

---

Subject: Renguard obtains serial?

Posted by [Crimson](#) on Fri, 23 Apr 2004 18:57:22 GMT

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

---

A one-way hash is like a door that only locks from the inside with no keyhole on the other side. It can't be reversed to your actual serial. The advantage, however, is that your serial will always hash to the same value, which is why this sort of encryption is used for comparison purposes.

Let's say you have a serial:

102931379147924 (fake, obviously)

It may hash to something like:

3b44fac8

Now I could try every possible serial until I found one that hashed to the same value, but if I'm going to do that, I might as well just try to log into WOL with those serials I'm trying, then I'll be able to log in from a variety of valid serials instead of just trying to find yours.

Another example... you could have a 5.6 MB mp3 of some song you like. It may hash to something like "9b773ef3". How can you POSSIBLY reverse this short string of letters to a 5.6 MB file? It's used for comparison. In a perfect world, if your favorite band had two versions of a song and you had one, you could use this hash to compare whether the version you're going to download is the same or a different mix because the hash won't match.

Make sense? (credits to Blazer for some of these examples used earlier)

And another thing, **YOU WILL NOT BE BANNED FROM RENGUARD IF WE DON'T LIKE YOU.** Banning is very strictly reserved for those who are a threat to the network. An example would be someone who was repeatedly caught by our intrusion detection code as attempting to bypass RenGuard... or someone who successfully got past it and didn't tell us how. Basically people that you shouldn't want on your server anyway.

---