
Subject: Re: IGAL encrypted folder
Posted by [Xemuth](#) on Thu, 31 Dec 2020 10:02:02 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello idkfa46,

My knowledge about this kind of software is extremely limited so don't take my word for truth !

In my opinion it won't really help you.

To crack this kind of software you need the algorithm used to encrypt. In your case, if you know the algorithm you can still try to create a quick program that decrypts your file with a random key then if the hash of your file matches with the original one then you have the decryption key. On paper this way of working will always work but in reality if IGAL uses an encryption algorithm based on a key with a minimum size of 256 bits then it's gonna be impossible to find the decryption key by using brute forcing.

Quote: Even if you use Tianhe-2 (MilkyWay-2), the fastest supercomputer in the world, it will take millions of years to crack 256-bit AES encryption.

Again, I'm far from being an expert and my knowledge is highly limited.
