Subject: Re: how can i turn my serial hash back into a serial?
Posted by Olaf van der Spek on Sat, 19 Mar 2011 23:54:29 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Wed, 09 March 2011 15:14
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.
It's 22 digits of which 4 can be calculated. That's 10^18 or about 2^60 combinations.
Finding out the used hash algorithm itself isn't the hard part.

60 bits might be a bit too much for existing rainbow based attacks.