

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/>





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.

```
Atividades Terminal 16 de jan 11:05
experiment@laboratory: /media/experiment

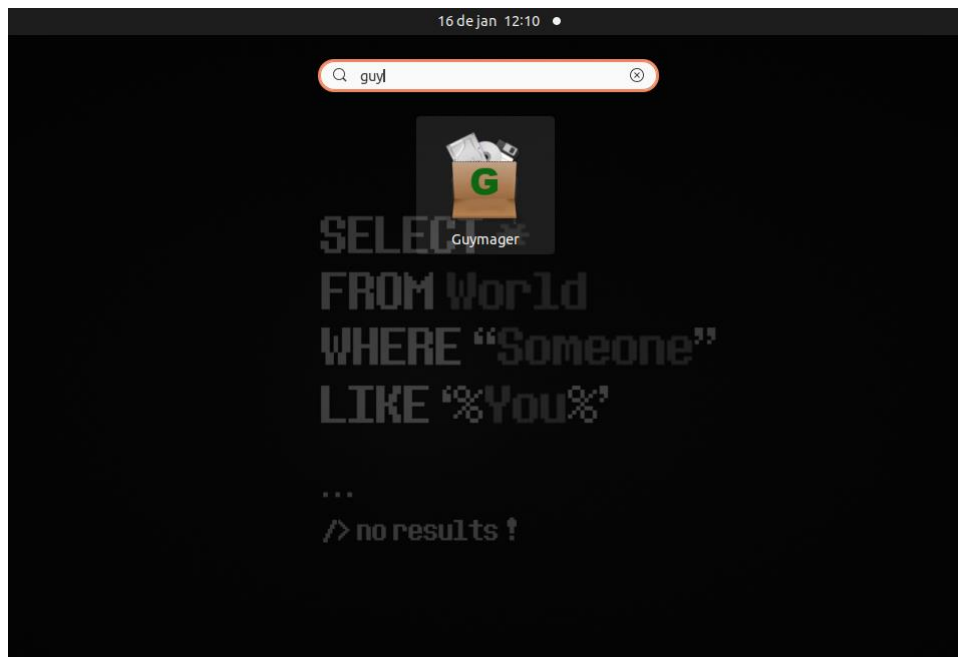
experiment@laboratory:~$ cd /media
experiment@laboratory:/media$ ls
experiment
experiment@laboratory:/media$ cd experiment
experiment@laboratory:/media/experiment$ ls
experiment@laboratory:/media/experiment$

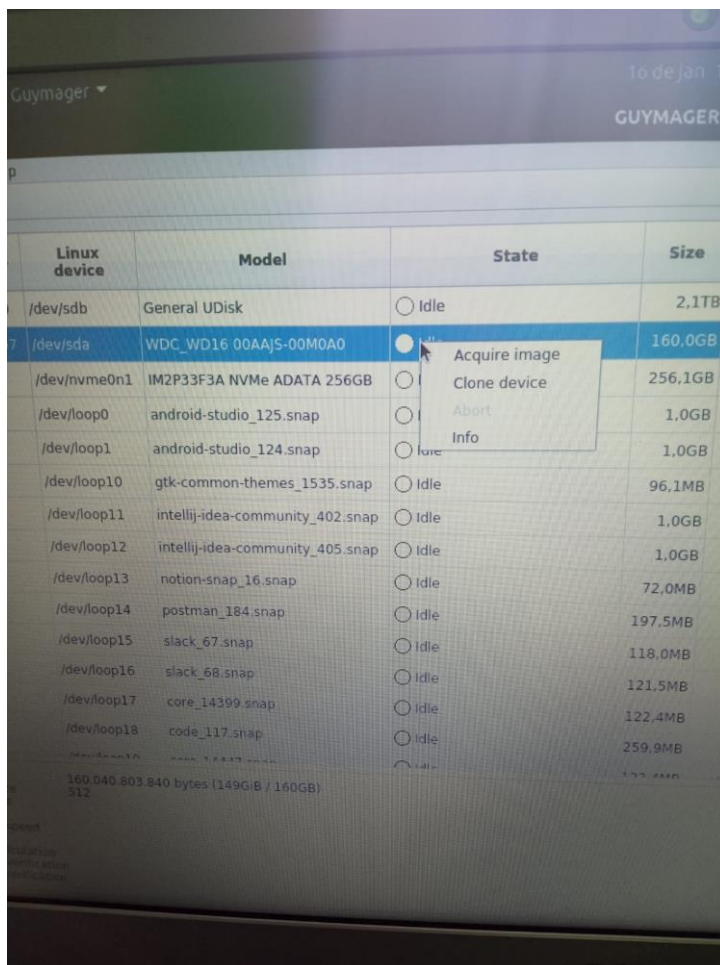
SELECT *
FROM World
WHERE "Someone"
LIKE "%You%"

...
/> no results !
```

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.

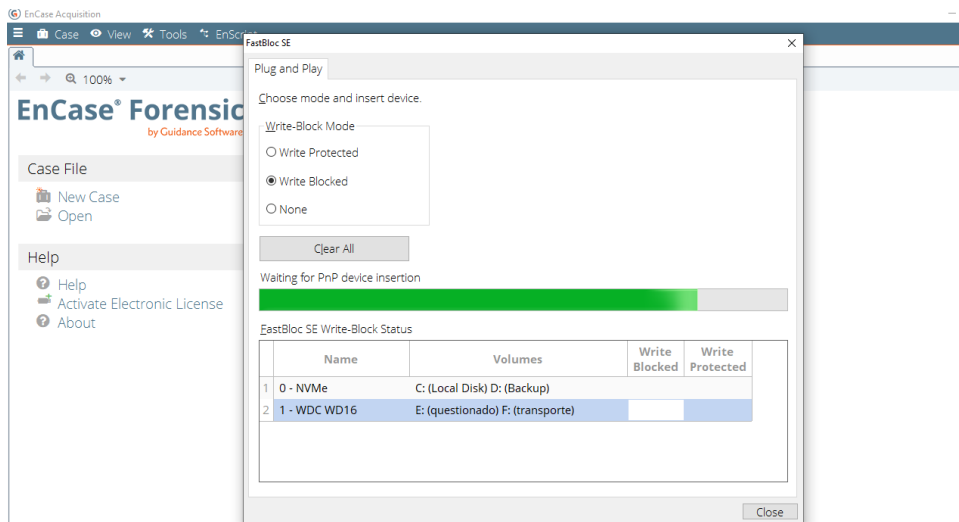
```

Abrir  caso001.info  Salvar
destino /media/experiment/destino

225 -----
226 Linux device      : /dev/sda
227 Device size      : 160040803840 (160.0GB)
228 Format            : Linux dd raw image - file extension is .dd
229 Image path and file name: /media/experiment/destino/caso001.dd
230 Info path and file name: /media/experiment/destino/caso001.info
231 Hash calculation  : MD5
232 Source verification : off
233 Image verification : on
234
235 No bad sectors encountered during acquisition.
236 State: Finished successfully
237
238 MD5 hash          : df917a811126ff7ace4283bc8f57e197
239 MD5 hash verified source : --
240 MD5 hash verified image  : df917a811126ff7ace4283bc8f57e197
241 SHA1 hash          : --
242 SHA1 hash verified source : --
243 SHA1 hash verified image  : --
244 SHA256 hash         : --
245 SHA256 hash verified source: --
246 SHA256 hash verified image : --
247 Image verification OK. The image contains exactly the data that was written.
248
249 Acquisition started : 2023-01-16 23:45:32 (ISO format YYYY-MM-DD HH:MM:SS)
250 Verification started: 2023-01-17 00:57:49
251 Ended              : 2023-01-17 02:14:03 (2 hours, 28 minutes and 30 seconds)
252 Acquisition speed   : 35.20 MByte/s (1 hours, 12 minutes and 16 seconds)
253 Verification speed  : 33.37 MByte/s (1 hours, 16 minutes and 14 seconds)
254
255
256 Generated image files and their MD5 hashes
257 -----
258
259 No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
260 MD5          Image file
261 n/a          caso001.dd

```

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.

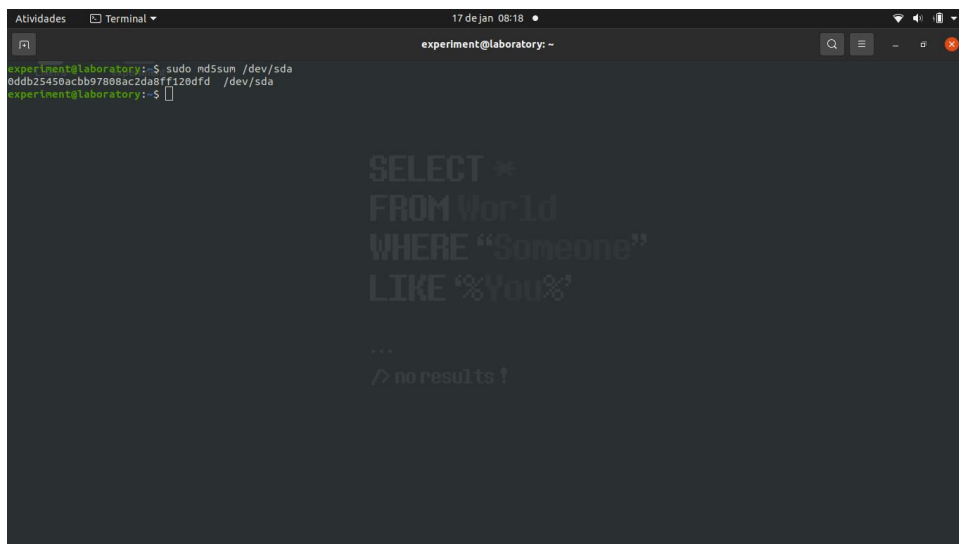


Como é possível observar o bloqueio de escrita é ineficaz com o uso de adaptador do tipo sata 3.0 com disco conectado a ele.

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: Cruzier 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:

DevicesMiscHelp

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queue usage [%]
20060877600EEB830F66	/dev/sda	SanDisk Cruzer_Blade	● Idle	4.0GB	unknown					
DL402HBWFRBQ	/dev/vmm0n1	IM2P3F3A NVMe ADATA 256GB	○ Idle	256.1GB	unknown					
	/dev/loop0	android-studio_125.snap	○ Idle	1.0GB	unknown					
	/dev/loop1	android-studio_124.snap	○ Idle	1.0GB	unknown					
	/dev/loop10	gtk-common-themes_1535.snap	○ Idle	96.1MB	unknown					
	/dev/loop11	postman_184.snap	○ Idle	197.5MB	unknown					
	/dev/loop12	slack_68.snap	○ Idle	121.5MB	unknown					
	/dev/loop13	slack_67.snap	○ Idle	118.0MB	unknown					
	/dev/loop14	snapd_17883.snap	○ Idle	52.0MB	unknown					
	/dev/loop15	snap-store_599.snap	○ Idle	48.2MB	unknown					
	/dev/loop16	snapd_17950.snap	○ Idle	52.2MB	unknown					
	/dev/loop17	core18_2654.snap	○ Idle	58.3MB	unknown					
	/dev/loop18	gnome-3-28-1804_161.snap	○ Idle	172.8MB	unknown					
	/dev/loop19	core18_2667.snap	○ Idle	58.3MB	unknown					
	/dev/loop2	core_14399.snap	○ Idle	122.4MB	unknown					
Size 4.004.511.744 bytes (3.73GiB / 4.00GB)										
Sector size 512										
Image file										
Info file										
Current speed										
Started										
Hash calculation										
Source verification										
Image verification										

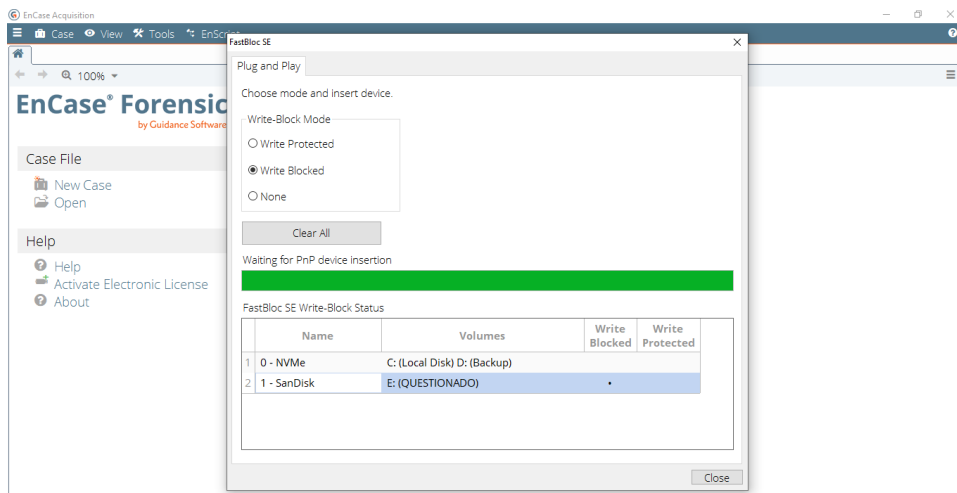
Hash da aquisição:

```
Atividades Editor de texto 17 de jan 14:20
caso002.info [Somente leitura]
~/AmbienteDeTestes/Forense digital/caso002

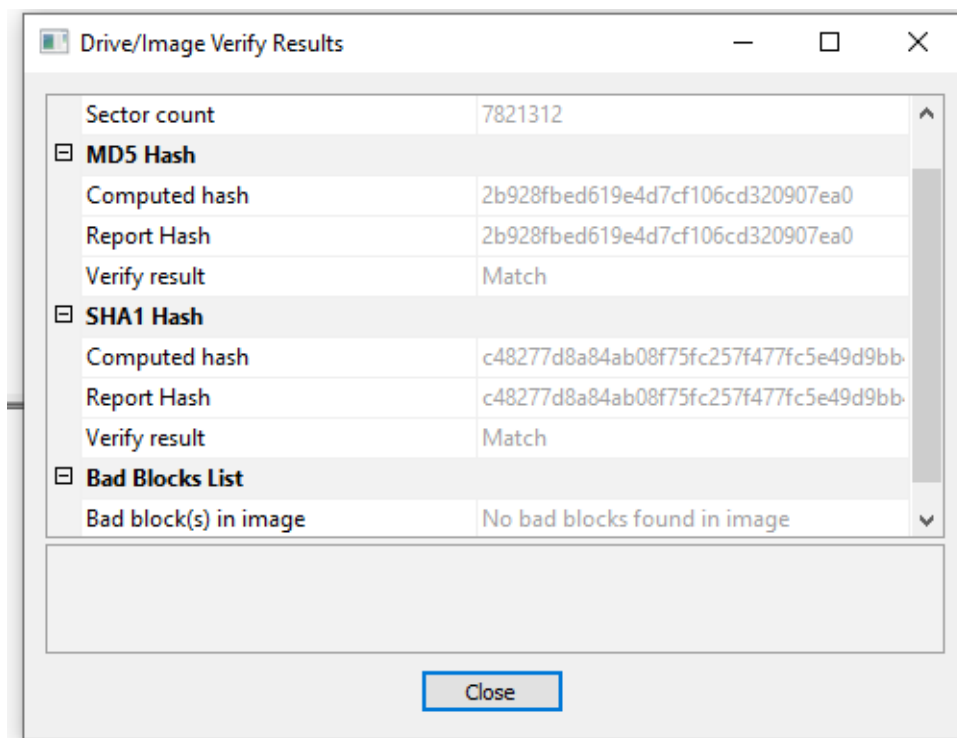
77 Linux device      : /dev/sda
78 Device size       : 4004511744 (4,0GB)
79 Format            : Linux dd raw image - file extension is .dd
80 Image path and file name: /home/experiment/AmbienteDeTestes/Forense digital/caso002/caso002.dd
81 Info path and file name: /home/experiment/AmbienteDeTestes/Forense digital/caso002/caso002.info
82 Hash calculation   : MD5
83 Source verification : off
84 Image verification : on
85
86 No bad sectors encountered during acquisition.
87 State: Finished successfully
88
89 MD5 hash           : 2b928fbed619e4d7cf106cd320907ea0
90 MD5 hash verified source : --
91 MD5 hash verified image : 2b928fbed619e4d7cf106cd320907ea0
92 SHA1 hash          : --
93 SHA1 hash verified source : --
94 SHA1 hash verified image : --
95 SHA256 hash         : --
96 SHA256 hash verified source: --
97 SHA256 hash verified image : --
98 Image verification OK. The image contains exactly the data that was written.
99
100 Acquisition started : 2023-01-17 14:12:36 (ISO format YYYY-MM-DD HH:MM:SS)
101 Verification started: 2023-01-17 14:15:57
102 Ended               : 2023-01-17 14:16:05 (0 hours, 3 minutes and 28 seconds)
103 Acquisition speed   : 19.09 MByte/s (0 hours, 3 minutes and 20 seconds)
104 Verification speed  : 545.57 MByte/s (0 hours, 0 minutes and 7 seconds)
105
106
107 Generated image files and their MD5 hashes
108 =====
109
110 No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
111 MD5      Image file
112 n/a      caso002.dd
```

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.