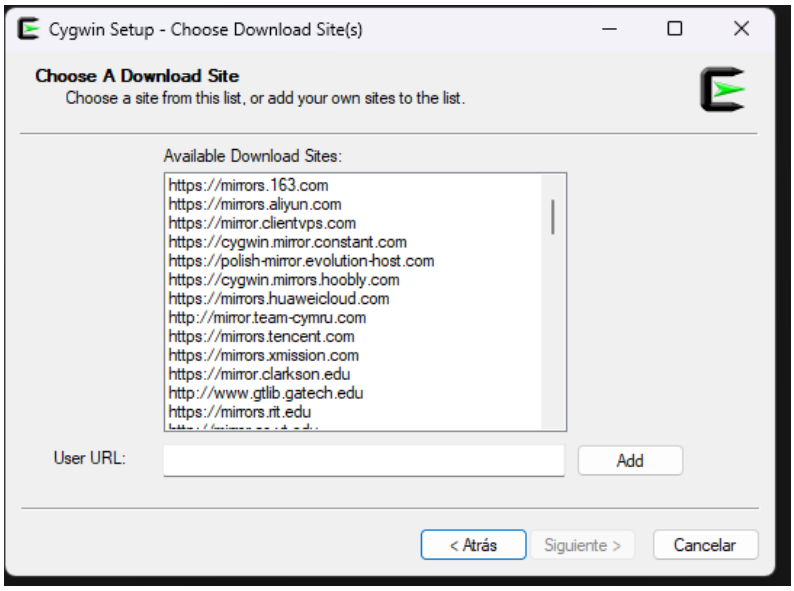
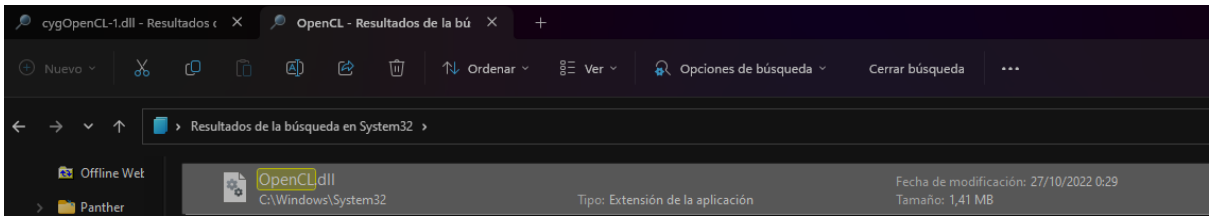
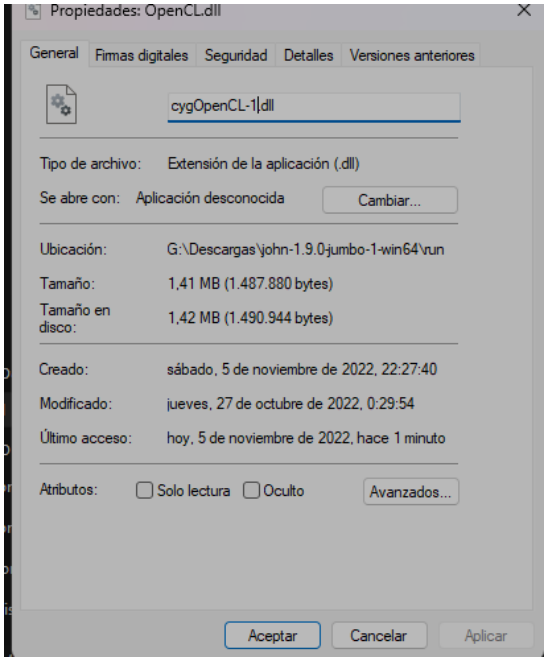
Contraseñas extra

1º: Habilitar gpu en John the ripper

Para habilitar el uso de la gpu he seguido los pasos de esta web: https://suay.site
El proceso consiste en instalar OpenCL, Nvidia CUDA, Cygwin y alli copiar los ficheros del john the ripper, luego copiar un par de ficheros mas y cambiarles de nombre para que john los reconozca.





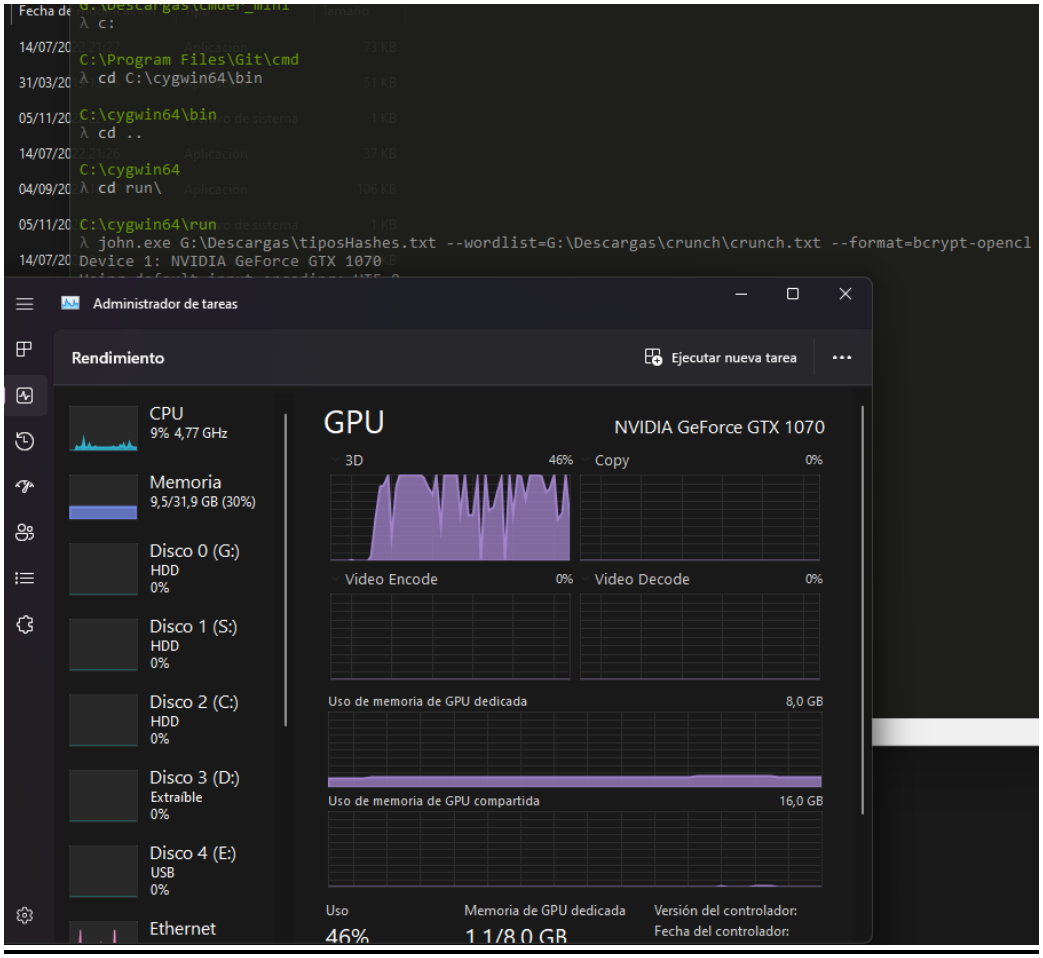


Comprobamos que tenemos la ultima version de los controladores de nvidia.

```
G:\Descargas\john-1.9.0-jumbo-1-win64\run
λ nvidia-smi
Sat Nov  5 22:17:07 2022
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 526.47       Driver Version: 526.47       CUDA Version: 12.0     |
|-------------------------------+----------------------+----------------------+
| GPU  Name            TCC/WDDM | Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  NVIDIA GeForce ... WDDM  | 00000000:08:00.0  On |                  N/A |
|  0%   37C    P8    11W / 200W |    868MiB /  8192MiB |      0%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|    0   N/A  N/A      1828    C+G   ...perience\NVIDIA Share.exe    N/A      |
|    0   N/A  N/A      2392    C+G   ...418.26\msedgewebview2.exe    N/A      |
|    0   N/A  N/A      3132    C+G   ...ekyb3d8bbwe\HxOutlook.exe    N/A      |
|    0   N/A  N/A      4800    C+G   ...ge\Application\msedge.exe    N/A      |
|    0   N/A  N/A      4920    C+G   ...e\PhoneExperienceHost.exe    N/A      |
|    0   N/A  N/A      5520    C+G   ...kyb3d8bbwe\HxAccounts.exe    N/A      |
|    0   N/A  N/A      9928    C+G   ...y\ShellExperienceHost.exe    N/A      |
|    0   N/A  N/A     10136    C+G   C:\Windows\explorer.exe         N/A      |
|    0   N/A  N/A     10252    C+G   ...artMenuExperienceHost.exe    N/A      |
|    0   N/A  N/A     11256    C+G   ...n1h2txyewy\SearchHost.exe    N/A      |
|    0   N/A  N/A     12992    C+G   ...2txyewy\TextInputHost.exe    N/A      |
|    0   N/A  N/A     13944    C+G   ...me\Application\chrome.exe    N/A      |
|    0   N/A  N/A     15328    C+G   ...lPanel\SystemSettings.exe    N/A      |
|    0   N/A  N/A     17756    C+G   ...h2txyewy\FESearchHost.exe    N/A      |
|    0   N/A  N/A     18976    C+G   C:\Windows\explorer.exe         N/A      |
|    0   N/A  N/A     19328    C+G   ...8bbwe\Notepad\Notepad.exe    N/A      |
|    0   N/A  N/A     22396    C+G   ...bbwe\Microsoft.Photos.exe    N/A      |
+-----------------------------------------------------------------------------+

G:\Descargas\john-1.9.0-jumbo-1-win64\run
```

Y por ultimo comprobamos que ya reconoce la tarjeta grafica.

```
C:\cygwin64\run
λ john --test --format=wpapsk-opencl
Device 1: NVIDIA GeForce GTX 1070
Benchmarking: wpapsk-opencl, WPA/WPA2/PMF/PMKID PSK [PBKDF2-SHA1 OpenCL]... 6 errors generated.
Options used: -I kernels -cl-mad-enable -DSM_MAJOR=6 -DSM_MINOR=1 -D__GPU__ -DDEVICE_INFO=524306 -D__SIZEOF_HOST_SIZE_T__=8 -DDEV_VER_MAJO
```



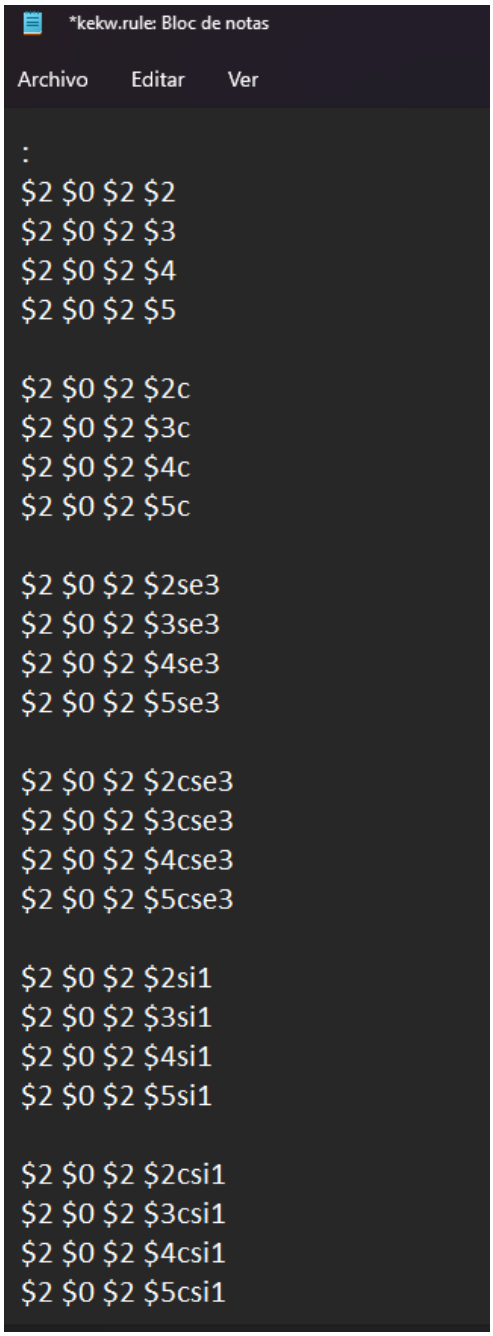
2º: Lo mismo del ejercicio de contraseñas pero con hashcat.

Shadow.txt

```
λ hashcat shadow.txt  -a 0 rockyou.txt -o claves.txt
hashcat (v6.2.6) starting in autodetect mode

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
CUDA API (CUDA 12.0)
====================
* Device #1: NVIDIA GeForce GTX 1070, 7231/8191 MB, 15MCU

OpenCL API (OpenCL 3.0 CUDA 12.0.70) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce GTX 1070, skipped

OpenCL API (OpenCL 2.1 WINDOWS) - Platform #2 [Intel(R) Corporation]
====================================================================
* Device #3: AMD Ryzen 7 5800X 8-Core Processor, skipped
```

```
G:\Descargas\hashcat-6.2.6
λ cat claves.txt
$6$xonBhxE19HmG8.DR$LdediY0FTHMUPyeQAiEFVgUR6rKVrOGcCECCn.EQupIwH2EyZqib3gc5kJfuwp/ppLJY41Ap5KEUf7RCk3T4O0:dragon
$6$yMJT8Nf23i7Z1WkF$ChxmECeWSs3W8Or1Ogf4eapPz5FNcBM4SBvZG.21fI0wpNUmR1yCmK71r7sYFMXCL3deD5BWDD/6A4WU66cjv0:whatever
$6$ooyV5Z5dEaDfyPom$VnKneoTa7s7DJRFFarye2sjZiwWbrr1jQ28lzw36OGaAChy1K14GY6BEFTABLGjZ8Xs4iSmbaZdfDXYFi9ED71:princesa
$6$a5m5M9J/FEJGzyrd$shv36BNOS58W8VQBbjLKESl/3QjJxomkBb84j9Mw2g04JW3TIVGstOmJQFT5wdpl1soe9XjI3YjDNNH6uXv7s1:administrator
```

Ahora vamos a hacer lo mismo con las claves de windows. Lo primero sera adaptar las reglas que hicimos en john, creadno un nuevo fichero .rule, para qeu hashcat pueda leerlo.



Ahora vamos a probar a sacar las contraseñas

```
G:\Descargas\hashcat-6.2.6
λ hashcat windows.txt -m 1000 -D 1 -a 0 diccionario.txt -o clavesW.txt -r rules\kekw.rule
hashcat (v6.2.6) starting

CUDA API (CUDA 12.0)
====================
* Device #1: NVIDIA GeForce GTX 1070, skipped

OpenCL API (OpenCL 3.0 CUDA 12.0.70) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce GTX 1070, skipped

OpenCL API (OpenCL 2.1 WINDOWS) - Platform #2 [Intel(R) Corporation]
====================================================================
* Device #3: AMD Ryzen 7 5800X 8-Core Processor, 16313/32691 MB (4086 MB allocatable), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 9 digests; 9 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 129
```

```
G:\Descargas\hashcat-6.2.6
λ hashcat windows.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1000 | NTLM | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

b32db29f51c06e0b7ae42f8355dab807:oscar
9ab721ecba25a83055ea8ba89c7c717b:D@ni3l0cf2022
a2212d8b2bb5a18c1f0f9343956b3f23:APCWalls2022
edba5cbc1ed46b673a7f0a86fdbfca2f:L0r3nz0NPBB2023
cf74007f626c01b74c94f0e95423ab50:J@v1erGuerr@2025
93609de8c3eeaa8113d33131230a192f:cesargil2022
6a5d34a235d3553fb8aa3b1c036ff684:carlos2023
186cb09181e2c2ecaac768c47c729904:a
cadceffacb32144a358cbd798d8c132f:Patr1c1aCaP2022
```

El hash de tipo SHA1 sale, al igual que en john the ripper

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: 5688393f91356d29723cbf17958b5a5d08228222
Time.Started.....: Sun Nov 06 15:37:58 2022 (2 secs)
Time.Estimated...: Sun Nov 06 15:38:00 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (..\crunch\crunch.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#3.........: 16268.0 kH/s (0.26ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 33521664/58000800 (57.80%)
Rejected.........: 0/33521664 (0.00%)
Restore.Point....: 33505280/58000800 (57.77%)
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#3....: donpaN11]FIN -> donpaS07 FIN
Hardware.Mon.#3..: N/A
```

El MD5 también sale

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 8a72877c4baf89da0a37fc09375b271d
Time.Started.....: Sun Nov 06 15:40:09 2022 (2 secs)
Time.Estimated...: Sun Nov 06 15:40:11 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (..\crunch\crunch.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#3.........: 17537.6 kH/s (0.20ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 33521664/58000800 (57.80%)
Rejected.........: 0/33521664 (0.00%)
Restore.Point....: 33505280/58000800 (57.77%)
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#3....: donpaN11]FIN -> donpaS07 FIN
Hardware.Mon.#3..: N/A
```

Al igual que en john the ripper, me ha sido imposible sacar los hashes de tipe bcrypt

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: tiposHashes.txt
Time.Started.....: Sun Nov 06 15:32:44 2022 (1 min, 21 secs)
Time.Estimated...: Thu Nov 10 11:23:39 2022 (3 days, 19 hours)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (..\crunch\crunch.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#3.........:      351 H/s (11.34ms) @ Accel:16 Loops:16 Thr:1 Vec:1
Recovered........: 0/2 (0.00%) Digests (total), 0/2 (0.00%) Digests (new), 0/2 (0.00%) Salts
Progress.........: 27904/116001600 (0.02%)
Rejected.........: 0/27904 (0.00%)
Restore.Point....: 13824/58000800 (0.02%)
Restore.Sub.#3...: Salt:1 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#3....: donaaE18?FIN -> donaaE26\FIN
Hardware.Mon.#3..: N/A

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```