

Forum:[Hack Forums](#)

Thread: [Find RAR password, Does Knowing Contain files Help?](#)

Digiraite - November 27, 2019, 1:46 am

Hello, I found an old & small RAR file with unknown password. It contains a single PNG file (5473 Byte)(5.4 KB)

I have a vague Idea of what that image might be and it's nothing important. still I want to try to find the password

I remember the password was short like 5-8, But I don't trust my memory that much

I tried many methods for Brutal force attack and didn't get it. password might even contain Arabic characters

now I can ask my question

I know that this file contains a single PNG file that starts with a known signature and Winrar probably used AES. can that help for finding password by a method rather than Brutal-Force Attack. like Plain text.

If it was an unknown type file. it didn't matter.

but can knowing the file type inside an encrypted RAR file. help on cracking it?

I would be happy to hear your comments about it. Thank you

File on G.Drive

drive.google.com/file/d/1PUblVQqBK2XXC_HmGEN-xpuYj5QgBUlf/view?usp=sharing

CryTouch - November 27, 2019, 3:30 am

You may have better luck using a data pack extractor rather than 7zip or winrar directly. Can't remember the data unpacker's name of program I used to use. Its purpose was more for game modding and viewing content of packed and encrypted data or Pak type files but it did work for images in encrypted rar and zip. If some data package viewers don't help you could maybe try with a memory viewer and editor like ollydbg. I believe there are some tutorials online of how to crack a rar password in memory knowing the encrypted algorithm help. As for the brute force method you may be better off using rainbow tables rather than from a password list.

Digiraite - November 27, 2019, 5:16 am

(Nov 27, 2019 04:30 AM)CryTouch wrote: [\[CITE\]](#) You may have better luck using a data pack extractor rather than 7zip or winrar directly. Can't remember the data unpacker's name of program I used to use. Its purpose was more for game modding and viewing content of packed and encrypted data or Pak type files but it did work for images in encrypted rar and zip. If some data package viewers don't help you could maybe try with a memory viewer and editor like ollydbg. I believe there are some tutorials online of how to crack a rar password in memory knowing the encrypted algorithm help. As for the brute force method you may be better off using rainbow tables rather than from a password list.

I'll be Grateful if you tell the name of that data pack extractor if you happen to remember it. thanks

4Txe4y33C9zvNhMj - November 27, 2019, 5:33 am

Good afternoon,

you could use zip2john or rar2john to get the file hash. Just crack it using johntheripper afterwards.

Best regards,
4Txe4y33C9zvNhMj

Digiraite - November 28, 2019, 2:15 am

(Nov 27, 2019 06:33 AM)4Txe4y33C9zvNhMj Wrote: [\[CITE\]](#) you could use zip2john or rar2john to get the file hash. Just crack it using johntheripper afterwards.

I first thought that name is a joke. But that's another Brutal Force Attack Software that I rather avoid for the reasons I explain in next post. still, Thanks for your useful info

Noodlez_ - November 28, 2019, 2:32 am

(Nov 28, 2019 03:15 AM)Digiraite Wrote: [\[CITE\]](#) I first thought that name is a joke. But that's another Brutal Force Attack Software that I rather avoid for the reasons I explain in next post. still, Thanks for your useful info

From what I understood, the files are encrypted with the password either way. So there wouldn't be any use in extracting the files.

Digiraite - November 28, 2019, 2:46 pm

I Give up on Cracking this file for the reasons I'm going to tell you one by one. still, since you was so kind to me to give me some information, I try my best to give you some information as well.

What was that File?

Probably (Email Password) or (Credit Card Information) that I Create a PNG from them by Windows Snip Tool to make it unsearchable (Explain the Size and Format of Image) and then Encrypt it (with what I assume a Strong Long Password that what not going to be easy to Crack in a weekend). those Data are not for now important since they are out of Data. so I don't give myself more trouble for those.

AES is Strong!

I tried to Crack this file in hope for some vulnerability or some Bugs that help me crack it fast. But AES is so strong. maybe a SuperComputer be able to Crack such tiny file. But that just show How Hard it is to crack Bigger ones. so I strictly learned that I can trust AES, But I shall not forget my passwords.

(Rainbow Tables) NotGoing to work

Based on an Answer, Rainbow is good for unSlated Hashes which RAR is a Salt Hash
stackoverflow.com/questions/3817941/rar-passwords-why-dont-rainbow-tables-work

RAR 3.x is Safer

Based on what this site says, RAR 3.x is Harder to Crack (Which is Mine) and Cracking a RAR 5.x is much easier.

passcovery.com/helpdesk/knowledgebase.php?article=35

Knowing Content won't help

I was hoping that Knowing content help to give a clue about how to Crack it. But I created several RAR file with and without PNG and without any password.

It seems the first thing Compression do is messing up the first lines of PNG file. the Data is first Compressed and then Encrypted.

But if you have the Exact non Encrypted File or one file inside RAR. that might Help. But I'm not sure

In Conterary, If the Header of file was Encrypted and didn't let me see list of file insides. It was Easier to Crack.

if when you're trying to open RAR archive you're getting "Enter the password" message immediately — without seeing even contents of archive — then it means "header encryption" was used. And for password recovery process it's better because we don't need to unpack whole file, just check several bytes within decrypted header.

passcovery.com/helpdesk/knowledgebase.php?article=3

Thank you all for your Answers. I hope my information was a little helpful to you guys as well