Obrigado!

A evolução de GPGPU: O problema de se armazenar hashes de senhas

Autores:
Marco Constantino

Luiz Otávio Duarte

Autores:

Marco Constantino

Luiz Otávio Duarte

Autores:
Marco Co

Luiz Otáv

General-Purpose Computation on Graphics Hardware


PowerColor
DIAMOND
Radeon
HD 6990


536MB GDDR5
GeForce
GTX580
DS
SC SSC FTW
EVGA


intel
Core™ i5
intel
Core™ i7

O que é?

Como funciona?

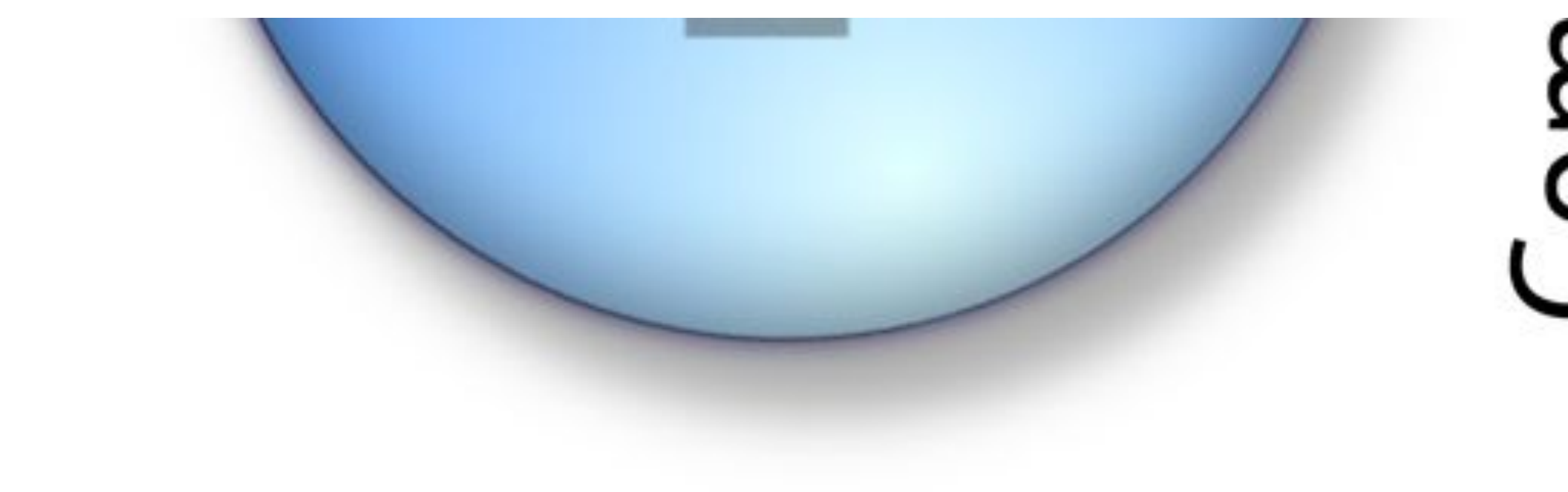
O que é?

Propósito geral


Propósito geral

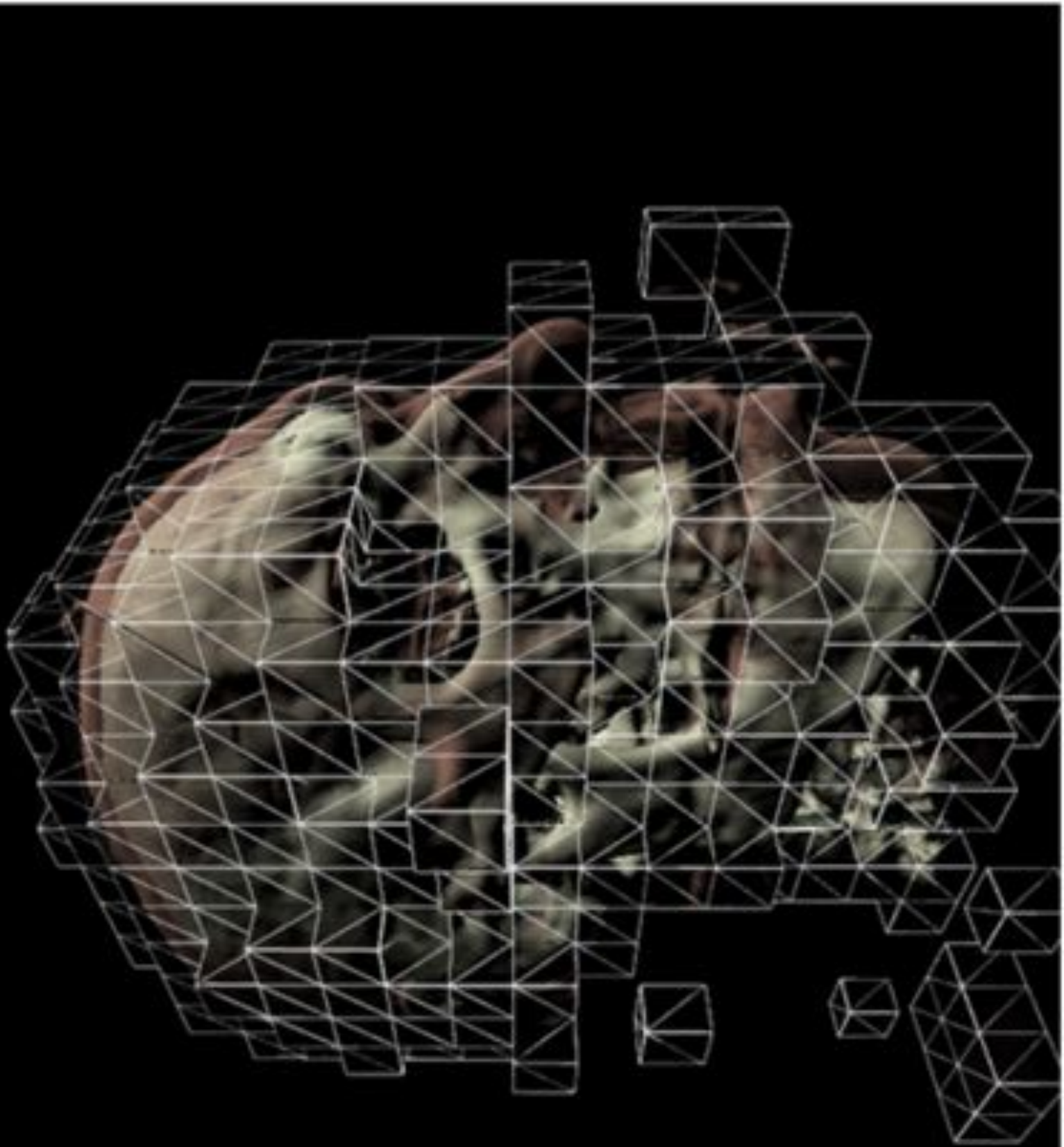
O que é?

Como funciona?

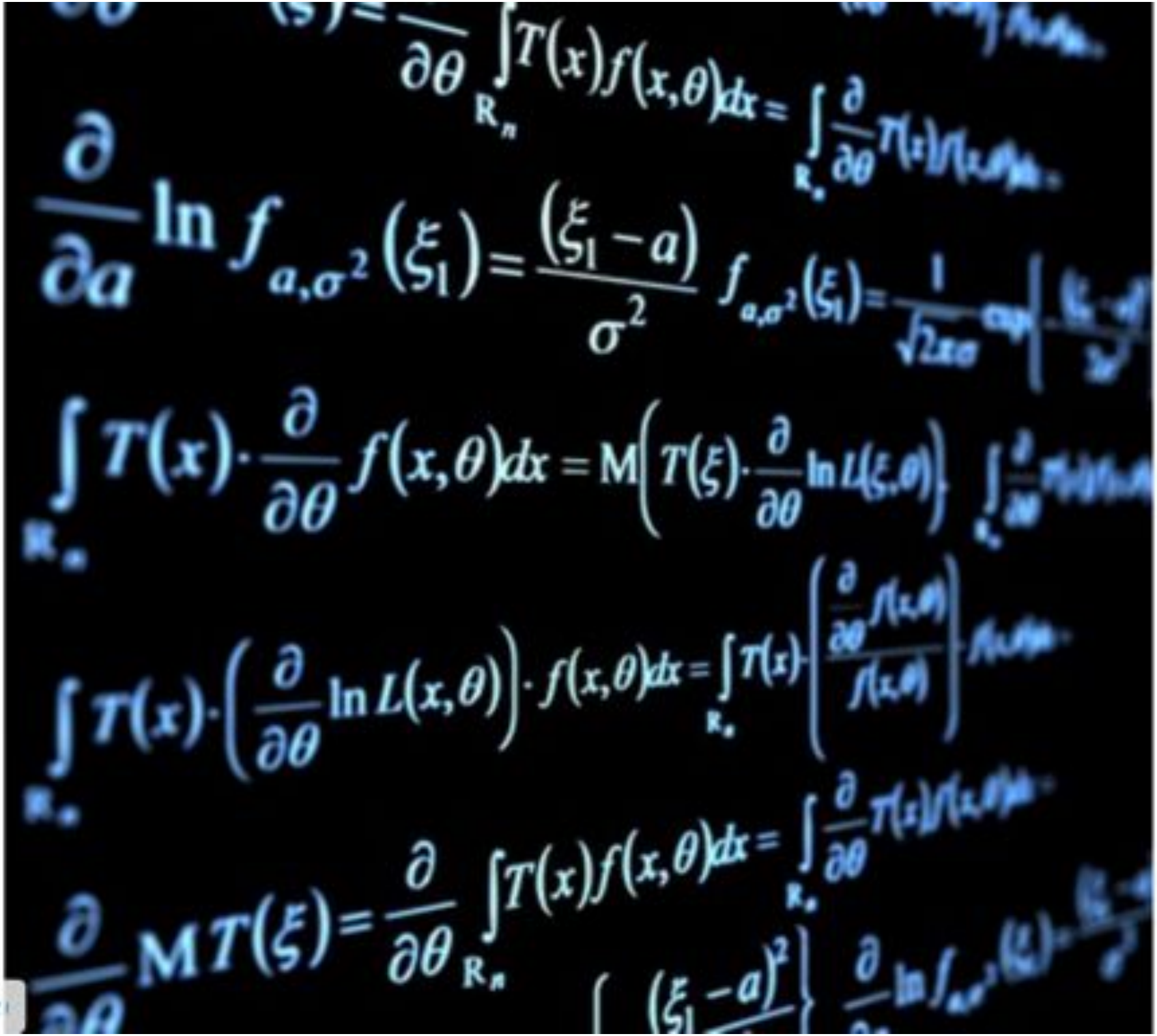


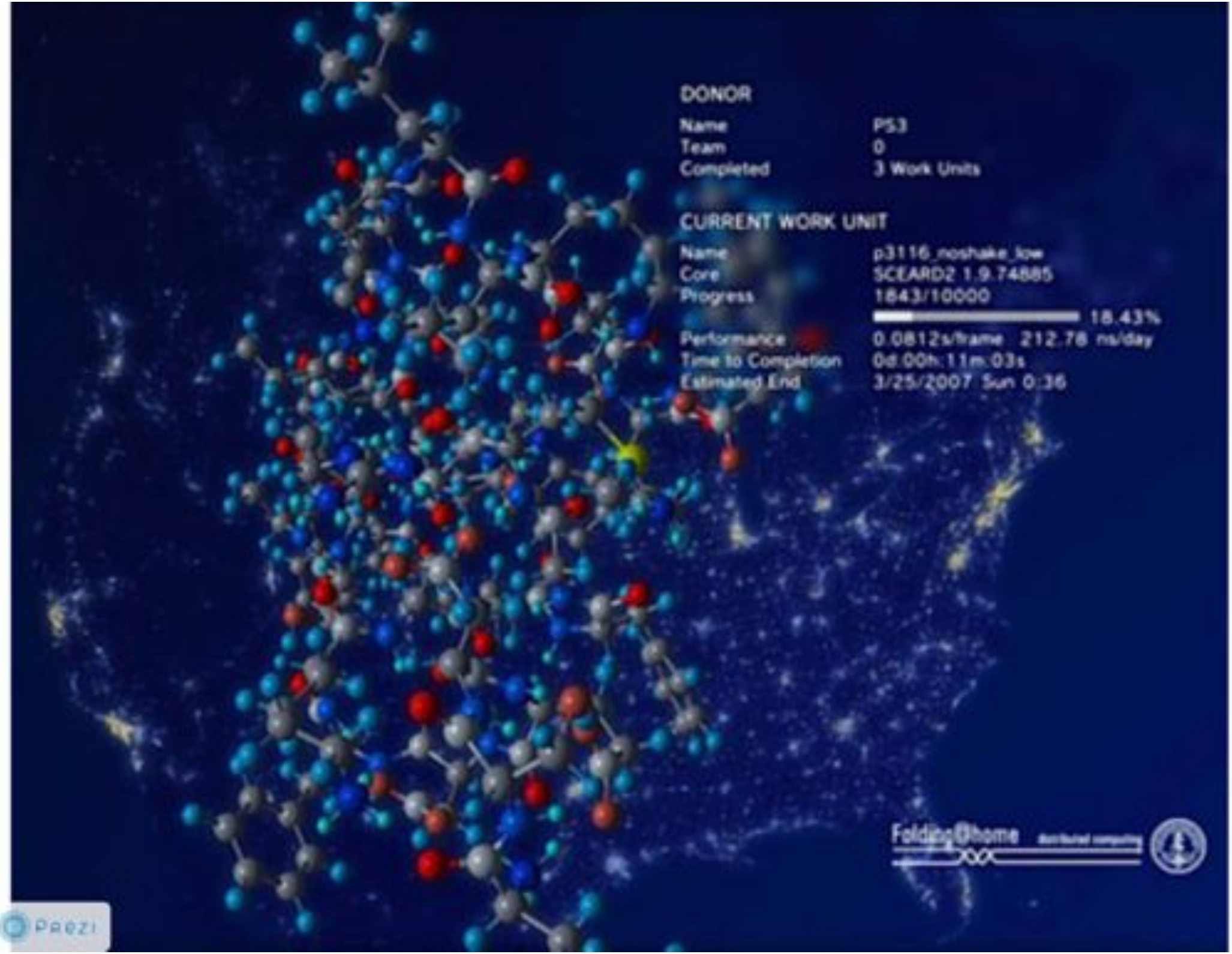
Pra que serve?

Utilidades



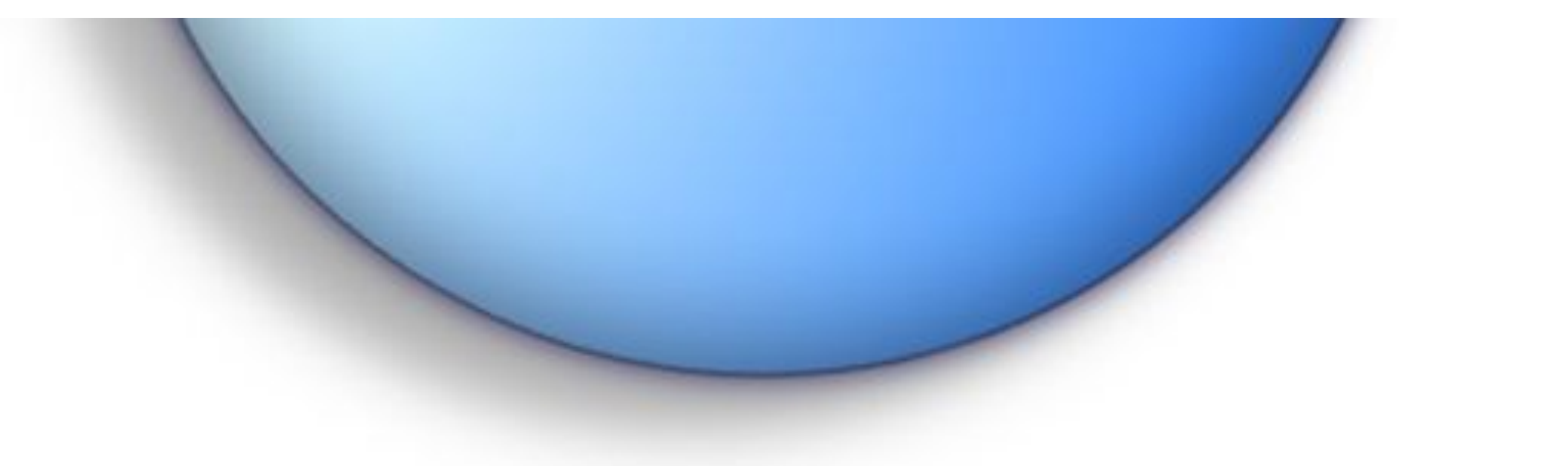
Utilidades


$\frac{\partial}{\partial a}\ln f_{a,\sigma^2}(\xi_1) = \frac{(\xi_1 - a)}{\sigma^2} f_{a,\sigma^2}(\xi_1)$
$\int_{R_n} T(x)\cdot\frac{\partial}{\partial\theta} f(x,\theta)dx = M\left(T(\xi)\cdot\frac{\partial}{\partial\theta}\ln L(\xi,\theta)\right)$
$\int_{R_n} T(x)\cdot\left(\frac{\partial}{\partial\theta}\ln L(x,\theta)\right)\cdot f(x,\theta)dx = \int_{R_n} T(x)\cdot\left(\frac{\frac{\partial}{\partial\theta} f(x,\theta)}{f(x,\theta)}\right)$
$\frac{\partial}{\partial\theta} M T(\xi) = \frac{\partial}{\partial\theta}\int_{R_n} T(x) f(x,\theta)dx = \int_{R_n}\frac{\partial}{\partial\theta} T(x) f(x,\theta)dx$


DONOR
Name PS3
Team 0
Completed 3 Work Units
CURRENT WORK UNIT
Name p3116_noshake_low
Core SCEARD2 1.9.74885
Progress 1843/10000
18.43%
Performance 0.0812s/frame 212.78 ns/day
Time to Completion 0d:00h:11m:03s
Estimated End 3/25/2007 Sun 0:36
Folding@home

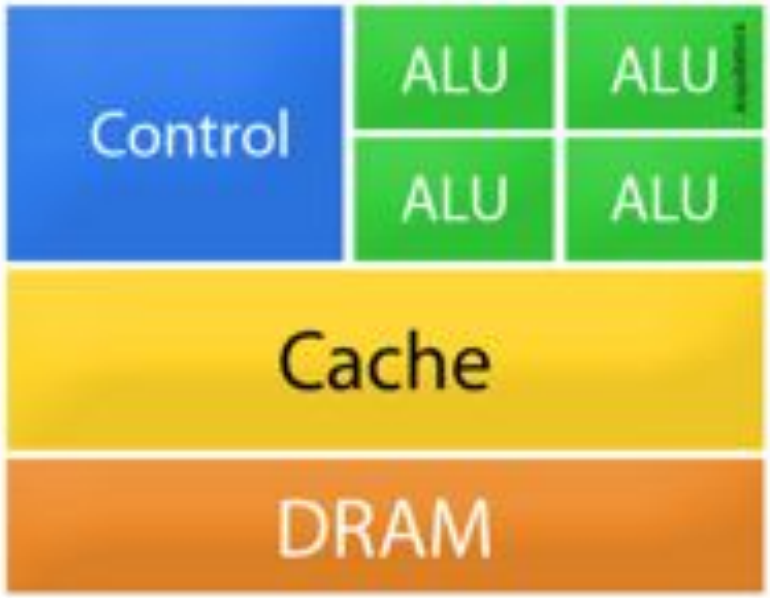
O que é?

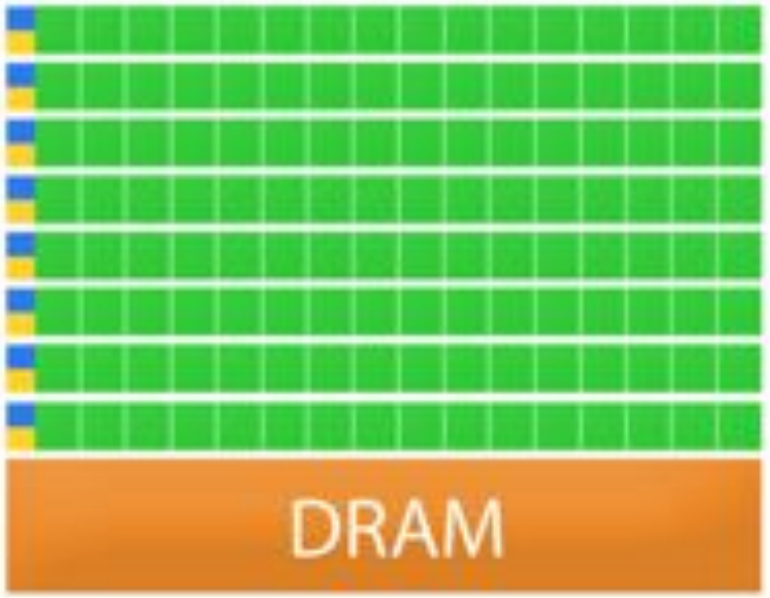
Como funciona?

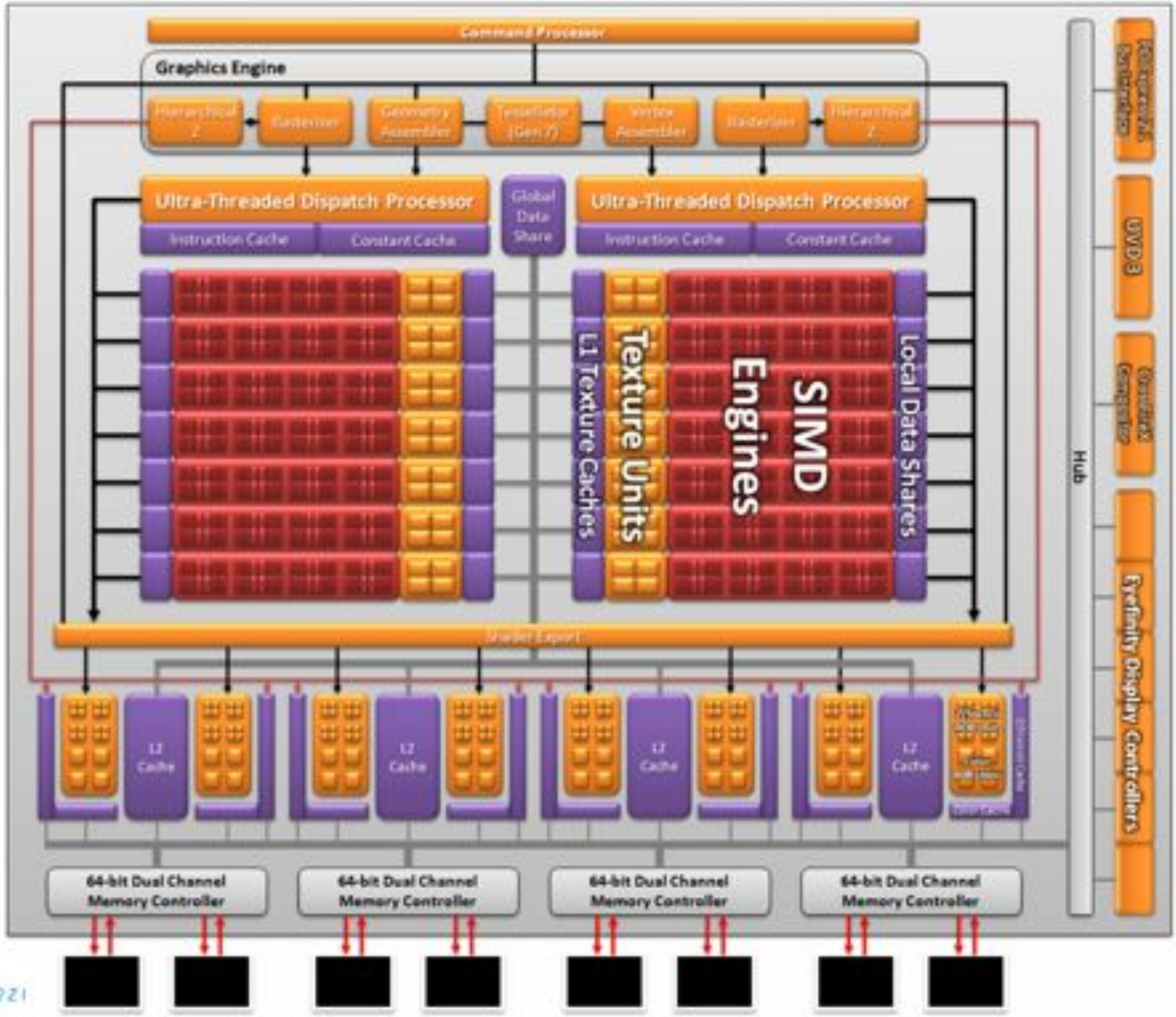


Como funciona?

Arquitetura






Command Processor
Graphics Engine
Rasterizer
Rasterizer
Ultra-Threaded Dispatch Processor
Instruction Cache
Constant Cache
Global Data Share
Ultra-Threaded Dispatch Processor
Instruction Cache
Constant Cache
L1 Texture Caches
Texture Units
SIMD Engines
Local Data Shares
Hub
UVD 3
Eyefinity Display Controllers
L2 Cache
L2 Cache
L2 Cache
L2 Cache
64-bit Dual Channel Memory Controller
64-bit Dual Channel Memory Controller
64-bit Dual Channel Memory Controller
64-bit Dual Channel Memory Controller

CPU x GPU

CPU x GPU

Plain Old CPU Processing

GPGPU Processing


password

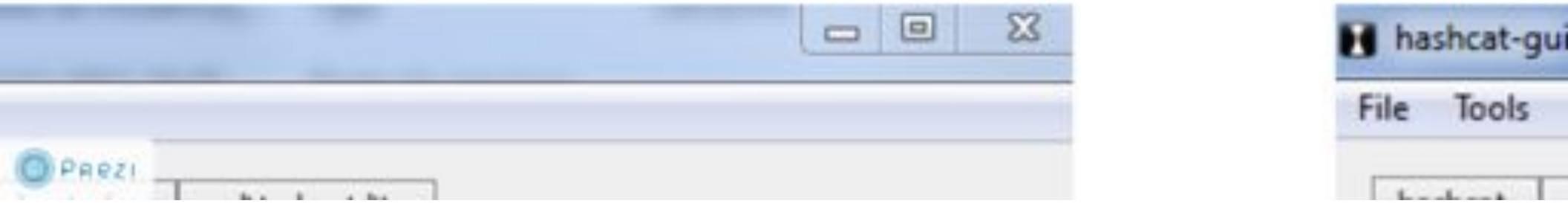
Utilizando GPGPU para quebrar Hash de senhas

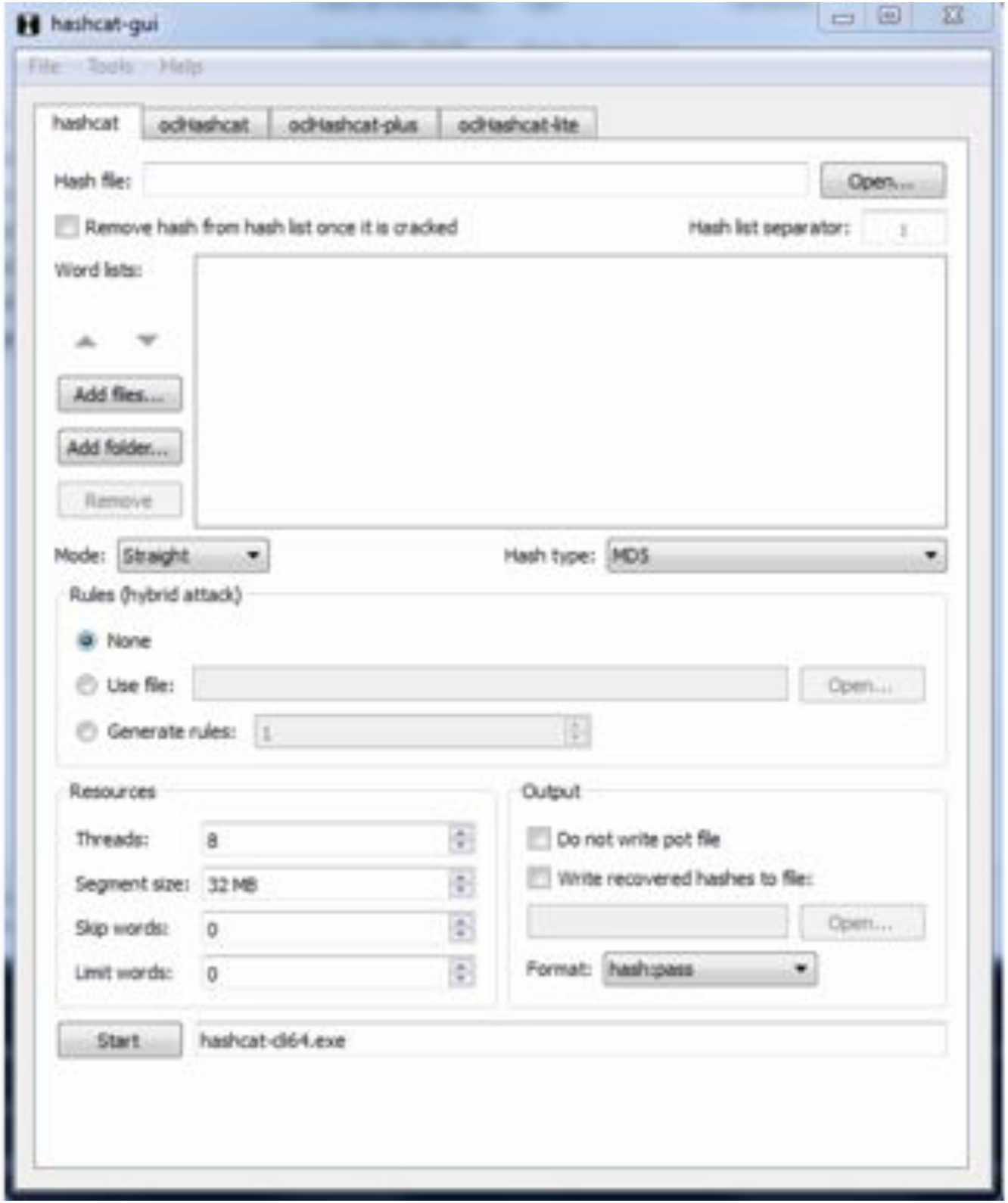
Ferramenta

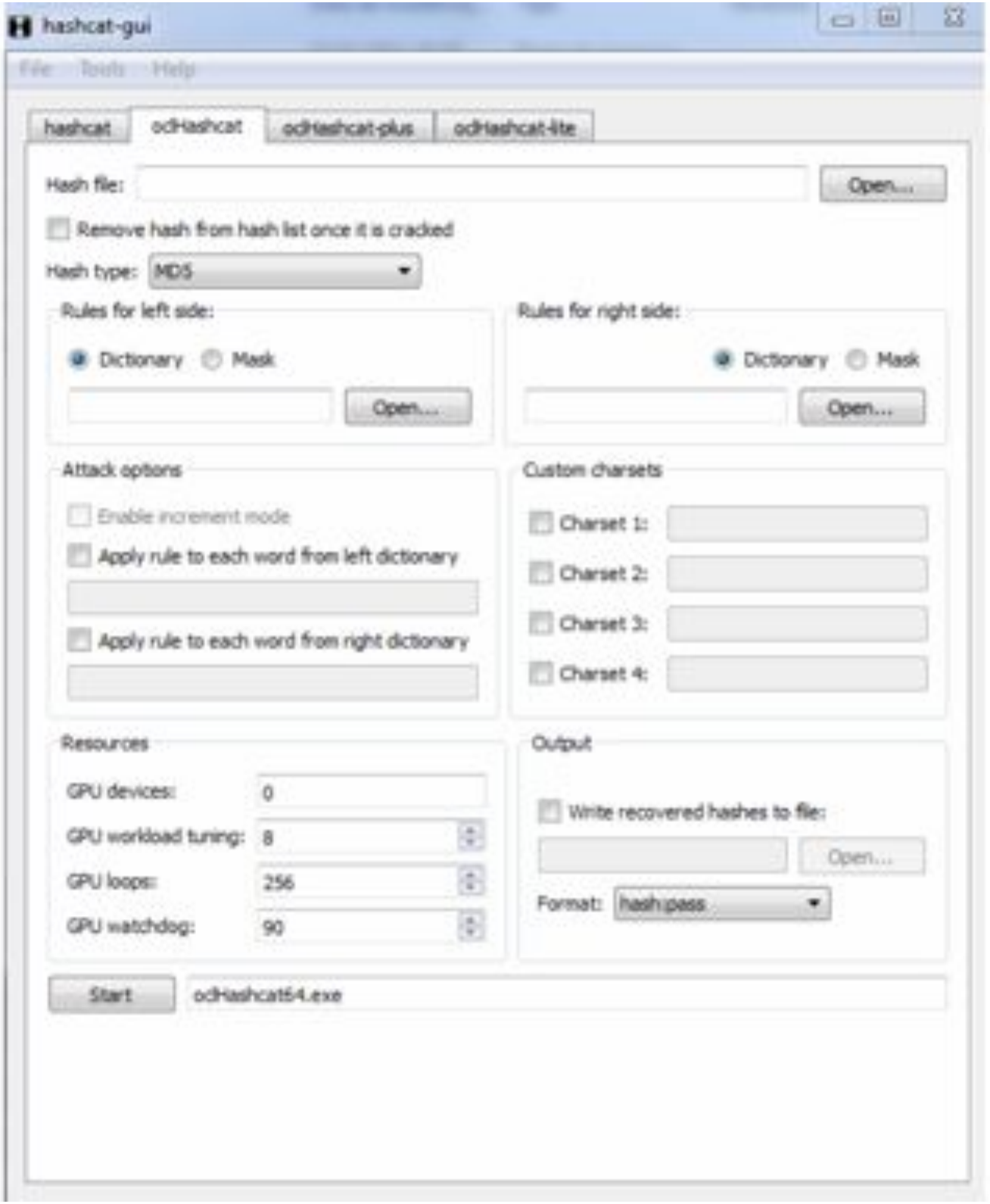
hashcat

advanced password recovery

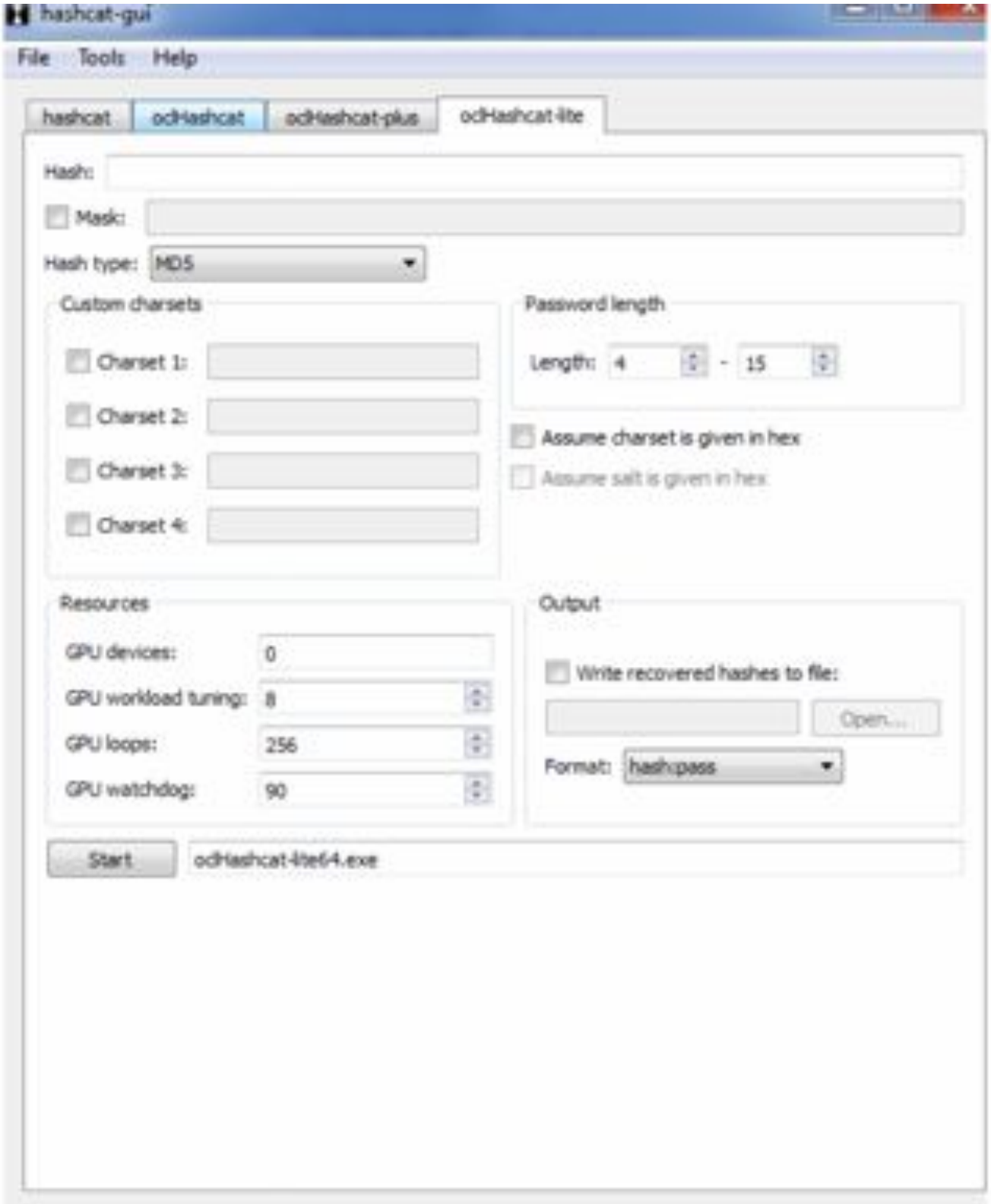
Interface hashcat-gui




hashcat-gui
File Tools Help
hashcat
oclHashcat
oclHashcat-plus
oclHashcat-lite
Hash file:
Open...
Remove hash from hash list once it is cracked
Hash list separator:
Word lists:
Add files...
Add folder...
Remove
Mode:
Straight
Hash type:
MD5
Rules (hybrid attack)
None
Use file:
Open...
Generate rules:
Resources
Threads:
8
Segment size:
32 MB
Skip words:
0
Limit words:
0
Output
Do not write pot file
Write recovered hashes to file:
Open...
Format:
hash:pass
Start
hashcat-cli64.exe


hashcat-gui
File Tools Help
hashcat oclHashcat oclHashcat-plus oclHashcat-lite
Hash file:
Open...
Remove hash from hash list once it is cracked
Hash type: MD5
Rules for left side:
Dictionary Mask
Open...
Rules for right side:
Dictionary Mask
Open...
Attack options
Enable increment mode
Apply rule to each word from left dictionary
Apply rule to each word from right dictionary
Custom charsets
Charset 1:
Charset 2:
Charset 3:
Charset 4:
Resources
GPU devices: 0
GPU workload tuning: 8
GPU loops: 256
GPU watchdog: 90
Output
Write recovered hashes to file:
Open...
Format: hash:pass
Start
oclHashcat64.exe


hashcat-gui
File
Tools
Help
hashcat
oclHashcat
oclHashcat-plus
oclHashcat-lite
Hash file or hash:
Open...
Remove hash from hash list once it is cracked
Ignore username in hashfile
Word lists:
Add files...
Add folder...
Remove
Mode:
Straight
Hash type:
MD5
Rules
Use rules:
Open...
Generate rules:
1
Resources
GPU devices:
0
GPU workload tuning:
8
GPU loops:
256
GPU watchdog:
90
Segment size:
32 MB
Output
Write recovered hashes to file:
Open...
Format:
hash:pass
Start
oclHashcat-plus64.exe

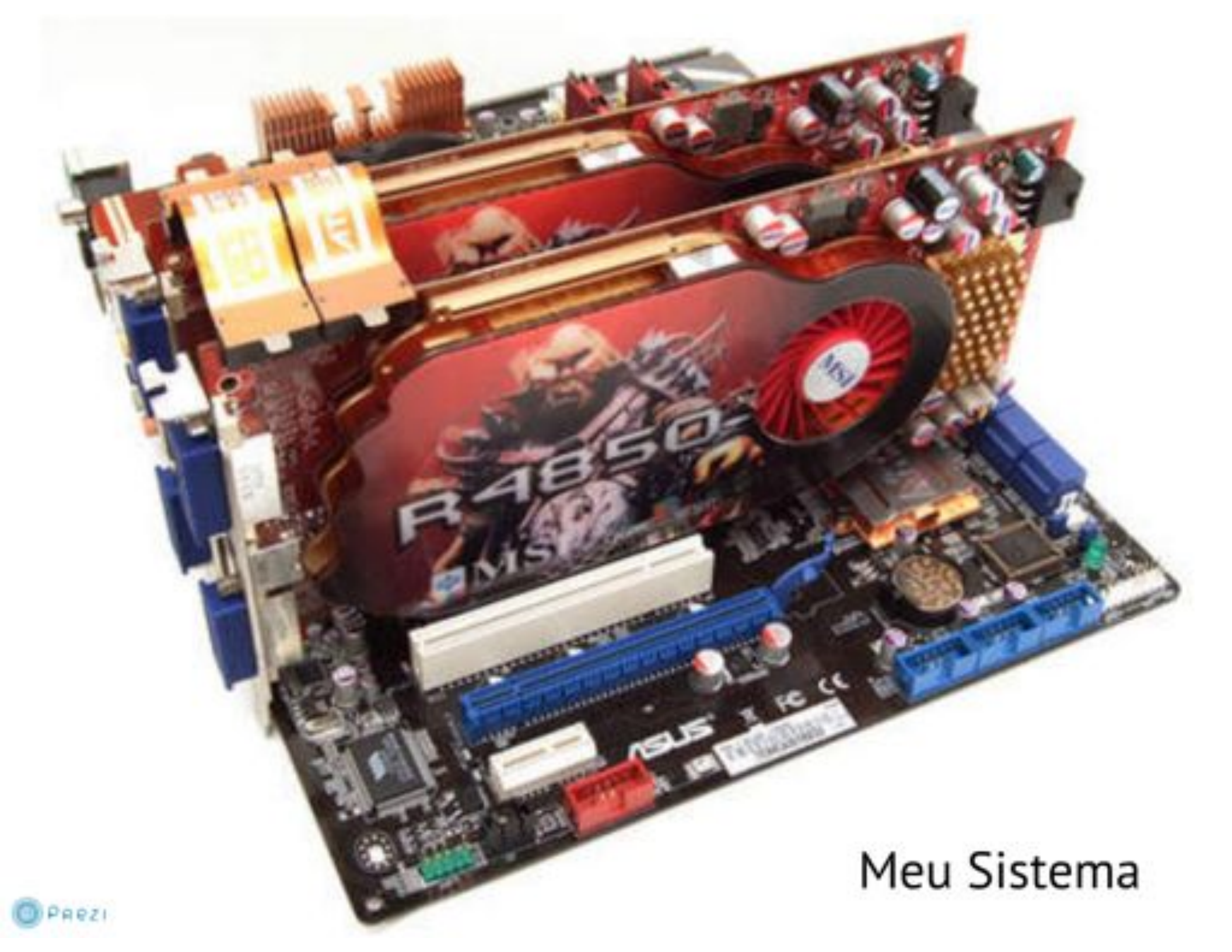

hashcat-gui
File
Tools
Help
hashcat
oclHashcat
oclHashcat-plus
oclHashcat-lite
Hash:
Mask:
Hash type:
MD5
Custom charsets
Charset 1:
Charset 2:
Charset 3:
Charset 4:
Password length
Length:
4
15
Assume charset is given in hex
Assume salt is given in hex
Resources
GPU devices:
0
GPU workload tuning:
8
GPU loops:
256
GPU watchdog:
90
Output
Write recovered hashes to file:
Open...
Format:
hash:pass
Start
oclHashcat-lite64.exe

Attack Modes

es

- Brute-Force attack
- Combinator attack
- Dictionary attack
- Fingerprint attack
- Hybrid attack
- Mask attack
- Permutation attack
- Rule-based attack
- Table-Lookup attack
- Toggle-Case attack

Meu Sistema



Meu Sistema

MD5= 2500M/s

SHA1=800M/s

SHA256=523M/S

Outros Sistemas

5970 • stock core clock

Vidia gtx570 • 1600Mhz core clock

DK v2.4 • 8x ATI hd6970 • stock core clock

x580 • 1594Mhz core clock

Performance

- PC1: Windows7, 64 bit · Catalyst 11.11 · 1x ATI hd5970 · stock core clock
- PC2: Windows7, 64 bit · ForceWare 285.62 · 1x NVidia gtx570 · 1600Mhz core clock
- PC3: Ubuntu 10.10, 64 bit · Catalyst 11.6 + Stream SDK v2.4 · 8x ATI hd6970 · stock core clock
- PC4: Ubuntu 10.10, 64 bit · ForceWare 280.13 · 7x NVidia gtx580 · 1594Mhz core clock

Hash Type	PC1	PC2	PC3	PC4
MD5	9786M c/s	2161M c/s	451523M c/s	162668M c/s
md5($pass.$salt)	2300M c/s	2161M c/s	451523M c/s	162708M c/s
md5(md5($pass))	2299M c/s	611M c/s	114168M c/s	47858M c/s
vBulletin < v3.8.5	1625M c/s	611M c/s	114168M c/s	47868M c/s
vBulletin > v3.8.5	1648M c/s	425M c/s	81448M c/s	32798M c/s
SHA1	3426M c/s	799M c/s	157128M c/s	60538M c/s
sha1($pass.$salt)	3426M c/s	799M c/s	157208M c/s	60628M c/s
MySQL > v4.1	1410M c/s	348M c/s	64248M c/s	26388M c/s
nsldap, SHA-1(Base64), Netscape LDAP SHA	3426M c/s	799M c/s	157128M c/s	60538M c/s
nsldaps, SSHA-1(Base64), Netscape LDAP SSHA	3426M c/s	799M c/s	157128M c/s	60628M c/s
MD4	177658M c/s	39178M c/s	867208M c/s	291848M c/s
NTLM	165428M c/s	37428M c/s	821848M c/s	285328M c/s
Domain Cached Credentials	5264M c/s	1221M c/s	249368M c/s	91928M c/s
MSSQL(2000)	3382M c/s	787M c/s	157128M c/s	60038M c/s
SHA256	1306M c/s	272M c/s	62458M c/s	20398M c/s
descrypt, DES(Unix), Traditional DES	697568k c/s	256138k c/s	382860k c/s	1912328k c/s
SL3	3397M c/s	789M c/s	157368M c/s	60038M c/s
Oracle 11g	3426M c/s	798M c/s	157208M c/s	60618M c/s
MSSQL(2005)	3388M c/s	789M c/s	156968M c/s	60038M c/s
Cisco-PIX MD5	5836M c/s	1473M c/s	273208M c/s	110968M c/s

Políticas de Senhas


DESKTOP
PASSWORD:
r4ewo1ss89

Rockyou.com Statistics

[*] Line Count Statistics...

[+] 8: 20% (2966004)

[+] 7: 17% (2506264)

[+] 9: 15% (2191000)

[+] 10: 14% (2013690)

[+] 6: 13% (1947858)

[+] 11: 06% (865973)

[+] 12: 03% (555333)

[+] 13: 02% (364169)

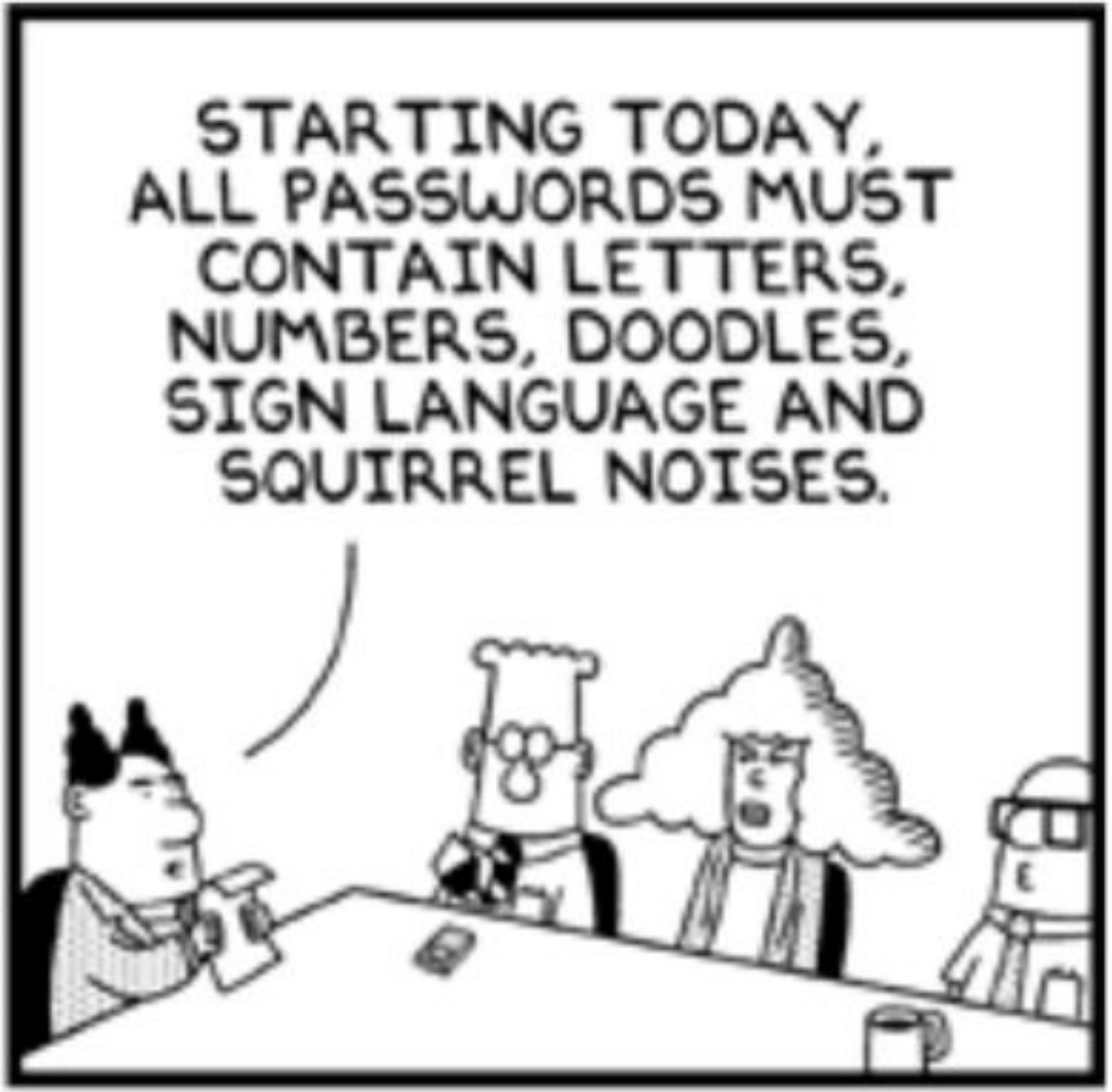
[+] 5: 01% (259174)

[+] 14: 01% (248514)

[+] 15: 01% (161181)

Rockyou Stats Cont.

[+] loweralphanum: 42% (6075055)
[+] loweralpha: 25% (3726656)
[+] numeric: 16% (2346842)
[+] loweralphaspecialnum: 03% (472673)
[+] upperalphanum: 02% (407436)
[+] mixedalphanum: 02% (382246)
[+] loweralphaspecial: 02% (381095)
[+] upperalpha: 01% (229893)
[+] mixedalpha: 01% (159332)
[+] mixedalphaspecialnum: 00% (53240)
[+] mixedalphaspecial: 00% (49633)
[+] upperalphaspecialnum: 00% (27732)
[+] upperalphaspecial: 00% (26795)
[+] special: 00% (5763)


STARTING TODAY, ALL PASSWORDS MUST CONTAIN LETTERS, NUMBERS, DOODLES, SIGN LANGUAGE AND SQUIRREL NOISES.
9-10-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.

Agradecimentos

Atom - Codder Hashcat

pure_hate - team Hashcat

T0X|C - team Hashcat

hashcat @ rizon.net

Obrigado!