/dev/sda2                     2573       2573          0       0B 63 GNU HURD ou SysV
/dev/sda4                 28049408   28049848        441  220,5K  0 Vazia

Partições lógicas fora da ordem do disco.
experiment@laboratory:~$
```

Aquisição com o Guymager:

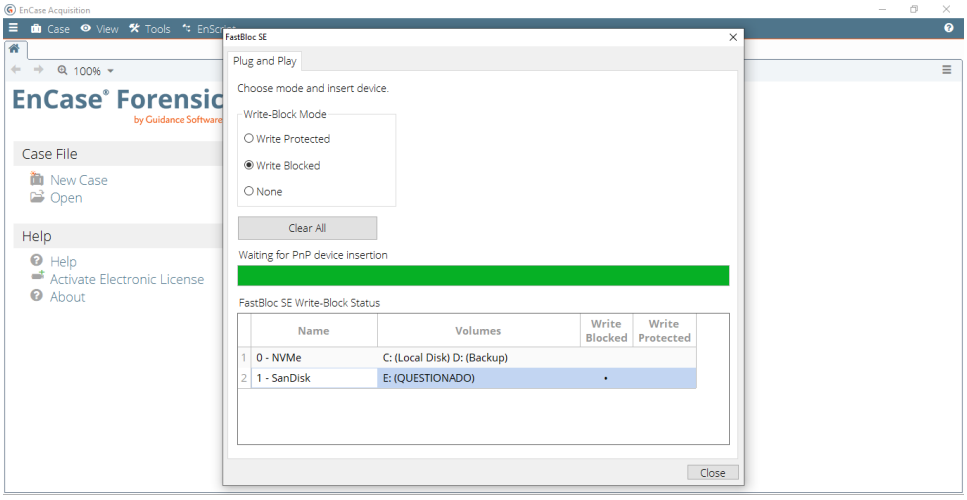


Hash da aquisição:

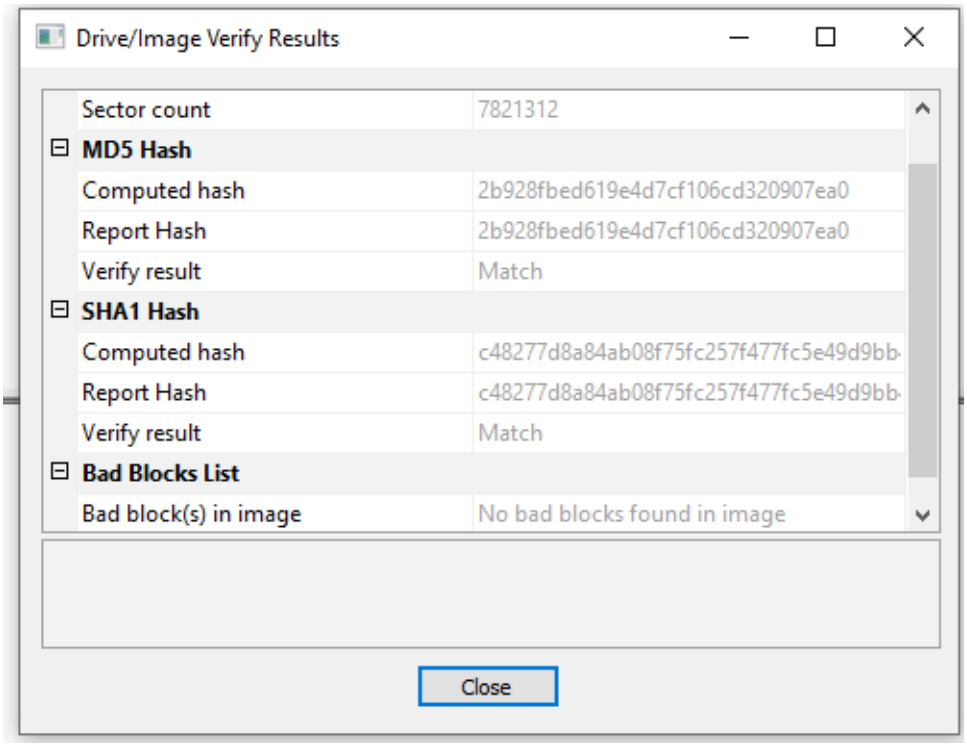


MD5 hash : 2b928fbed619e4d7cf106cd320907ea0

Bloqueio de escrita com o EnCase Acquisition:



Aquisição com o FTK imager:



MD5 hash com FTK imager : 2b928fbed619e4d7cf106cd320907ea0

MD5 hash com Guymager : 2b928fbed619e4d7cf106cd320907ea0

Então é possível determinar que no uso de um pen-drive o disco não foi modificado em ambas as ferramentas.