

# Trabalhando com Hashes

+ Para ver de maneira prática que realmente os protocolos de hashes geram hashes únicos (na vdd nem tão únicos, como é o caso do já ultrapassado MD5), podemos fazer os testes de conversão diretamente no próprio terminal:

```
echo -n "Ricardo" | md5sum
```

```
L# echo -n "Ricardo" | md5sum  
c899a91880ee511c03f5810cf9eaa022 -
```

```
echo -n "mrcat" | md5sum
```

```
L# echo -n "mrcat" | md5sum  
cd6689cf93ce0be22258bef928b160ec -
```

```
echo -n " Nome bem bem grandre" | md5sum
```

```
L# echo -n " Nome bem bem grandre" | md5sum  
5e1313ce943d8ed5aecde3fb668a2fde -
```

→ Veja que os nomes a serem criptografados são diferentes, mas os hashes têm tamanhos idênticos

+ Se baixarmos um programa como o putty.exe, podemos ver o hash associado a ele usando o seguinte comando

```
md5sum putty.exe
```

+ Se copiarmos o programa para pretty2.exe, por exemplo, o código hash ainda será o mesmo

+ Caso mudemos apenas 1 byte desse programa [na aula foi usado o blessed pra isso], o código hash já será diferente