

Forum:[Hack Forums](#)

Thread: [Length of Time to Brute Force?](#)

drew5494 - March 8, 2015, 7:35 pm

Hello just wondering how long it would take to brute force my encrypted HD knowing the password is 12 characters and also knowing it is made up of a word followed by a number and a word again. The key was picked with Apples Password Helper under Memorable.

Key Examples:

sneak57]bask

Laura90(irks

maul6&Dothan

HBO19_Astrid

Its encrypted with Filevault which uses XTS AES 128.

Any other solutions that you guys can recommend would be very helpful.

Thank you.

chick3nman - March 8, 2015, 8:08 pm

It would take millions and millions of years unless you got super super lucky and managed to nail the "word(randomx3)word" system. That's the best vector for key guessing and still boils down to years and years.

drew5494 - March 8, 2015, 8:29 pm

(Mar 8, 2015 08:08 PM)chick3nman Wrote: [\[CITE\]](#) It would take millions and millions of years unless you got super super lucky and managed to nail the "word(randomx3)word" system. That's the best vector for key guessing and still boils down to years and years. Hey again lol

Years is fine with me.

So do you have any idea how I can retrieve the hash at all from the HD even if it doesn't help its still worth trying.

Im bringing the HD to a hacker tomorrow who can apparently "hack into banks" according to my friend. Hopefully he can do something.

chick3nman - March 8, 2015, 8:35 pm

(Mar 8, 2015 08:29 PM)drew5494 Wrote: [\[CITE\]](#) Hey again lol

Years is fine with me.

So do you have any idea how I can retrieve the hash at all from the HD even if it doesn't help its still worth trying.

Im bringing the HD to a hacker tomorrow who can apparently "hack into banks" according to my friend. Hopefully he can do something.

Not to really burst your bubble here, but I highly doubt he will be able to retrieve the hash. I have found 0 documentation on where the hash and key information is stored. I would be careful with letting anyone tamper with the drive without do a complete disk image backup.

drew5494 - March 8, 2015, 8:36 pm

(Mar 8, 2015 08:35 PM)chick3nman Wrote: [\[CITE\]](#) Not to really burst your bubble here, but I highly doubt he will be able to retrieve the hash. I have found 0 documentation on where the hash and key information is stored. I would be careful with letting anyone tamper with the drive without do a

complete disk image backup.

Do you by any chance know how I can backup the disk image?

Thanks.

Minato Namikaze - March 8, 2015, 8:37 pm

I want to pick "Yes surely it can be cracked" because it can.

It will only take a hell of a long time I would think haha

chick3nman - March 8, 2015, 8:38 pm

(Mar 8, 2015 08:36 PM)drew5494 Wrote: [\[CITE\]](#) Do you by any chance know how I can backup the disk image?

Thanks.

There are PLENTY of services for that. That's a huge thing among data recovery companies. They may not be able to decrypt the data, but I'd be willing to bet all of them can clone your disk onto a second drive perfectly. I'm pretty sure even BestBuy offers(or used to offer) this service.

drew5494 - March 8, 2015, 8:43 pm

(Mar 8, 2015 08:38 PM)chick3nman Wrote: [\[CITE\]](#) There are PLENTY of services for that. That's a huge thing among data recovery companies. They may not be able to decrypt the data, but I'd be willing to bet all of them can clone your disk onto a second drive perfectly. I'm pretty sure even BestBuy offers(or used to offer) this service.

Mm ok thanks ;) Remember that software called passware I mentioned a while back. They have a disk decryption service you can send them an encrypted dapple DMG and they will do their best to decrypt it.

Maybe if I can find a way to extract it I have a slim chance.

(Mar 8, 2015 08:37 PM)Minato Namikaze Wrote: [\[CITE\]](#) I want to pick "Yes surely it can be cracked" because it can.

It will only take a hell of a long time I would think haha

Lol funny bra a long time is ok with me as long as Im not dead by the time it finishes.