

Re: Revert MD4

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg05537.html>

- *From:* Federico Bertola <federico.bertola.job@xxxxxxxxxx>
 - *Date:* Mon, 29 Oct 2007 17:52:34 EDT
-

2^{128} (you write this right?) are teorically possibles COLLISIONS that means that a file has the same hash value as the original but with a infinite range of length.

For example a file of 3 Mb may have a collision in a 300 Kb file as in a 2 Tb file!!!

If I close the range of possibilities fixing the length I can find (at leas one if the length is the same as the original) very fewer collisions!

I mean a MD4 in a not-so-hostile environment where you have some information about the original file.

.