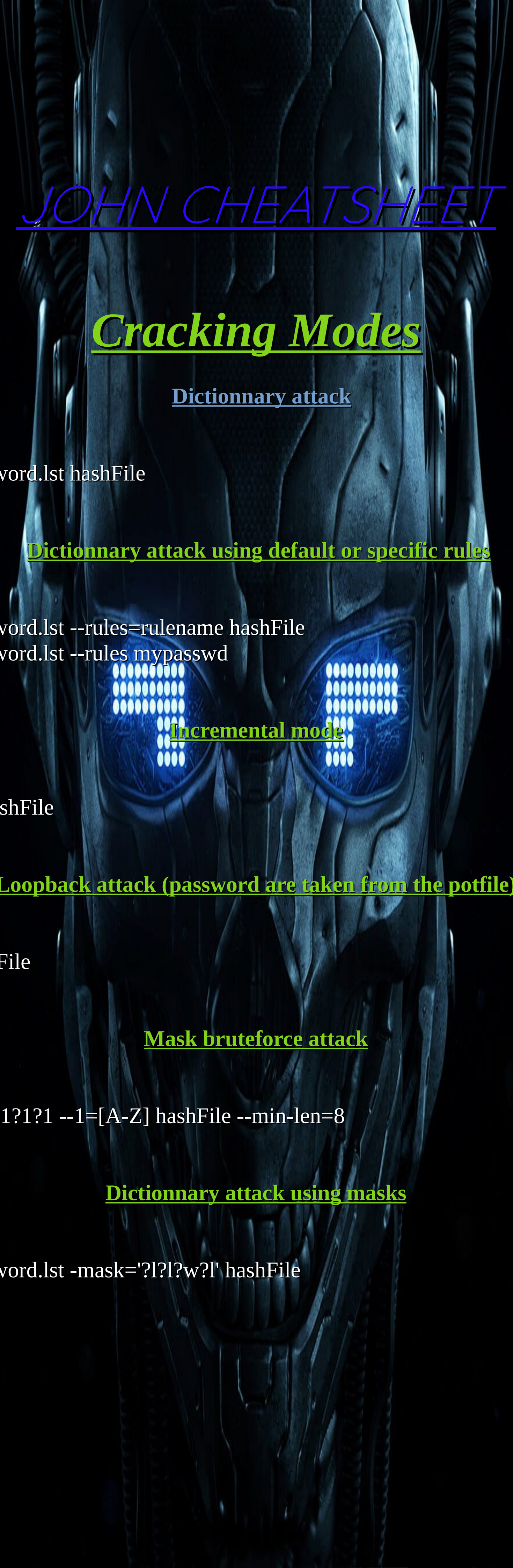
JOHN THE RIPPER CHEATSHEET

THIS CHEATSHEET MAKES YOUR WORK EASIER THAN BEFORE.

--powered by--

INDIAN CYBER ARMY
WEB DRAGON



JOHN CHEATSHEET

Cracking Modes

Dictionnary attack

```
john --wordlist=password.lst hashFile
```

Dictionnary attack using default or specific rules

```
john --wordlist=password.lst --rules=rulename hashFile
john --wordlist=password.lst --rules mypasswd
```

Incremental mode

```
john --incremental hashFile
```

Loopback attack (password are taken from the potfile)

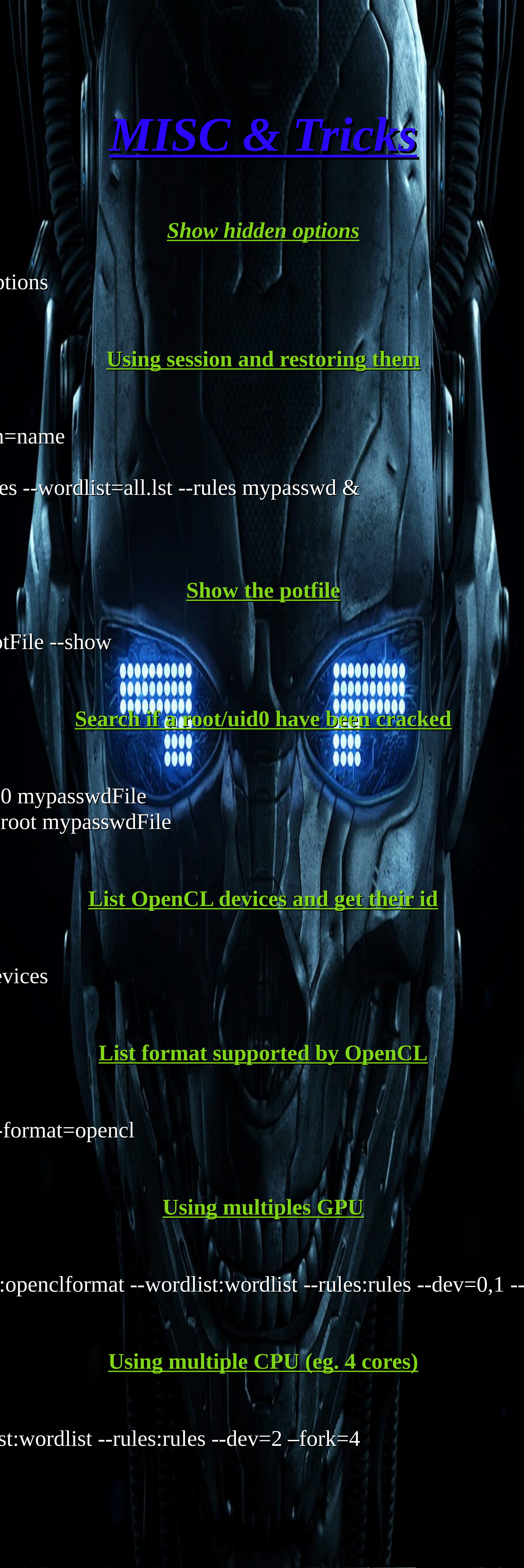
```
john --loopback hashFile
```

Mask bruteforce attack

```
john --mask=?1?1?1?1?1?1 --1=[A-Z] hashFile --min-len=8
```

Dictionnary attack using masks

```
john --wordlist=password.lst -mask='?l?l?w?l' hashFile
```



MISC & Tricks

Show hidden options

```
john --list=hidden-options
```

Using session and restoring them

```
john hashes --session=name
john --restore=name
john --session=allrules --wordlist=all.lst --rules mypasswd &
john status
```

Show the potfile

```
john hashes --pot=potFile --show
```

Search if a root/uid0 have been cracked

```
john --show --users=0 mypasswdFile
john --show --users=root mypasswdFile
```

List OpenCL devices and get their id

```
john --list=opencl-devices
```

List format supported by OpenCL

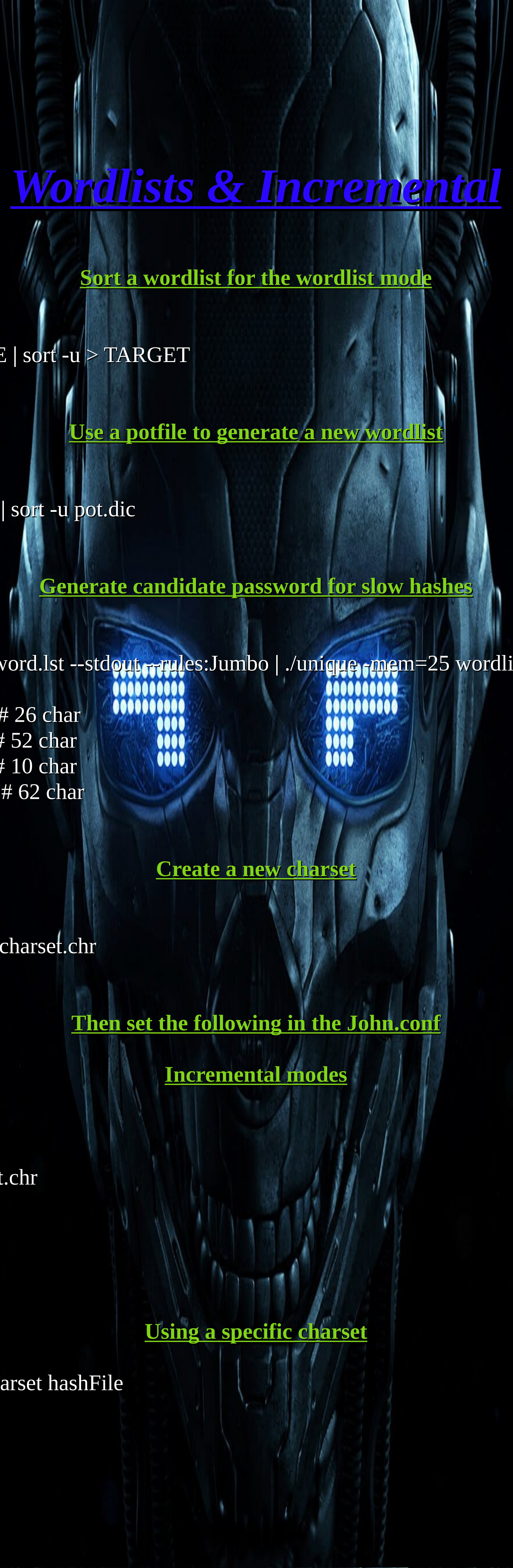
```
john --list=formats --format=opencl
```

Using multiples GPU

```
john hashes --format:openclformat --wordlist:wordlist --rules:rules --dev=0,1 --fork=2
```

Using multiple CPU (eg. 4 cores)

```
john hashes --wordlist:wordlist --rules:rules --dev=2 –fork=4
```



Wordlists & Incremental

Sort a wordlist for the wordlist mode

```
tr A-Z a-z < SOURCE | sort -u > TARGET
```

Use a potfile to generate a new wordlist

```
cut -d ':' -f 2 john.pot | sort -u pot.dic
```

Generate candidate password for slow hashes

```
john --wordlist=password.lst --stdout --rules:Jumbo | ./unique -mem=25 wordlist.uniq

--incremental:Lower # 26 char
--incremental:Alpha # 52 char
--incremental:Digits # 10 char
--incremental:Alnum # 62 char
```

Create a new charset

```
john --make-charset=charset.chr
```

Then set the following in the John.conf

Incremental modes

```
[Incremental:charset]
File = $JOHN/charset.chr
MinLen = 0
MaxLen = 31
CharCount = 95
```

Using a specific charset

```
john --incremental:charset hashFile
```

Rules

Predefined rules

```
--rules:Single
--rules:Wordlist
--rules:Extra
--rules:Jumbo   # All the above
--rules:KoreLogic
--rules:All   # All the above
```

Create a new rule in John.conf

```
[List.Rules:Tryout]
l
u
...
```

Rule	Description
l	Convert to lowercase
u	Convert to uppercase
c	Capitalize
l r	Lowercase the word and reverse it
l Az"2015"	Lowercase the word and append "2015" at the end
d	Duplicate
l A0"2015"	Lowercase the word and append "2015" at the beginning
A0"#"Az"#"	Add "#" at the beginning and the end of the word
C	Lowercase the first char and uppercase the rest
t	Toggle case of all char
TN	Toggle the case of the char in position N
r	Reverse the word
f	Reflect (Fred --> Fredderf)
{	Rotate the word left
}	Rotate the word right
$x	Append char X to the word
^x	Prefix the word with X char
[	Remove the first char from the word
]	Remove the last char from the word
DN	Delete the char in position N
xNM	Extract substring from position N for M char
iNX	Insert char X in position N and shift the rest right
oNX	Overstrike char in position N with X
S	Shift case
V	Lowercase vowels and uppercase consonants
R	Shift each char right on the keyboard
L	Shift each char left on the keyboard
<N	Reject the word unless it is less than N char long
>N	Reject the word unless it is greater than N char long
\'N	Truncate the word at length N