

---

Subject: Re: how can i turn my serial hash back into a serial?

Posted by [danpaul88](#) on Wed, 09 Mar 2011 14:14:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

halo2pac wrote on Wed, 09 March 2011 01:36 Actually you can bruteforce a 12 digit md5 hash in a few dats time on a i7. and if you have applications that run cross network aka slave server bruteforcers you can crack that with a hundred computers in a couple days.

Except a renegade serial is 20 digits and who said it was an MD5 hash? For all we know it could be SHA-1, or double MD5 or even a combination of different hashes ran one after the other.

Also, in order to brute force something you need a method to programatically determine if the input which produced the required hash was ACTUALLY the original input. Since multiple inputs produced the same hash you can easily wind up 'brute forcing' completely the wrong value unless you have some way to validate the result.

---