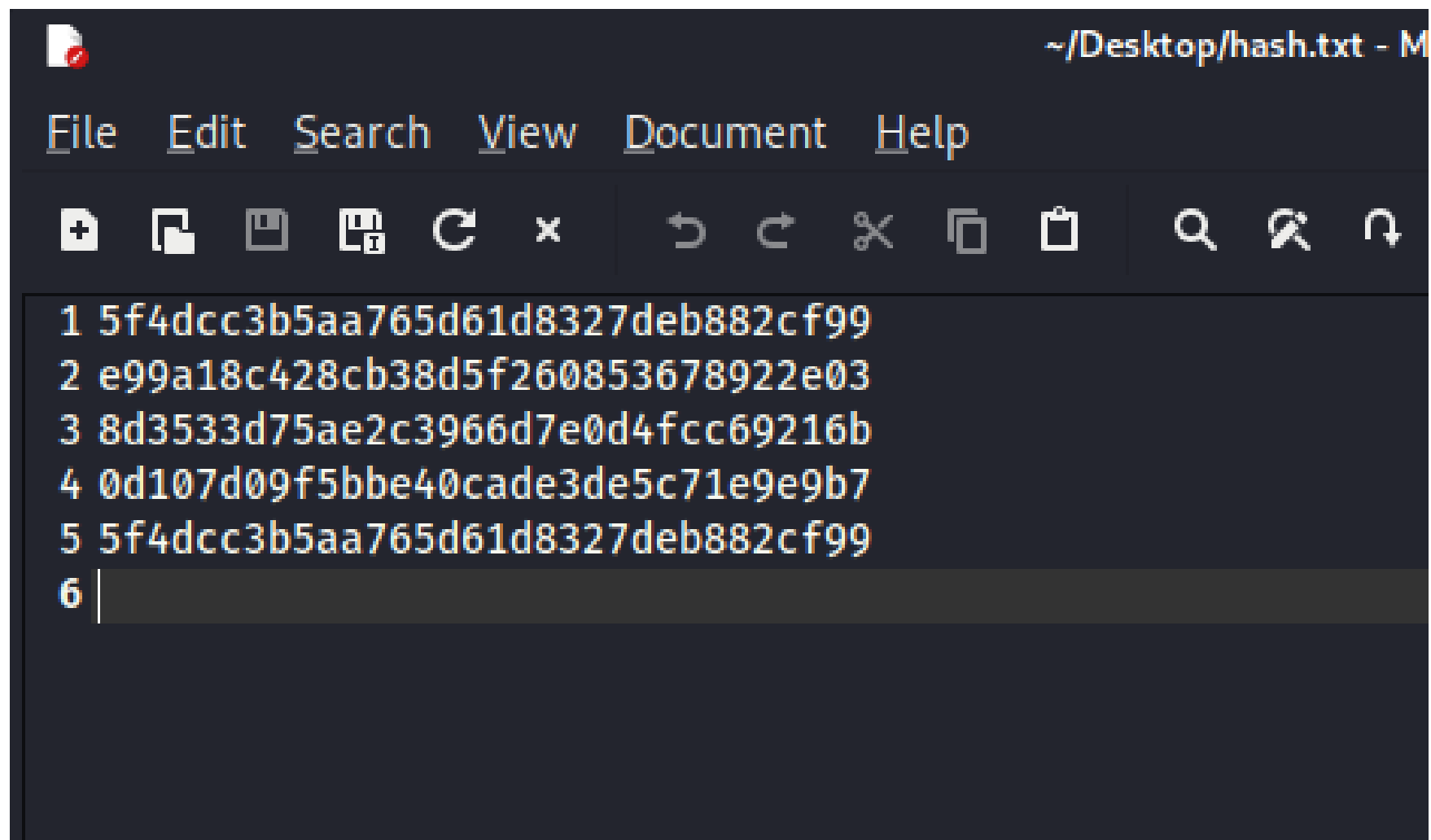


Crittografia Hash

File con le pw in codice Hash



The image shows a text editor window titled `~/Desktop/hash.txt - M`. The menu bar includes `File`, `Edit`, `Search`, `View`, `Document`, and `Help`. The toolbar contains icons for file operations (new, open, save, save as, undo, redo, close, copy, paste) and editing (find, replace, repeat). The text area contains five lines of MD5 hashes, each preceded by a number from 1 to 5. The sixth line is being edited, showing the number 6 followed by a cursor.

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6 |
```

John /home/kali/Desktop/hash.txt

```
└─$ john /home/kali/Desktop/hash.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
```

John /home/kali/Desktop/hash.txt -format=Raw-MD5

```
(kali@kali)-[~]  
$ john /home/kali/Desktop/hash.txt --format=Raw-md5  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=6  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
password      (?)  
password      (?)  
abc123        (?)  
letmein       (?)  
Proceeding with incremental:ASCII  
charley       (?)  
5g 0:00:00:00 DONE 3/3 (2023-06-07 09:31) 23.80g/s 848371p/s 848371c/s 852028C/s stevy13..chertsu  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

John /home/kali/Desktop/hash.txt --show --format=Raw-MD5

```
(kali@kali)-[~]  
$ john /home/kali/Desktop/hash.txt --show --format=Raw-md5  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
5 password hashes cracked, 0 left  
  
(kali@kali)-[~]  
$
```

Conclusioni

- In se il tool john the ripper , è molto intuitivo e semplicemente con quei 3 comandi sono riuscito a capire come decifrare le password in hash.
- Le password ad ogni modo erano molto semplici e facili da decifrare, se fossero state più complicate, sarebbero state più complicate da craccare.