```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-02-28 08:53) 200.0g/s 144000p/s 144000c/s 192000C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 ./Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

┌──(kali㉿kali)-[~]
└─$
```

In questa prima fase, possiamo notare di aver effettuato un attacco di tipo dictionary, in questo caso usando il dizionario rockyou.txt che precedentemente abbiamo unzippato nella directory che segue. Il comando –wordlist usa appunto il dizionario specificato per ricercare le password ricercate, con il comando –format=raw-md5 gli stiamo dicendo che l'hash in cui troverà le password è md5, quindi saprà come decodificarle. Successivamente gli passiamo il file in cui troverà gli hash e ci restituirà come da screen le password. Con il comando show, ci restituisce anche le password doppiate.

```
┌──(kali㉿kali)-[~]
└─$ john --incremental --format=raw-md5 Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (?)
charley          (?)
password         (?)
letmein          (?)
4g 0:00:00:00 DONE (2024-02-28 10:25) 4.040g/s 2579Kp/s 2579Kc/s 3028KC/s letebru..letmish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

In questa fase, con il comando incremental, stiamo effettuando un attacco di tipo dictionary, ma è un comando più lento di wordlist, siccome proverà tutte le combinazioni di password, partendo da 1 sola lettera. Proverà quindi con a,b,c,d,e ecc.. Per poi passare a due lettere e provare tutte le possibili combinazioni e così via fino a trovare la password. Anche in questo caso gli passiamo il comando –format=raw-md5 per dirgli il formato in cui saranno scritti gli hash. E successivamente gli passeremo anche il file da cui riceve gli hash, ci risponderà come da screen con le password.

Con il comando show, come prima, ci restuituirà anche le password doppiate.