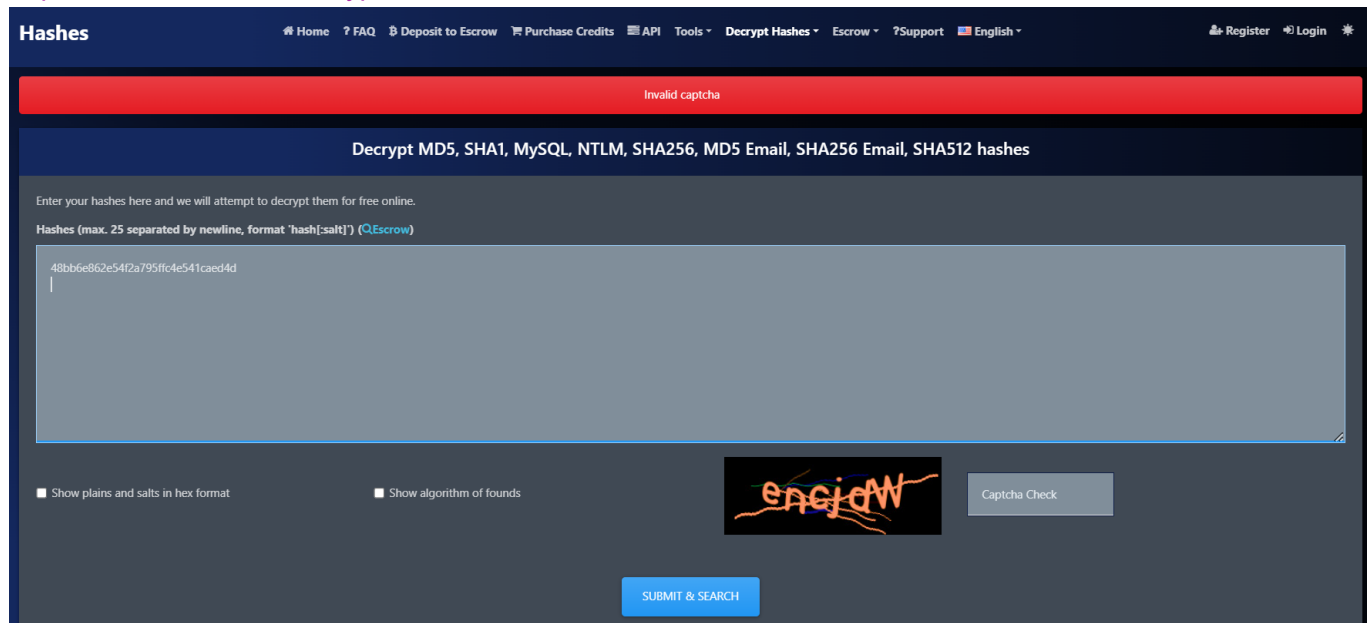


<https://tryhackme.com/room/crackthehash>

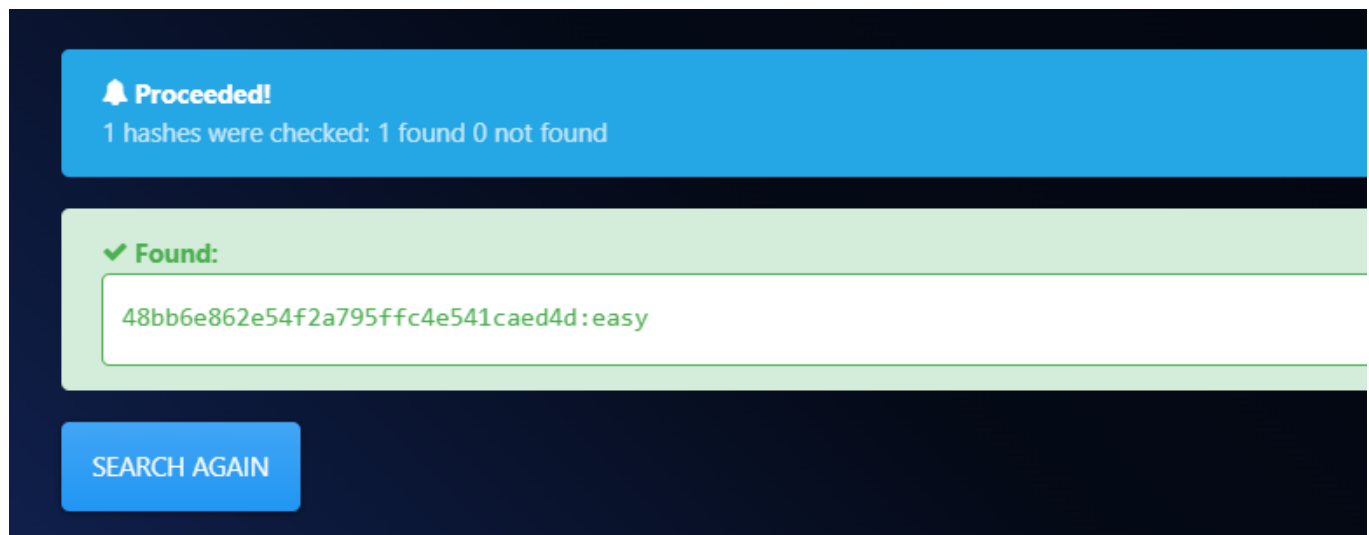
Level 1

For all the question in level 1 and first two in level 2 you can use the tool below. All you have to do is just copy and pasting the hash there and you will get the original text.

<https://hashes.com/en/decrypt/hash>



The screenshot shows the Hashes.com website interface. At the top, there's a navigation bar with links like Home, FAQ, Deposit to Escrow, Purchase Credits, API, Tools, Decrypt Hashes, Escrow, Support, and a language selector set to English. There are also links for Register and Login. Below the navigation bar, a red banner displays "Invalid captcha". The main heading is "Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512 hashes". A subtext says "Enter your hashes here and we will attempt to decrypt them for free online." Below this, a label indicates "Hashes (max. 25 separated by newline, format 'hash[:salt]') (Escrow)". A large text input field contains the hash "48bb6e862e54f2a795ffc4e541caed4d". At the bottom left, there are two checkboxes: "Show plains and salts in hex format" and "Show algorithm of founds". In the center is a "SUBMIT & SEARCH" button. To the right of the button is a "captcha" logo and a "Captcha Check" button.



The screenshot shows the result of a successful hash decryption on the Hashes.com website. A blue banner at the top says "Proceeded!" and "1 hashes were checked: 1 found 0 not found". Below this, a green banner says "Found:". A white box displays the result: "48bb6e862e54f2a795ffc4e541caed4d : easy". At the bottom, there is a blue button labeled "SEARCH AGAIN".

Question 1: 48bb6e862e54f2a795ffc4e541caed4d

Answer: easy

Question 2: CBFDAC6008F9CAB4083784CBD1874F76618D2A97

Answer: password123

Question 3: 1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032

Answer: letmein

Question 4: 2y\$12Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom

Answer: bleh

Question 5: 279412f945939ba78ce0758d3fd83daa

Answer: Eternity22

Level 2

Question 1: F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85

Answer: paule

Question 2: 1DFECA0C002AE40B8619ECF94819CC1B

Answer: n63umy8lkf4i

For the last 2 questions we have a salted hash. A salted hash is a cryptographic hash function that is used in combination with a random value called a "salt" to enhance the security of password storage.

We can crack salted hashes with hashcat tool.

Question 3:

Hash:\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxlf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.

Salt: aReallyHardSalt

First we need to identify the hash type. On the website https://hashcat.net/wiki/doku.php?id=example_hashes we look for the hash starting with \$6 and find that it is SHA12 crypt with mode 1800.

1800	sha512crypt \$6\$, SHA512 (Unix) ²	\$6\$52450745\$k5ka2p8bFuSmoVT1tzOyyuaREkkKBcCNqoDKzYiJL9RaE8yM
------	---	---

Now, we can crack the hash.

We will run `hashcat -m 1800 <hash file location> <wordlist file location>` on terminal.

Create file named myhash.txt and paste the hash in this file. As a wordlist we will use rockyou.txt which is saved on THM attackbox by default and located in `/usr/share/wordlists/rockyou.txt`

Run: `hashcat -m 1800 myhash.txt /usr/share/wordlists/rockyou.txt`

```
$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJML9be.cfi3/qxIf.hsGpS41
BqMhSrHVXgMpdjS6xeKZAs02.:waka99

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: $6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPM...ZAs02.
Time.Started.....: Fri Sep 29 20:28:51 2023 (0 secs)
Time.Estimated...: Fri Sep 29 20:28:51 2023 (0 secs)
Guess.Base.....: File (rockyou2.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 168 H/s (1.07ms) @ Accel:8 Loops:1024 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4096-5000
Candidates.#1...: waka99 -> waka99
```

Answer: waka99

Question 4:

Hash: e5d8870e5bdd26602cab8dbe07a942c8669e56d6

Salt: tryhackme

We can also use hash analyzer tool to identify the hash type: <https://www.tunnelsup.com/hash-analyzer/>

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Analyze

Hash:	e5d8870e5bdd26602cab8dbe07a942c8669e56d6
Salt:	Not Found
Hash type:	SHA1 (or SHA 128)
Bit length:	160
Character length:	40
Character type:	hexadecimal

Hash type is SHA128, and on hashcat we can find the mod for salted SHA1 which is 110

100	SHA1
110	sha1(\$pass.\$salt)
120	sha1(\$salt.\$pass)

And after copying our hash to another file named myhash2.txt, we run the command `hashcat -m 110 myhash2.txt /usr/share/wordlists/rockyou.txt` as before.

Answer: `hashcat -m 110 myhash2.txt /usr/share/wordlists/rockyou.txt`