VERSION 1.0

MARCH 30, 2013

CUDA CRACKING

PRESENTED BY: ROHIT SHAW

XIARCH SOLUTIONS PVT LTD
NEW DELHI

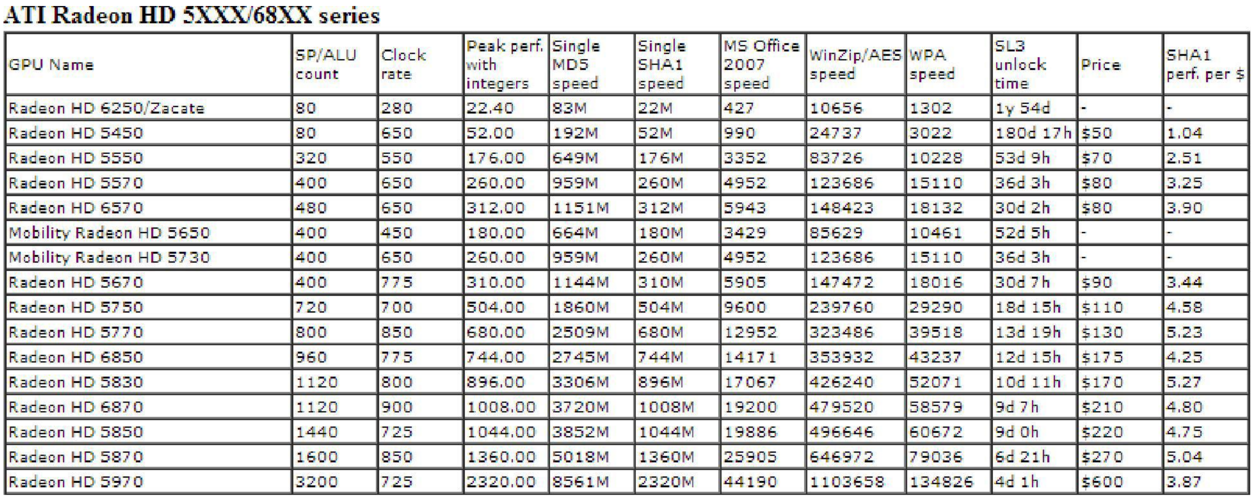
CUDA Cracking

Compute Unified Device Architecture (CUDA) is a parallel computing architecture developed by Nvidia for graphics processing. CUDA is the computing engine in Nvidia graphics processing units (GPUs) that is accessible to software developers through variants of industry standard programming languages.

Introduction: Cuda cracking means cracking passwords with the help of Graphics card which have GPU, it means the speed of password cracking is much faster than CPU speed.

Building a CUDA Machine: For building a monster cuda machine we have to invest a huge amount on it. First we have to select a motherboard which supports more than one GPU because the more GPU means the process of password cracking is much faster. I suggest MSI Big Bang Marshall Motherboard which supports multiple GPUs up to 8 graphic cards. Another unique feature of this motherboard that it is cross platform GPU supportable it means it can support both ATI and Nvidia graphic cards at a time. Use Quad core processors or Intel's I family processors for better performance. RAM up to 16 GB is efficient for this motherboard. Another important thing to keep in mind that is the power supply system we have to supply up to 1250 watt power to this machine. Also use cooling fans as much as possible because during process graphic cards heats very intensively.

Graphic Card Selection: Graphic card selection is the core important thing before assembling a cuda machine. Before investing in graphic card first decides which graphic cards has much cuda cores. Graphics card runs on cuda core it means the number of core is high then the password cracking performance is also high. Also keep in mind which motherboard is you are using because all graphic cards did not compatible with all motherboards. We can see the list of GPU estimations and map the performance of card according to your budget.



ATI Radeon HD 5XXX/68XX series

GPU Name	SP/ALU count	Clock rate	Peak perf. with integers	Single MD5 speed	Single SHA1 speed	MS Office 2007 speed	WinZip/AES speed	WPA speed	SL3 unlock time	Price	SHA1 perf. per $
Radeon HD 6250/Zacate	80	280	22.40	83M	22M	427	10656	1302	1y 54d	-	-
Radeon HD 5450	80	650	52.00	192M	52M	990	24737	3022	180d 17h	$50	1.04
Radeon HD 5550	320	550	176.00	649M	176M	3352	83726	10228	53d 9h	$70	2.51
Radeon HD 5570	400	650	260.00	959M	260M	4952	123686	15110	36d 3h	$80	3.25
Radeon HD 6570	480	650	312.00	1151M	312M	5943	148423	18132	30d 2h	$80	3.90
Mobility Radeon HD 5650	400	450	180.00	664M	180M	3429	85629	10461	52d 5h	-	-
Mobility Radeon HD 5730	400	650	260.00	959M	260M	4952	123686	15110	36d 3h	-	-
Radeon HD 5670	400	775	310.00	1144M	310M	5905	147472	18016	30d 7h	$90	3.44
Radeon HD 5750	720	700	504.00	1860M	504M	9600	239760	29290	18d 15h	$110	4.58
Radeon HD 5770	800	850	680.00	2509M	680M	12952	323486	39518	13d 19h	$130	5.23
Radeon HD 6850	960	775	744.00	2745M	744M	14171	353932	43237	12d 15h	$175	4.25
Radeon HD 5830	1120	800	896.00	3306M	896M	17067	426240	52071	10d 11h	$170	5.27
Radeon HD 6870	1120	900	1008.00	3720M	1008M	19200	479520	58579	9d 7h	$210	4.80
Radeon HD 5850	1440	725	1044.00	3852M	1044M	19886	496646	60672	9d 0h	$220	4.75
Radeon HD 5870	1600	850	1360.00	5018M	1360M	25905	646972	79036	6d 21h	$270	5.04
Radeon HD 5970	3200	725	2320.00	8561M	2320M	44190	1103658	134826	4d 1h	$600	3.87

We can see the list above here you see that SP/ALU count column it refers the no. of cuda cores and also see the cracking speed of hashes like MD5, SHA1, WPA and more.
Here we are using Radeon HD 5970 and it has 3200 cuda cores that why the cracking speed is much pretty good.

Now after card selection you have to select a proper GPU supported tool from which you will able to crack hash. There are many tools which supports GPU processor. Tools are based on operating systems some tools are Windows Supported and some of them are Linux supported. We are going to now describe some tools according to operating system compatibility.

WindowsSupportedTools:

IGHASHGPU: This tool is developed by Ivan Golubev. This tool can crack only three hashes SHA1, MD5 and MD4. It is compatible with ATI and Nvidia cards. The ATI cards which supports are Radeon HD 4550, 4670, 4830, 4730, 4770, 4850, 4870, 4890, 5750, 5770, 5850, 5870, 5970 and Nvidia cards with CUDA support.

BarsWF: BarsWF is developed by Svarichevsky Mikhail. It supports on Nvidia cards and also known as world’s fastest MD5 cracker. Hash supports only MD5.

Extreme GPU Bruteforcer: It is a commercial tool developed by InsidePro. It supports total 58 types of hashes MD5, MD4, NTLM, SHA-1, SHA-512 and many more. Utilizing the power of multiple graphics cards running simultaneously (supports up to 32 GPU), the software allows reaching incredible search speeds of billions of passwords per second. It supports only Nvidia cards.

Lightning Hash Cracker: Lightning Hash Cracker is developed by Elcomsoft and it is a freeware tool. It supports only MD5 hashes and Nvidia compatible.

Oclhashcat Plus: It is a popular hash cracker tool and it supports ATI and Nvidia cards simultaneously. It works on Windows and Linux based operating systems. Multi GPU supports up to 128 cards. It supports 57 types of hashes.

Cryptohaze Multiforcer: It is an open source tool. This is only a tool which can used on network based password cracking so multiple systems can work on the same. It supports 17 types of hashes MD5, MD4, NTLM, LM and more. It supports only Nvidia cards are 8000 series, 9000 series, GTX200 series, GTX400/500 series.

LinuxSupportedTools:

New Multiforcer: New Multiforcer is the new version for Cryptohaze Multiforcer and an open source tool which supports ATI and Nvidia cards. The older version means Cryptohaze Multiforcer does not supports ATI cards. New Multiforcer supports only 9 types of hashes.

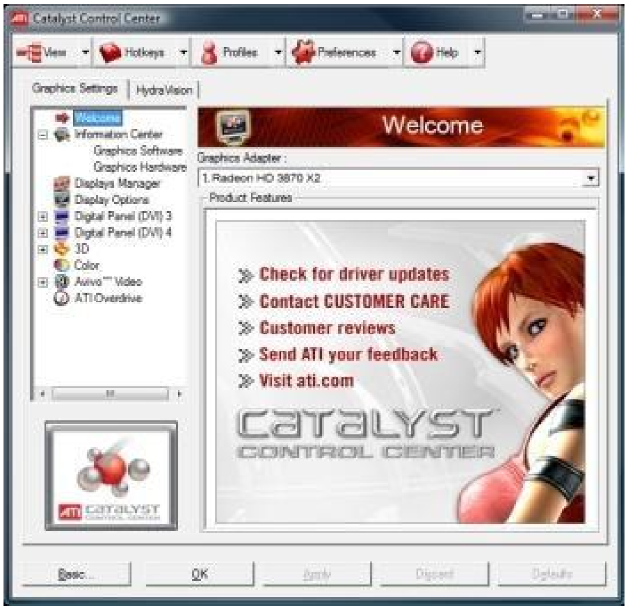
Oclhashcat Plus: It is a muti platform working tools runs on Windows and Linux based operating systems. It also supports a large number of hashes and GPU enabled cards up to 128 GPU cards. Works on both Cards ATI and Nvdia.

Whitepixel: Whitepixel is an open source tool supports only MD5 hash and runs only on ATI cards. The ATI cards which supported are AMD Radeon HD 5000 series and above series. It is also a Multi GPU supportable program upto 8 GPU cards.

Hashkill: Hashkill is an open source tool. It works on both AMD and Nvidia cards. It has 40 plugins for different type of passwords ranging from simple hashes MD5, SHA1 to private SSL key passphrases.

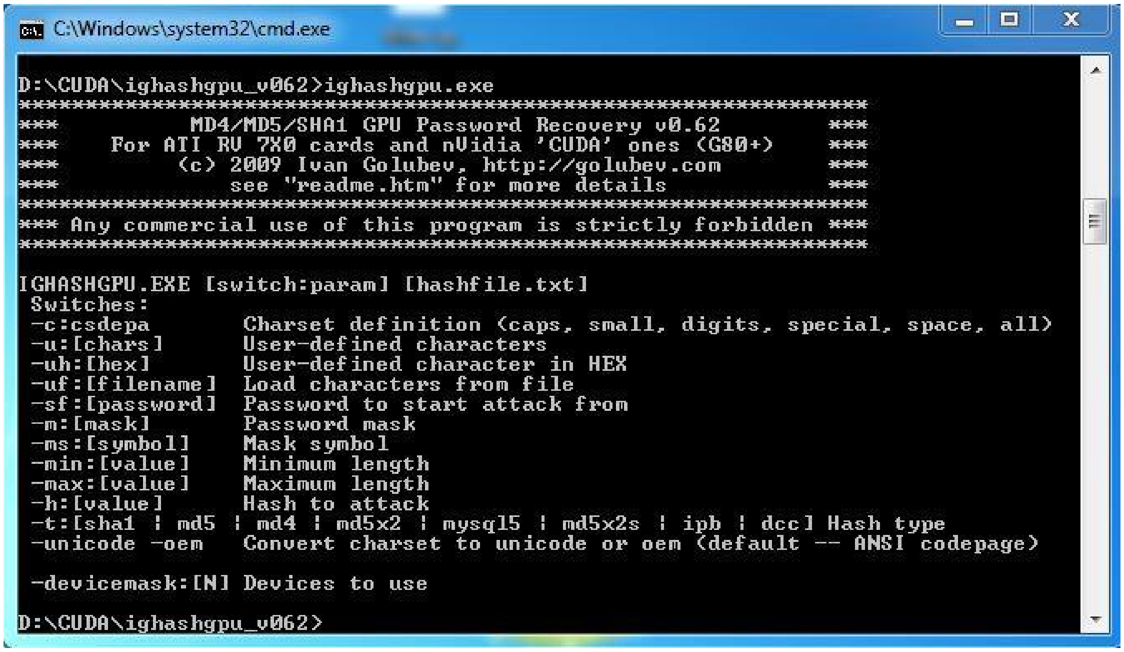
We can see now the description of all tools which are GPU supported but we can't identify that which tool is good and fast for hash cracking. So we will now test some of the tools on both Operating Systems (Windows & Linux) by cracking a MD5 hash and point out the cracking speed.

Windows CUDA Machine: For configuring cuda machine on Windows operating systems we have to install first ATI drivers the R.G catalyst according to your graphic card model.



Graphics Adapter : 1. Radeon HD 3870 X2

Tools Demonstration on Windows CUDA Machine: We are going to use IGHASHGPU. It is very simple command line tool now we will the usage command of IGHASHGPU.



```
D:\CUDA\ighashgpu_v062>ighashgpu.exe
****************************************************************
***          MD4/MD5/SHA1 GPU Password Recovery v0.62        ***
***    For ATI RV 7X0 cards and nVidia 'CUDA' ones (G80+)    ***
***         (c) 2009 Ivan Golubev, http://golubev.com        ***
***             see "readme.htm" for more details            ***
****************************************************************
*** Any commercial use of this program is strictly forbidden ***
****************************************************************

IGHASHGPU.EXE [switch:param] [hashfile.txt]
 Switches:
 -c:csdepa        Charset definition (caps, small, digits, special, space, all)
 -u:[chars]       User-defined characters
 -uh:[hex]        User-defined character in HEX
 -uf:[filename]   Load characters from file
 -sf:[password]   Password to start attack from
 -m:[mask]        Password mask
 -ms:[symbol]     Mask symbol
 -min:[value]     Minimum length
 -max:[value]     Maximum length
 -h:[value]       Hash to attack
 -t:[sha1 | md5 | md4 | md5x2 | mysql5 | md5x2s | ipb | dcc] Hash type
 -unicode -oem    Convert charset to unicode or oem (default -- ANSI codepage)

 -devicemask:[N] Devices to use

D:\CUDA\ighashgpu_v062>
```

By executing ighashgpu.exe from command line it will show the all command options with detail some of the syntax we will describe here which is necessary.

-c: for character sets defining (caps, small, digits, special, space, all)

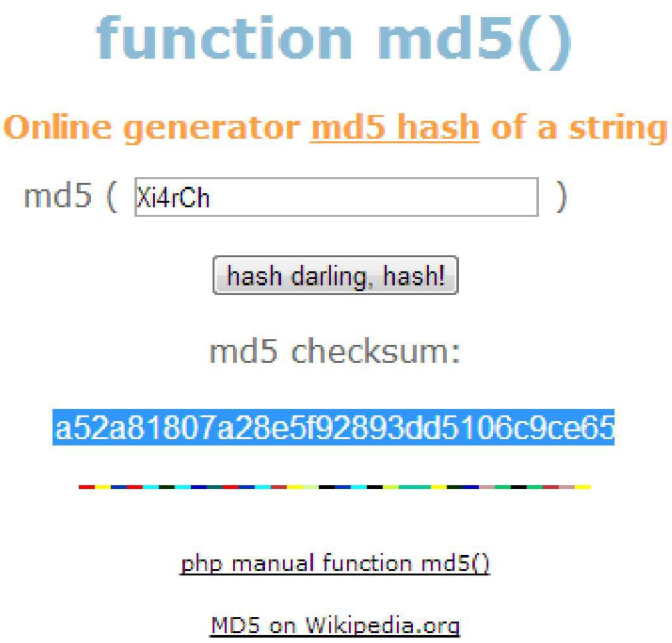
-h: hash value

-t: type of hash (MD5, MD4 or SHA1)

-min: minimum password length

-max: maximum password length

Now let us test our CUDA machine. We require a MD5 hash of a password let make it. Go to online md5 hash generator service like here we are using www.md5.cz and as password we are giving **Xi4rCh** and generate a MD5 hash of it.



function md5()

Online generator md5 hash of a string

md5 (Xi4rCh)

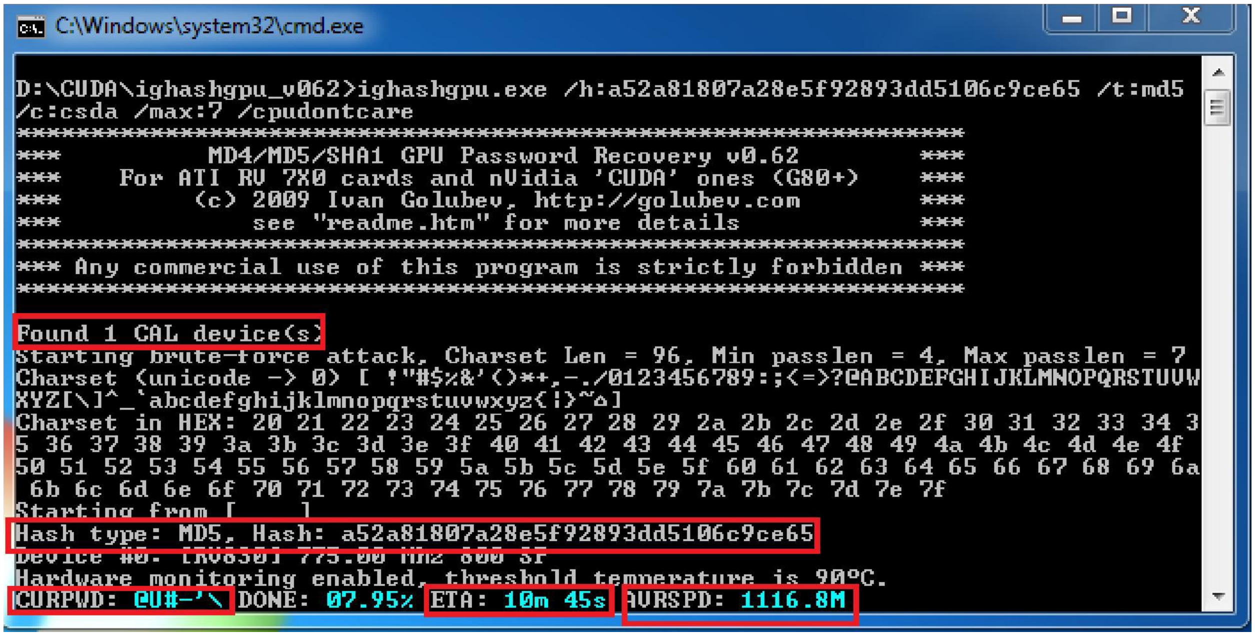
md5 checksum:

a52a81807a28e5f92893dd5106c9ce65

Now we can continue to further cracking process. Run ighashgpuu.exe and type in these commands

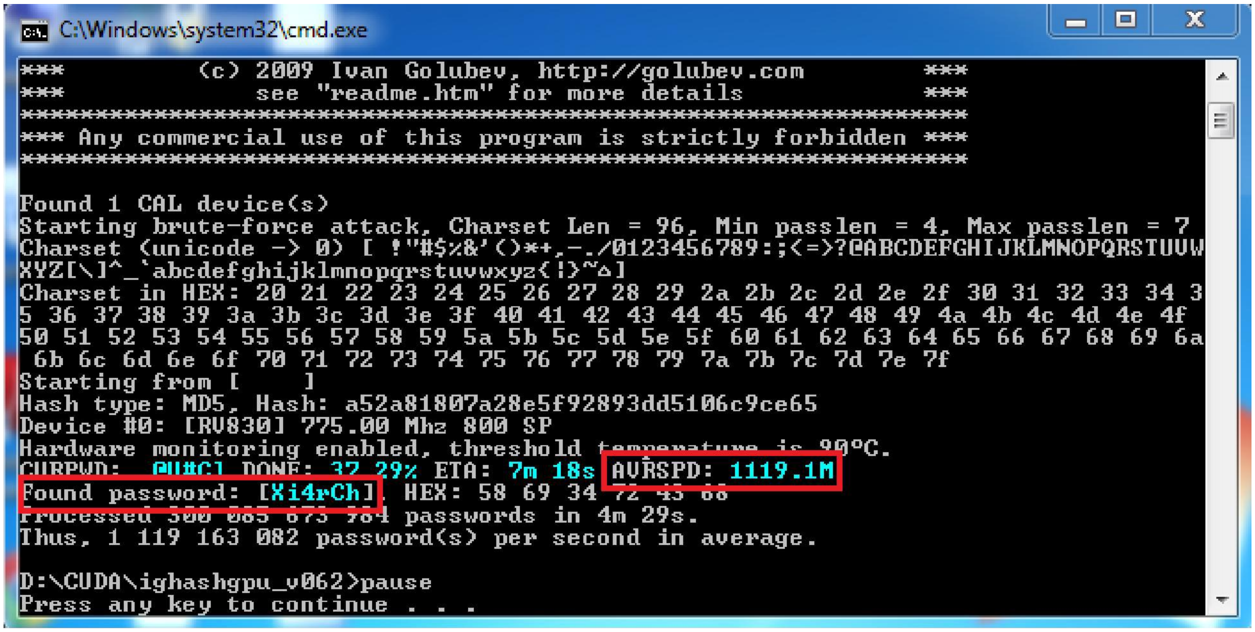
ighashgpu.exe /h:a52a81807a28e5f92893dd5106c9ce65 /t:md5 /c:csda /max:7 /cpudontcare

We already know about the syntax usage so we will not describe the syntax function here. The cracking process starts



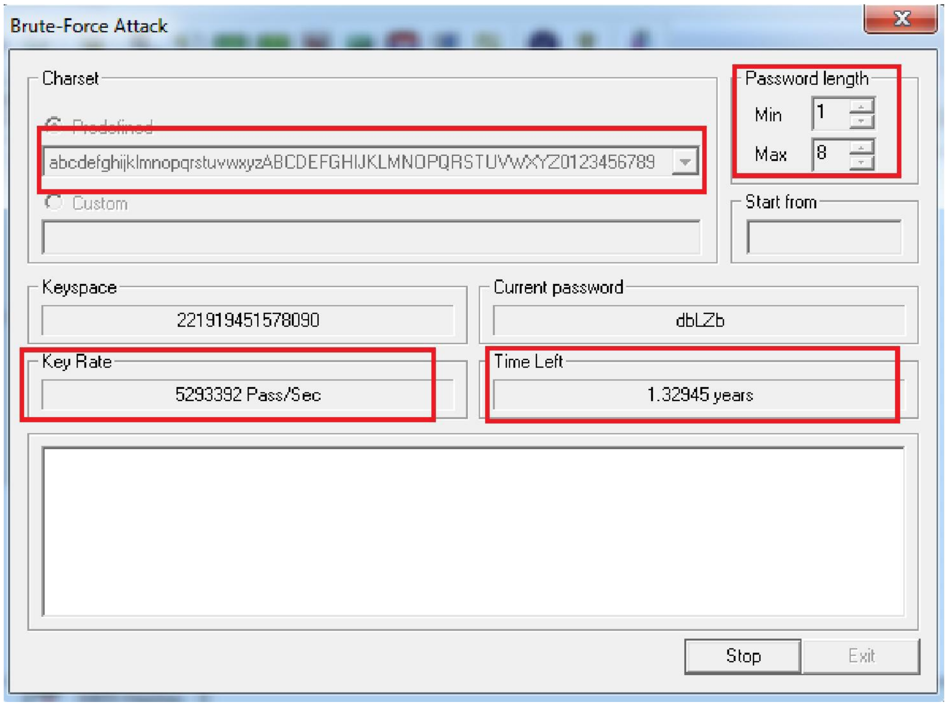
```
D:\CUDA\ighashgpu_v062>ighashgpu.exe /h:a52a81807a28e5f92893dd5106c9ce65 /t:md5
/c:csda /max:7 /cpudontcare
****************************************************************
***           MD4/MD5/SHA1 GPU Password Recovery v0.62       ***
***     For ATI RV 7X0 cards and nVidia 'CUDA' ones (G80+)    ***
***         (c) 2009 Ivan Golubev, http://golubev.com         ***
***              see "readme.htm" for more details            ***
****************************************************************
*** Any commercial use of this program is strictly forbidden ***
****************************************************************

Found 1 CAL device(s)
Starting brute-force attack, Charset Len = 96, Min passlen = 4, Max passlen = 7
Charset (unicode -> 0) [ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVW
XYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~⌂]
Charset in HEX: 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 3
5 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f
50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a
 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f
Starting from [     ]
Hash type: MD5, Hash: a52a81807a28e5f92893dd5106c9ce65
Device #0: [RV830] 775.00 MHz 800 SP
Hardware monitoring enabled, threshold temperature is 90°C.
CURPWD: @U#-'\ DONE: 07.95% ETA: 10m 45s AVRSPD: 1116.8M
```

Now in above figure we can see average password cracking speed is 1116.8 million per second and estimated time is showing approximately 11 min. But we in our case the password found in 5 minutes which we can see in below figure. The cracking speed is increases to 1119.1 million. Now we can see here that alphanumeric password (Uppercase, Lowercase, Digits) within 6 character can be cracked in 5 minutes.



```
***          (c) 2009 Ivan Golubev, http://golubev.com        ***
***              see "readme.htm" for more details            ***
*****************************************************************
*** Any commercial use of this program is strictly forbidden ***
*****************************************************************

Found 1 CAL device(s)
Starting brute-force attack, Charset Len = 96, Min passlen = 4, Max passlen = 7
Charset (unicode -> 0) [ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVW
XYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~⌂]
Charset in HEX: 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 3
5 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f
50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a
 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f
Starting from [     ]
Hash type: MD5, Hash: a52a81807a28e5f92893dd5106c9ce65
Device #0: [RV830] 775.00 Mhz 800 SP
Hardware monitoring enabled, threshold temperature is 90°C.
CURPWD:   @U#C] DONE: 37.29% ETA: 7m 18s AVRSPD: 1119.1M
Found password: [Xi4rCh] HEX: 58 69 34 72 43 68
Processed 300 085 673 784 passwords in 4m 29s.
Thus, 1 119 163 082 password(s) per second in average.

D:\CUDA\ighashgpu_v062>pause
Press any key to continue . . .
```

Let us try that if we crack the same MD5 hash with CPU power then what is the efficiency? So we are using here Cain n Able for cracking MD5 hash and see what happens.



Charset

○ Predefined

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

○ Custom

Password length

Min 1

Max 8

Start from

Keyspace 221919451578090

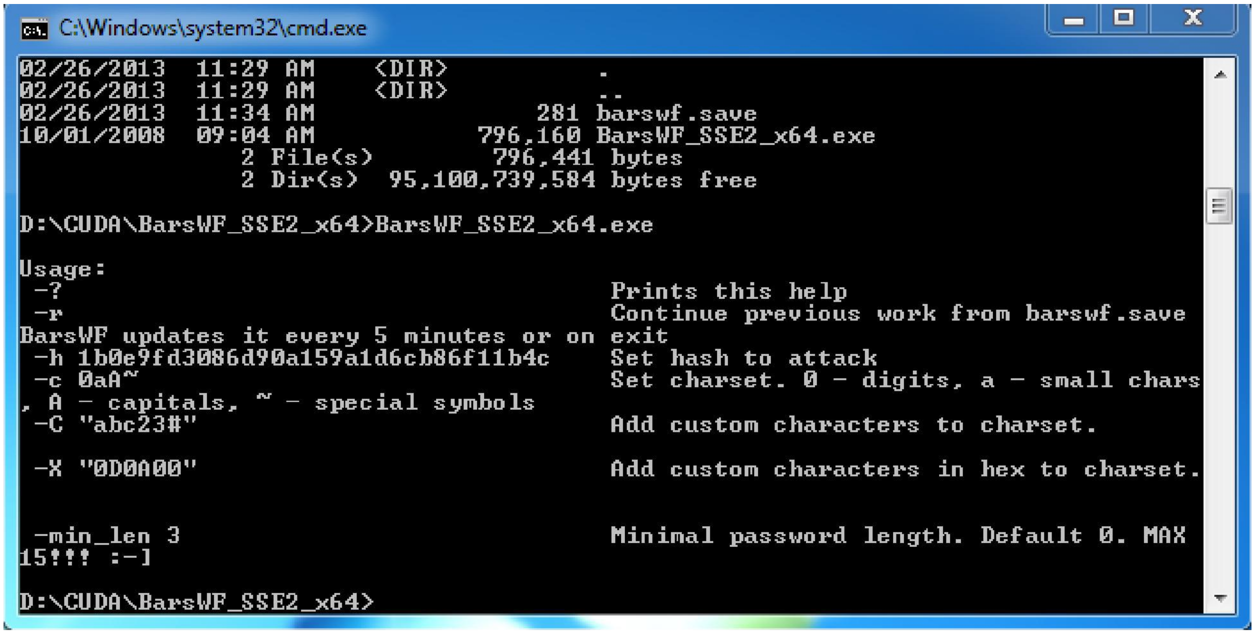
Current password dbLZb

Key Rate 5293392 Pass/Sec

Time Left 1.32945 years

In the above screenshot we can see the average time it will take to crack 1.32945 years so we can see the difference between the GPU and CPU efficiency.

BarsWF: It supports only Nvidia card so we are going to crack on CPU power**.** Execute the BarsWF.exe from command line and it will show all the command options in details some of the commands we will demonstrate here which we are going to use.



C:\Windows\system32\cmd.exe

```
02/26/2013  11:29 AM    <DIR>          .
02/26/2013  11:29 AM    <DIR>          ..
02/26/2013  11:34 AM               281 barswf.save
10/01/2008  09:04 AM           796,160 BarsWF_SSE2_x64.exe
               2 File(s)        796,441 bytes
               2 Dir(s)  95,100,739,584 bytes free

D:\CUDA\BarsWF_SSE2_x64>BarsWF_SSE2_x64.exe

Usage:
 -?                                     Prints this help
 -r                                     Continue previous work from barswf.save
BarsWF updates it every 5 minutes or on exit
 -h 1b0e9fd3086d90a159a1d6cb86f11b4c    Set hash to attack
 -c 0aA~                                Set charset. 0 - digits, a - small chars
, A - capitals, ~ - special symbols
 -C "abc23#"                            Add custom characters to charset.

 -X "0D0A00"                            Add custom characters in hex to charset.


 -min_len 3                             Minimal password length. Default 0. MAX
15!!! :-]

D:\CUDA\BarsWF_SSE2_x64>
```

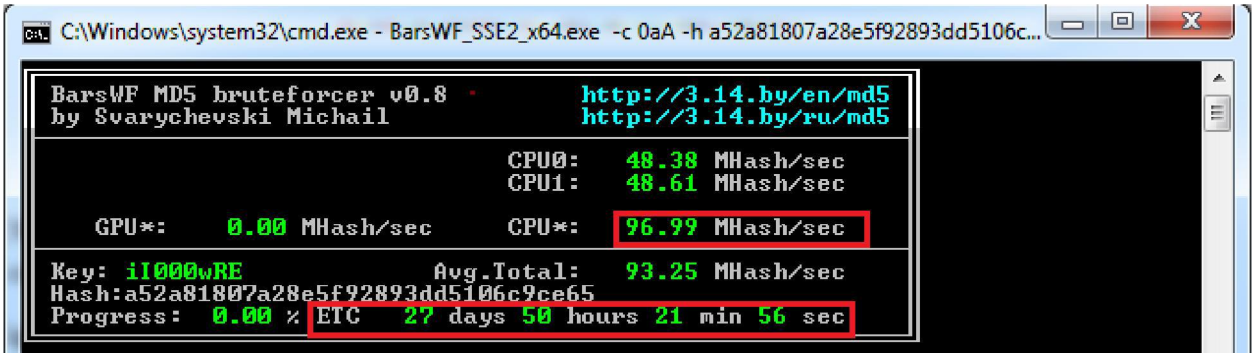
Usage Syntax:

-c: for character set defining (A-for caps, a-for small, 0-digit, ~-for special characters)

-h: hash here

-min_len: minimum password length

So here we will using the same MD5 hash and type in **BarsWF_SSE2_x64.exe –c A0a –h a52a81807a28e5f92893dd5106c9ce65 –min_len 8**



C:\Windows\system32\cmd.exe - BarsWF_SSE2_x64.exe -c 0aA -h a52a81807a28e5f92893dd5106c...

```
 BarsWF MD5 bruteforcer v0.8          http://3.14.by/en/md5
 by Svarychevski Michail              http://3.14.by/ru/md5

                              CPU0:    48.38 MHash/sec
                              CPU1:    48.61 MHash/sec

    GPU*:      0.00 MHash/sec      CPU*:    96.99 MHash/sec

 Key: iI000wRE              Avg.Total:    93.25 MHash/sec
 Hash:a52a81807a28e5f92893dd5106c9ce65
 Progress:   0.00 % ETC    27 days 50 hours 21 min 56 sec
```

We can see in above figure the estimate time it will take 27 days it means it is faster than Cain n Abel where it takes a year to crack this hash, BarsWF will take some days.

Linux CUDA Machine: Configuring CUDA machine in Linux system is not easy as Windows. The driver installation process is different in ATI and Nvidia cards.

ATI Driver installation:

1. Remove the old AMD drivers

```
sudo sh /usr/share/ati/fglrx-uninstall.sh
```

```
sudo apt-get remove --purge fglrx fglrx_* fglrx-amdcccle* fglrx-dev* xorg-driver-fglrx
```

2. Download the AMD drivers

Download from AMD website

Or via terminal

```
cd ~/; mkdir catalyst12.4; cd catalyst12.4/
```

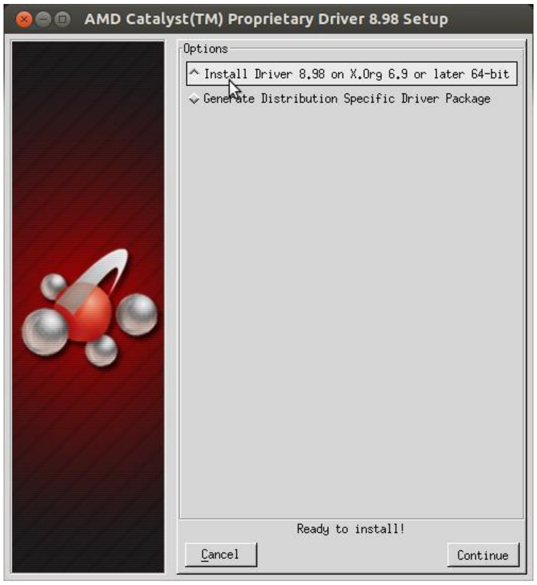
```
wget -O amd-driver-installer-12-4-x86.x86_64.run http://goo.gl/VGYWP
```

3. Installing Drivers

```
chmod +x amd-driver-installer-12-4-x86.x86_64.run
```

```
sudo sh ./amd-driver-installer-12-4-x86.x86_64.run
```

Now continue the installation wizard.



AMD Catalyst(TM) Proprietary Driver 8.98 Setup

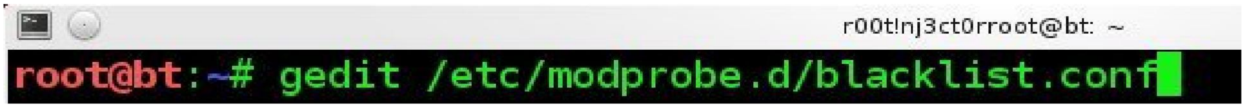
Options
Install Driver 8.98 on X.Org 6.9 or later 64-bit
Generate Distribution Specific Driver Package
Cancel
Continue

Ready to install!

Nvidia Driver Installation:

1. Edit the configuration files

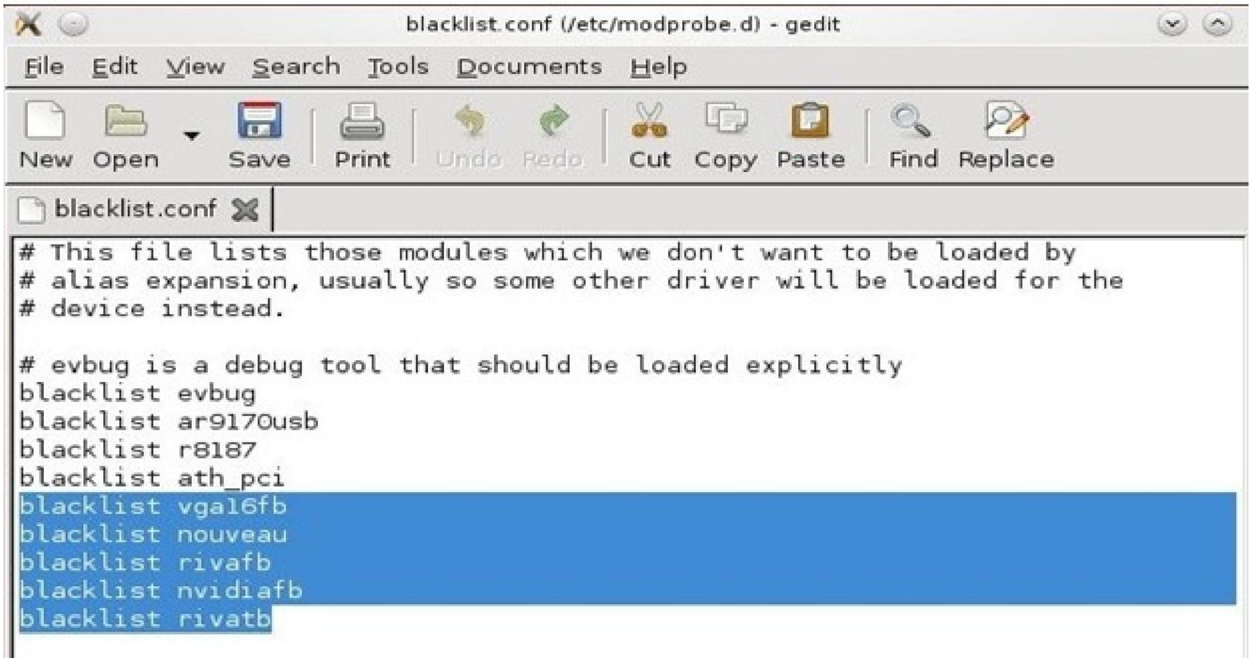
gedit /etc/modprobe.d/blacklist.conf



```
root@bt:~# gedit /etc/modprobe.d/blacklist.conf
```

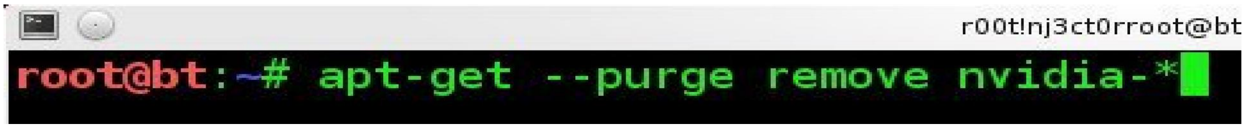
add these line in blacklist.conf file

blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv



```
# This file lists those modules which we don't want to be loaded by
# alias expansion, usually so some other driver will be loaded for the
# device instead.

# evbug is a debug tool that should be loaded explicitly
blacklist evbug
blacklist ar9170usb
blacklist r8187
blacklist ath_pci
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatb
```

2. **apt-get --purge remove nvidia-***

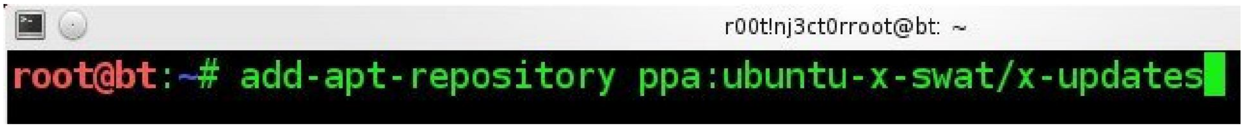


```
root@bt:~# apt-get --purge remove nvidia-*
```

3. Reboot the system.

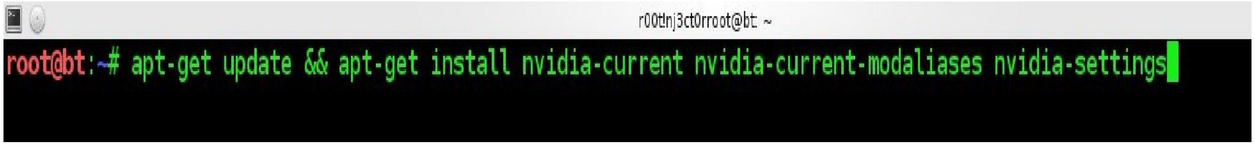
4. Installing Drivers

add-apt-repository ppa:ubuntu-x-swat/x-updates



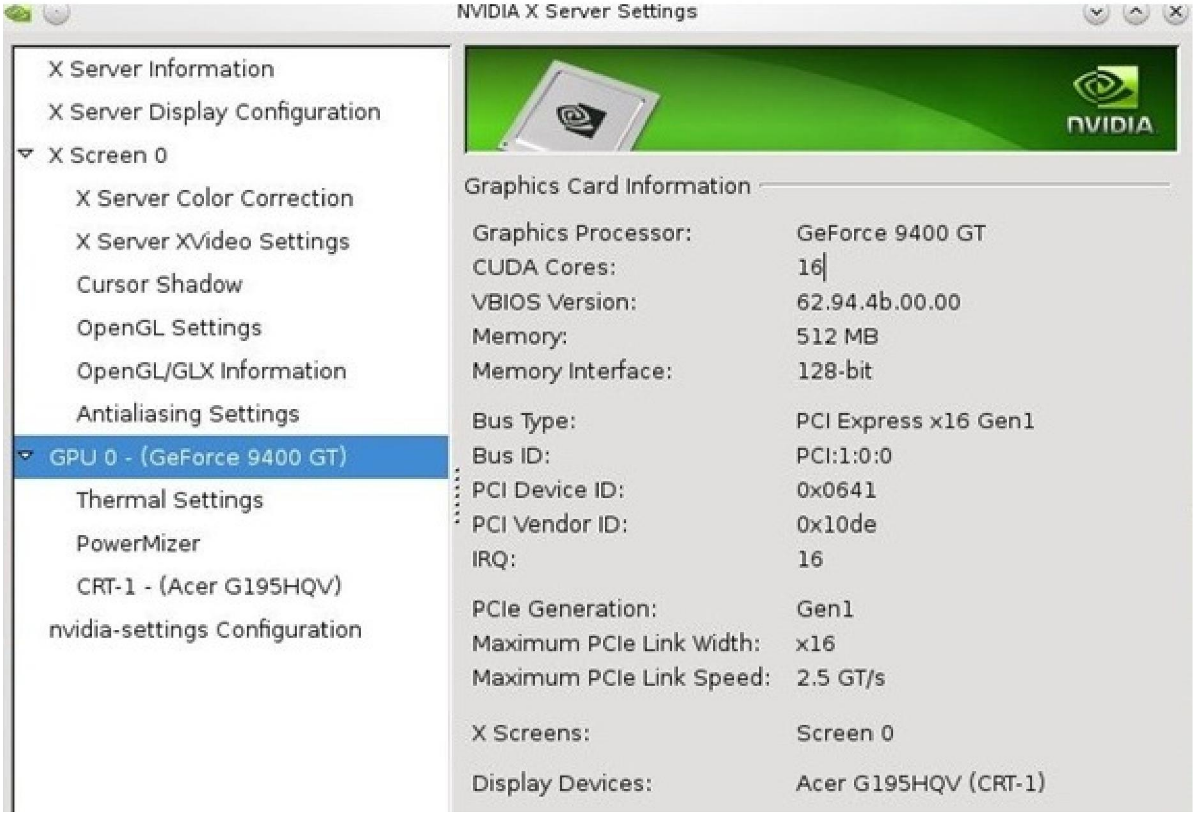
```
root@bt:~# add-apt-repository ppa:ubuntu-x-swat/x-updates
```

apt-get update && apt-get install nvidia-current nvidia-current-modaliases nvidia-settings



```
root@bt:~# apt-get update && apt-get install nvidia-current nvidia-current-modaliases nvidia-settings
```

5. Again reboot and you will Nvidia option in your utilities.



Graphics Card Information

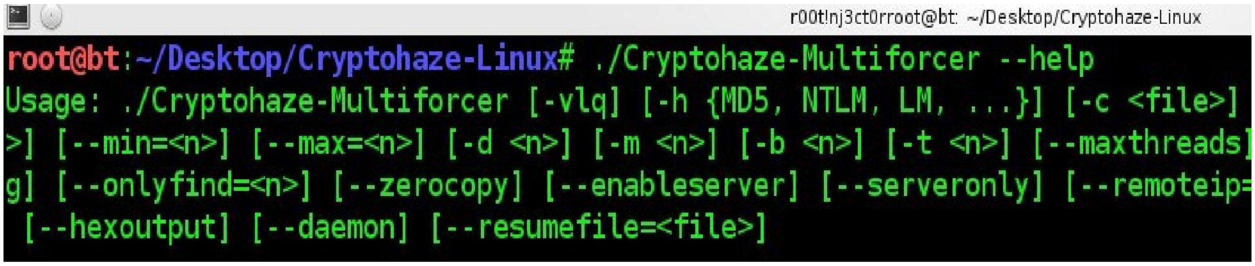
```
Graphics Processor:        GeForce 9400 GT
CUDA Cores:                16
VBIOS Version:             62.94.4b.00.00
Memory:                    512 MB
Memory Interface:          128-bit

Bus Type:                  PCI Express x16 Gen1
Bus ID:                    PCI:1:0:0
PCI Device ID:             0x0641
PCI Vendor ID:             0x10de
IRQ:                       16

PCIe Generation:           Gen1
Maximum PCIe Link Width:   x16
Maximum PCIe Link Speed:   2.5 GT/s

X Screens:                 Screen 0

Display Devices:           Acer G195HQV (CRT-1)
```

<u>ToolsDemonstrationonLinuxCUDAMachine:</u>

In Linux operating system we are going to use Nvidia cards with has less cuda cores than ATI Radeon card.

Cryptohaze Linux: Now let’s see the usage command for Cryptohaze. Type in this command

./Cryptohaze-Multiforcer –help



```
r00t!nj3ct0rroot@bt: ~/Desktop/Cryptohaze-Linux
root@bt:~/Desktop/Cryptohaze-Linux# ./Cryptohaze-Multiforcer --help
Usage: ./Cryptohaze-Multiforcer [-vlq] [-h {MD5, NTLM, LM, ...}] [-c <file>]
>] [--min=<n>] [--max=<n>] [-d <n>] [-m <n>] [-b <n>] [-t <n>] [--maxthreads]
g] [--onlyfind=<n>] [--zerocopy] [--enableserver] [--serveronly] [--remoteip=
 [--hexoutput] [--daemon] [--resumefile=<file>]
```

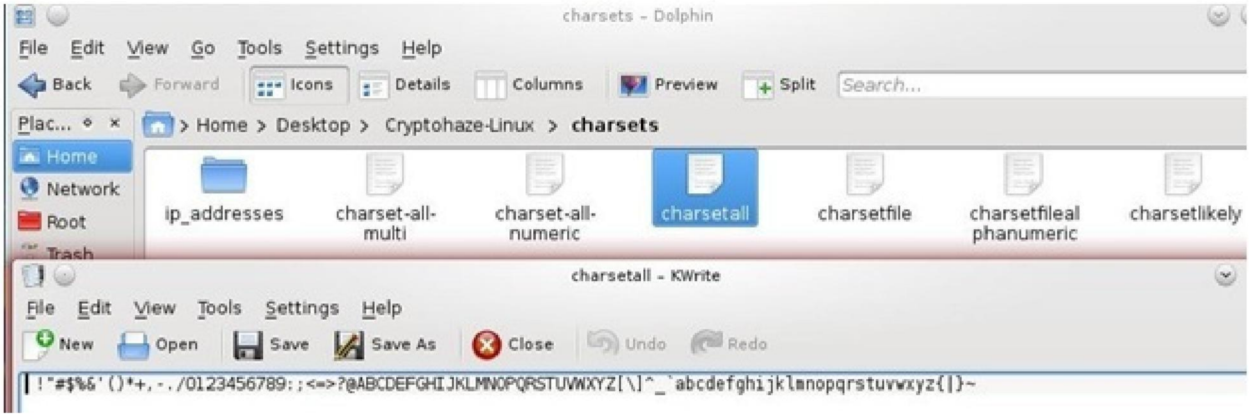
We have to use only three commands for cracking a hash, which is:

-c (For charset files)

-h (For defining hash type)

-f (For hash file location)

Charset: The term charset is short form of character set. It is a defined list of characters recognized by the computer hardware and software. Like you create a text document and define characters in lower case a-z and save it. Now you can create many charset file by defining own characters 0-9, A-Z and more like shown in below Figure.

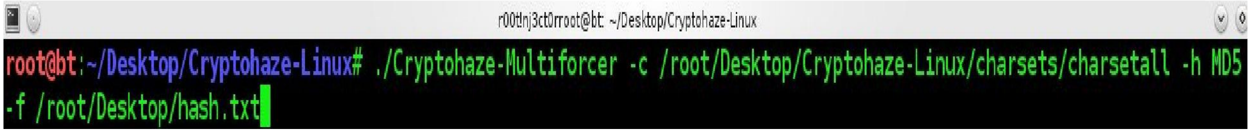


charsets – Dolphin
File Edit View Go Tools Settings Help
Back Forward Icons Details Columns Preview Split Search...
Plac...
Home
Network
Root
Trash
Home > Desktop > Cryptohaze-Linux > charsets
ip_addresses
charset-all-multi
charset-all-numeric
charsetall
charsetfile
charsetfilealphanumeric
charsetlikely
charsetall – KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo

```
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

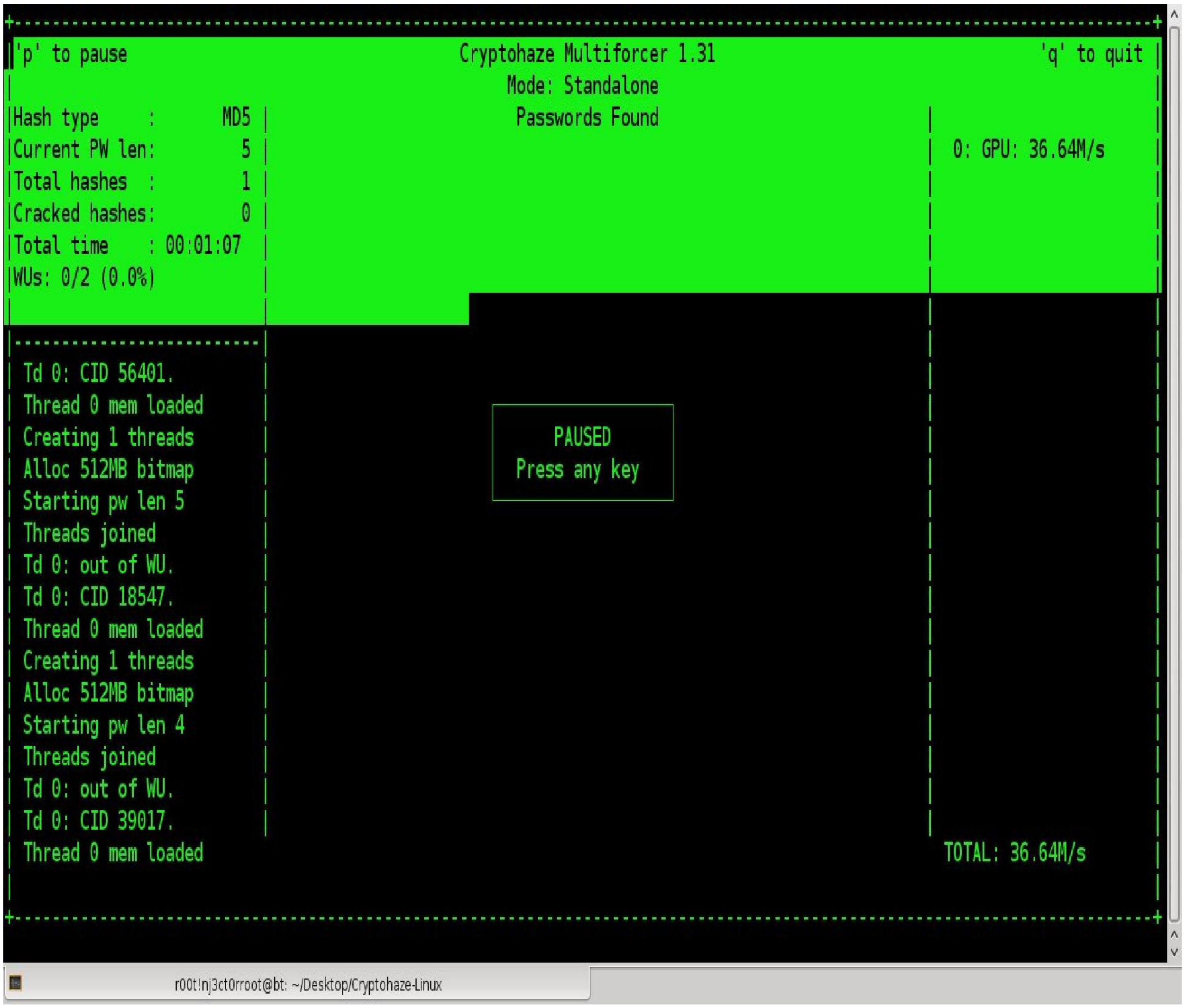
Now let’s start cracking. Type in:

./Cryptohaze-Multiforcer –c /root/Desktop/Cryptohaze-Linux/charsets/charsetall –h MD5 –f /root/Desktop/hash.txt



```
r00t!nj3ct0rroot@bt: ~/Desktop/Cryptohaze-Linux
root@bt:~/Desktop/Cryptohaze-Linux# ./Cryptohaze-Multiforcer -c /root/Desktop/Cryptohaze-Linux/charsets/charsetall -h MD5
-f /root/Desktop/hash.txt
```

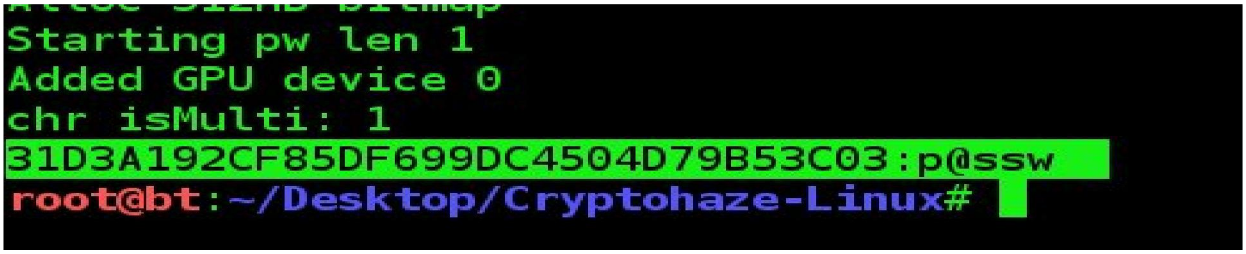
Then press enter and cracking process starts.



```
'p' to pause                     Cryptohaze Multiforcer 1.31                        'q' to quit
                                      Mode: Standalone
Hash type      :      MD5 |           Passwords Found                    |
Current PW len:         5 |                                              |  0: GPU: 36.64M/s
Total hashes  :         1 |                                              |
Cracked hashes:         0 |                                              |
Total time     : 00:01:07 |                                              |
WUs: 0/2 (0.0%)           |                                              |
                          |                                              |
 -----------------------  |                                              |
 Td 0: CID 56401.         |                                              |
 Thread 0 mem loaded      |                                              |
 Creating 1 threads       |               PAUSED                         |
 Alloc 512MB bitmap       |            Press any key                     |
 Starting pw len 5        |                                              |
 Threads joined           |                                              |
 Td 0: out of WU.         |                                              |
 Td 0: CID 18547.         |                                              |
 Thread 0 mem loaded      |                                              |
 Creating 1 threads       |                                              |
 Alloc 512MB bitmap       |                                              |
 Starting pw len 4        |                                              |
 Threads joined           |                                              |
 Td 0: out of WU.         |                                              |
 Td 0: CID 39017.         |                                              |
 Thread 0 mem loaded                                                        TOTAL: 36.64M/s
```

r00t!nj3ct0rroot@bt: ~/Desktop/Cryptohaze-Linux

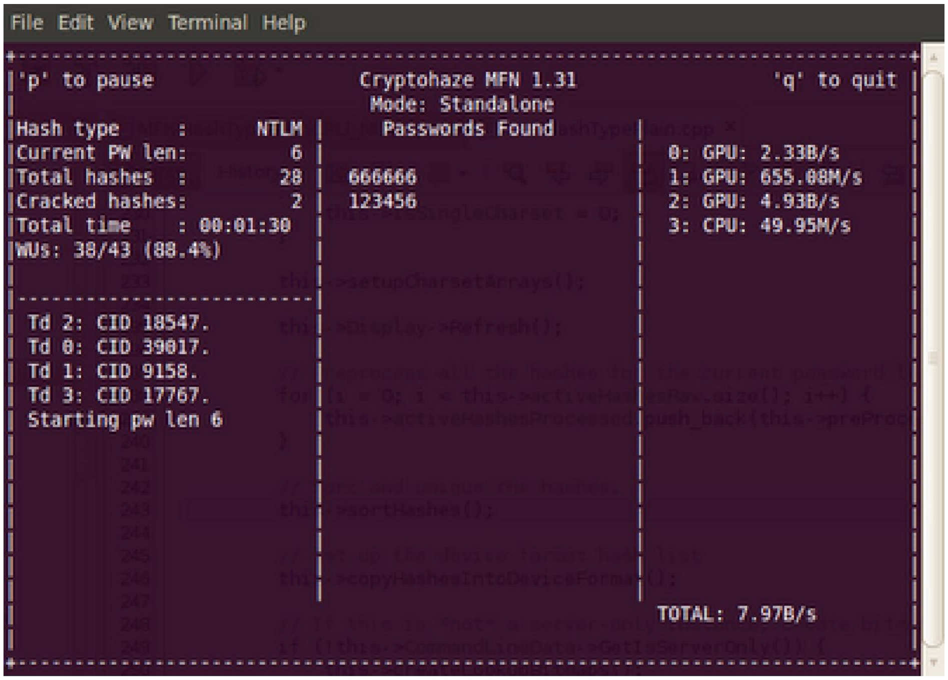
See in top right corner side there shows my GPU cracking speed is only 36.64M/s it's very slow because my Nvidia card has only 16 cuda cores. After successfully cracking it shows the password from your hash which is **p@ssw**



```
Alloc 512MB bitmap
Starting pw len 1
Added GPU device 0
chr isMulti: 1
31D3A192CF85DF699DC4504D79B53C03:p@ssw
root@bt:~/Desktop/Cryptohaze-Linux#
```

New Multiforcer: New Multiforcer is new revision version of Cryptohaze Multiforcer which supports ATI cards. The usage command is same as Cryptohaze Multiforcer. We have to pass these commands –openclplatform=0, --opencldevice=1 –bfi_init

./NewMultiforcer --openclplatform=0 --opencldevice=1 –bfi_init -h Hash type -c my charsets dir -f my file dir



```
+------------------------------------------------------------------------+
|'p' to pause               Cryptohaze MFN 1.31                'q' to quit |
|                            Mode: Standalone                              |
|Hash type      :      NTLM |    Passwords Found        |                  |
|Current PW len:          6 |                           |  0: GPU: 2.33B/s |
|Total hashes   :        28 |  666666                   |  1: GPU: 655.08M/s|
|Cracked hashes:          2 |  123456                   |  2: GPU: 4.93B/s |
|Total time     : 00:01:30  |                           |  3: CPU: 49.95M/s|
|WUs: 38/43 (88.4%)         |                           |                  |
|                           |                           |                  |
|---------------------------|                           |                  |
| Td 2: CID 18547.          |                           |                  |
| Td 0: CID 39017.          |                           |                  |
| Td 1: CID 9158.           |                           |                  |
| Td 3: CID 17767.          |                           |                  |
| Starting pw len 6         |                           |                  |
|                           |                           |                  |
|                           |                           |                  |
|                                                         TOTAL: 7.97B/s   |
|                                                                          |
+------------------------------------------------------------------------+
```

Which is better ATI or Nvidia?

Now which card is better it depends on many factors like price, tools and Cuda cores. If we are matching the speed of password cracking then we see ATI cards are better than Nvidia because the number of cuda cores is greater than Nvidia cards. Nvidia cards are expensive than ATI cards. But nvidia provides a high performance cards like Tesla cards and Titan cards which are very expensive but very fast performance. Maximum tools are Nvidia compatible on both platforms Windows and Linux. We found that very few tools are support ATI cards. We found that if you don't care of money then definitely go through with Nvidia cards but if you have small budget then go for ATI cards.

Conclusions: Hence we conclude that if we used a high performance graphic card with high cores which is greater than 512 cores and also use more than one card than the cracking speed of our machine is much faster than this machine, here we see the efficiency of both ATI and Nvidia cards. When we are using ATI card which has 3200 cuda cores it gives a speed of 1116.8 Million/second and when we were using only Nvidia card which has only 16 cuda cores it gives only 36 Million/second. Now you can understand the difference and importance of Cuda cores.

References:

http://en.wikipedia.org/wiki/CUDA

http://golubev.com/gpuest.htm

http://cyruslab.wordpress.com/2012/01/26/installing-nvidia-on-backtrack5r1/

About Me:

Rohit Shaw is a Certified Ethical Hacker works as a penetration tester with Xiarch AAG Group. He has experience in pentesting, social engineering, password cracking and malware obfuscation.