Zip-Bomb Attack

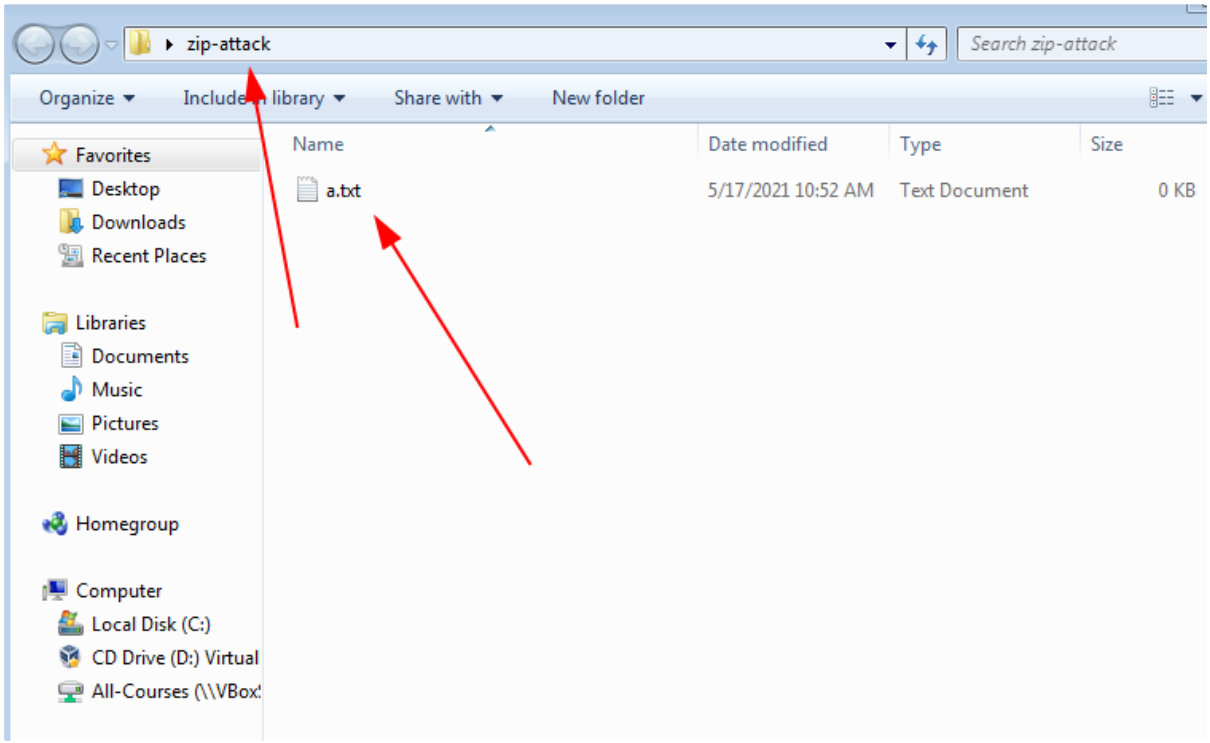
Learn about Zip Bomb attack - Theory + Practically - Both in Windows + Linux

A zip bomb, also known as a Zip of Death, is a malicious archive file designed to crash or render useless the program or Create a Zip Bomb - Zip of Deathsystem reading it.

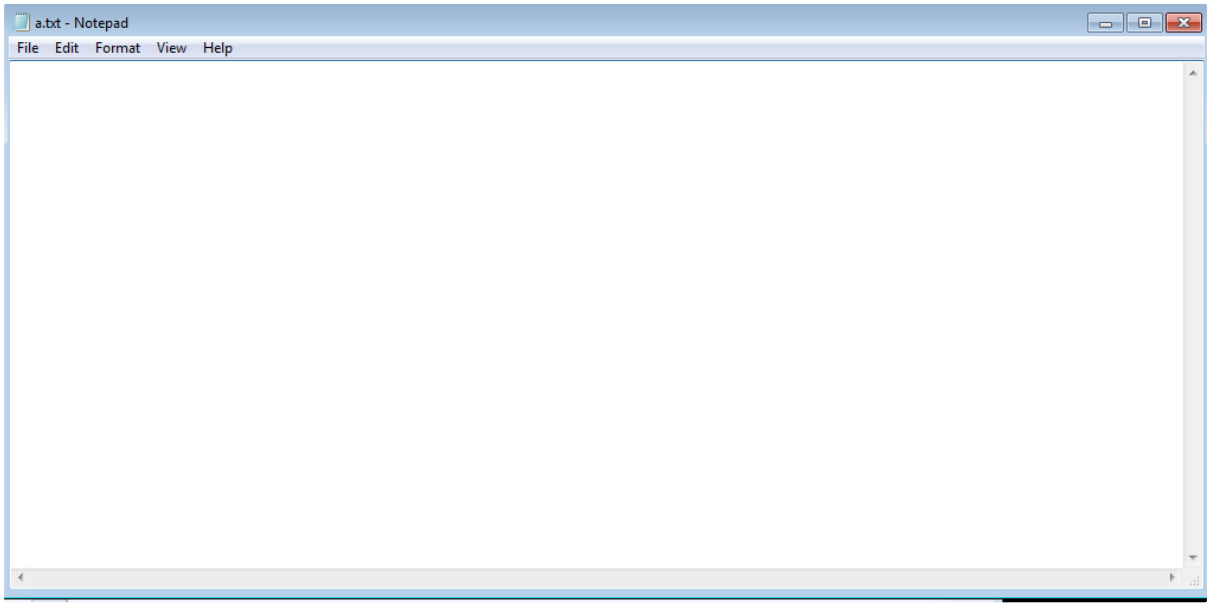
- Virus creater use this attack : to **disable antivirus**
  - after disable antivirus, hacker send more **virus** to get into system undetected
- A zip bomb is usually a small file (up to a few hundred kilobytes) for ease of transport and to avoid suspicion.
- **However, when the file is unpacked its contents are more than the system can handle**
- You can make your own zip bomb to annoy your friends or just out of curiosity (or wilderness) to experiment with it.
- BUT ⇒ **Make sure you don't open it in your end or in your computer**

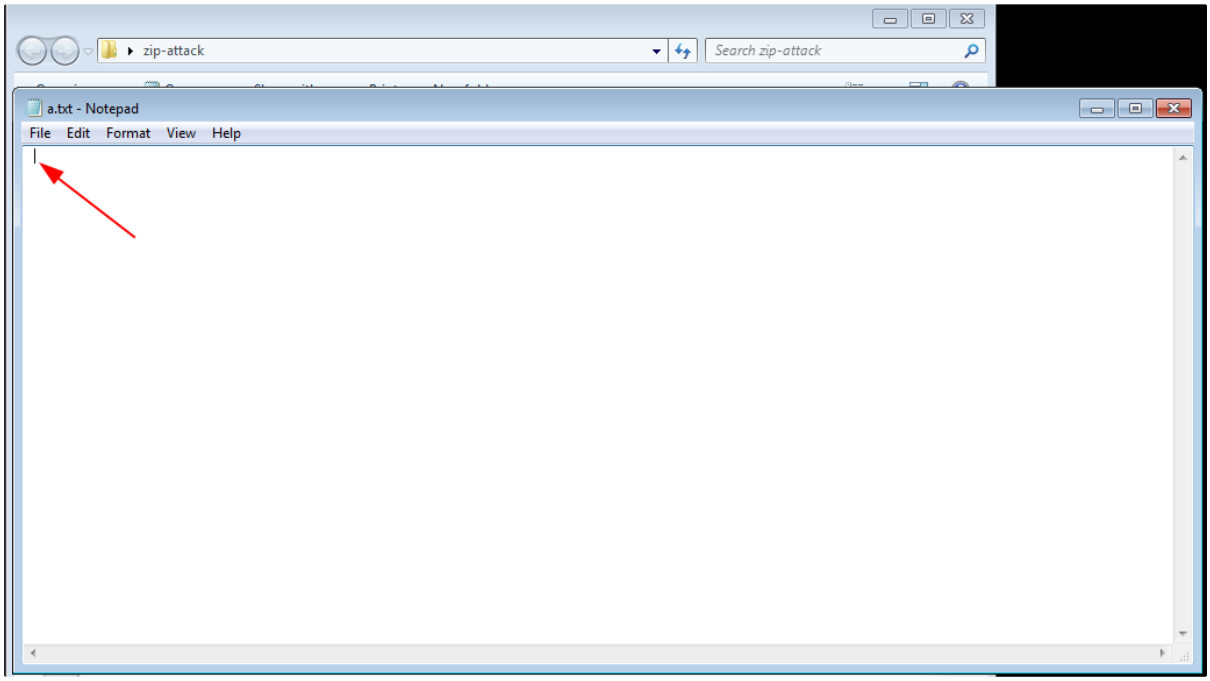
Enough talking, Let's now learn to make your own Zip of Death - Practically

- Step 1 ⇒ Create a new text file,name it a.txt



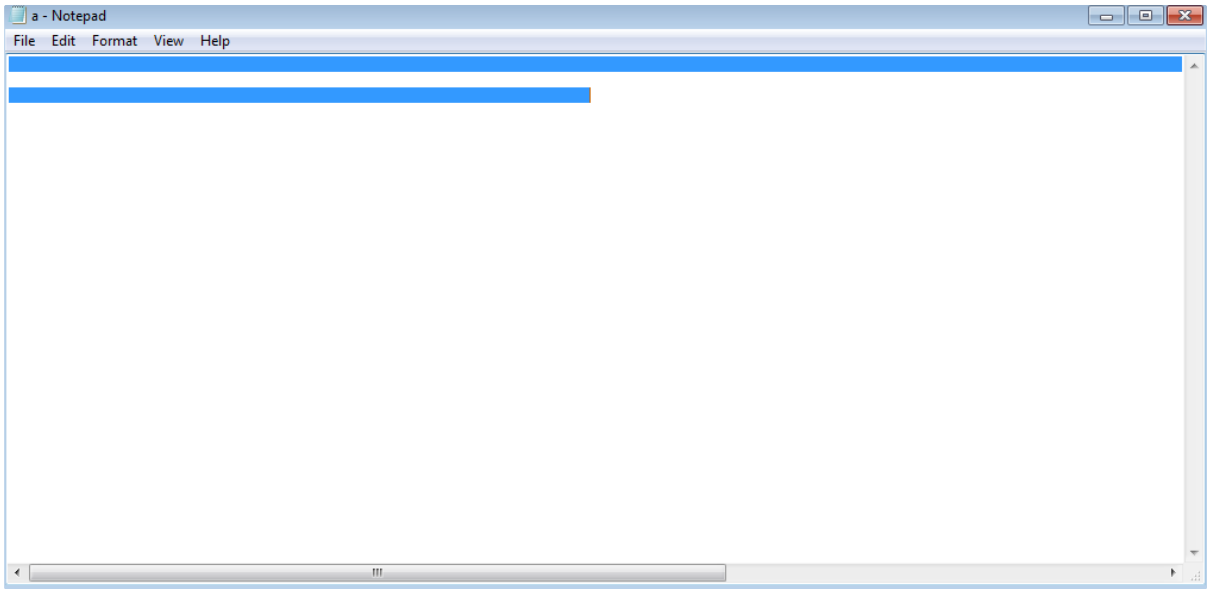
- Step 2 ⇒ Open and type the null character (alt + 255) in it. - blank space



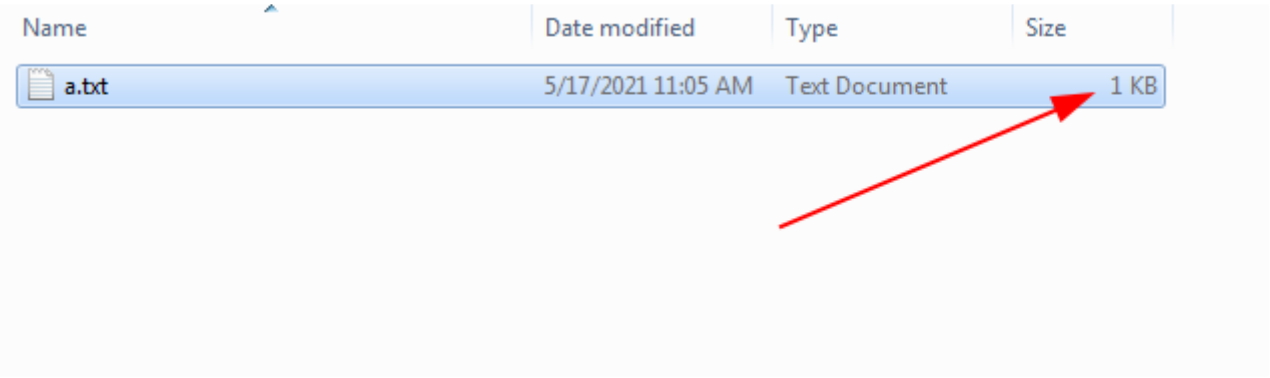


Notice - cursor place → that is blank space by using Alt+255

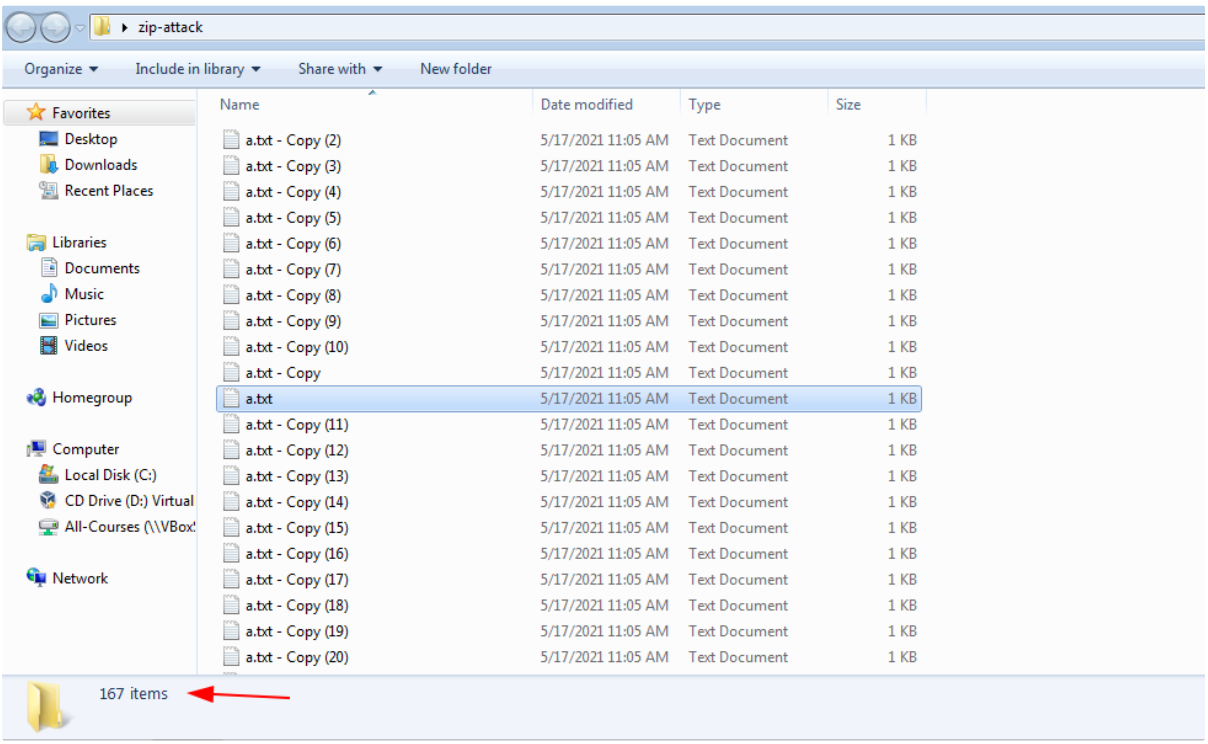
Add more spaces like below using SPACE



- Step 3 - Save it → Notice size is now 1 KB

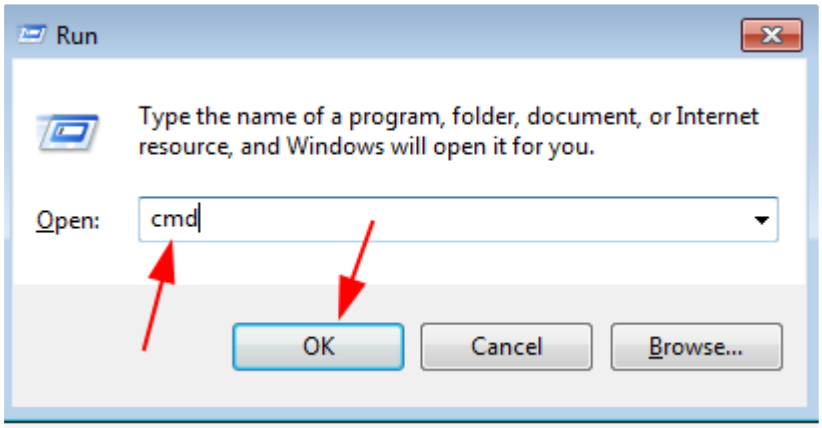


- Step 4 - Now, make copies of this text file. Make as much copies as you can. For example, I have created more then 100 copies of same file.



- Step 4 -

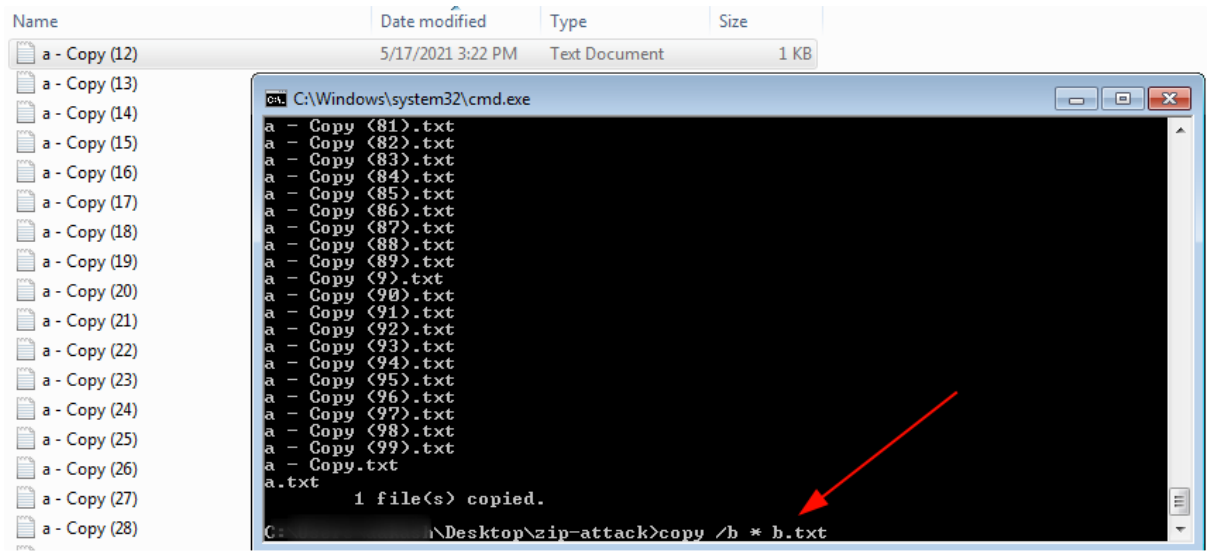
We will now copy content of all these small files into one file. For that we are going to use Command Prompt. To open Command Prompt, press **Windows Key + R**, type **cmd** and press Enter.



- Step 5 -

In CMD, Navigate to the folder where you have saved your text files and it's copies. For Example, my Zip Bomb directory in on Desktop, so I can navigate to it using following command.

- Step 6 - Once you are in that directory, type following command to copy content of all text files, into single text file.



Explanation ⇒

> copy ⇒ Used to copy files or folders
>
> /b ⇒ Used to copy binary content of files
>
> .txt ⇒ Copies all text files of current directory
>
> b.txt ⇒ Copy all the content in a new file with name b.txt

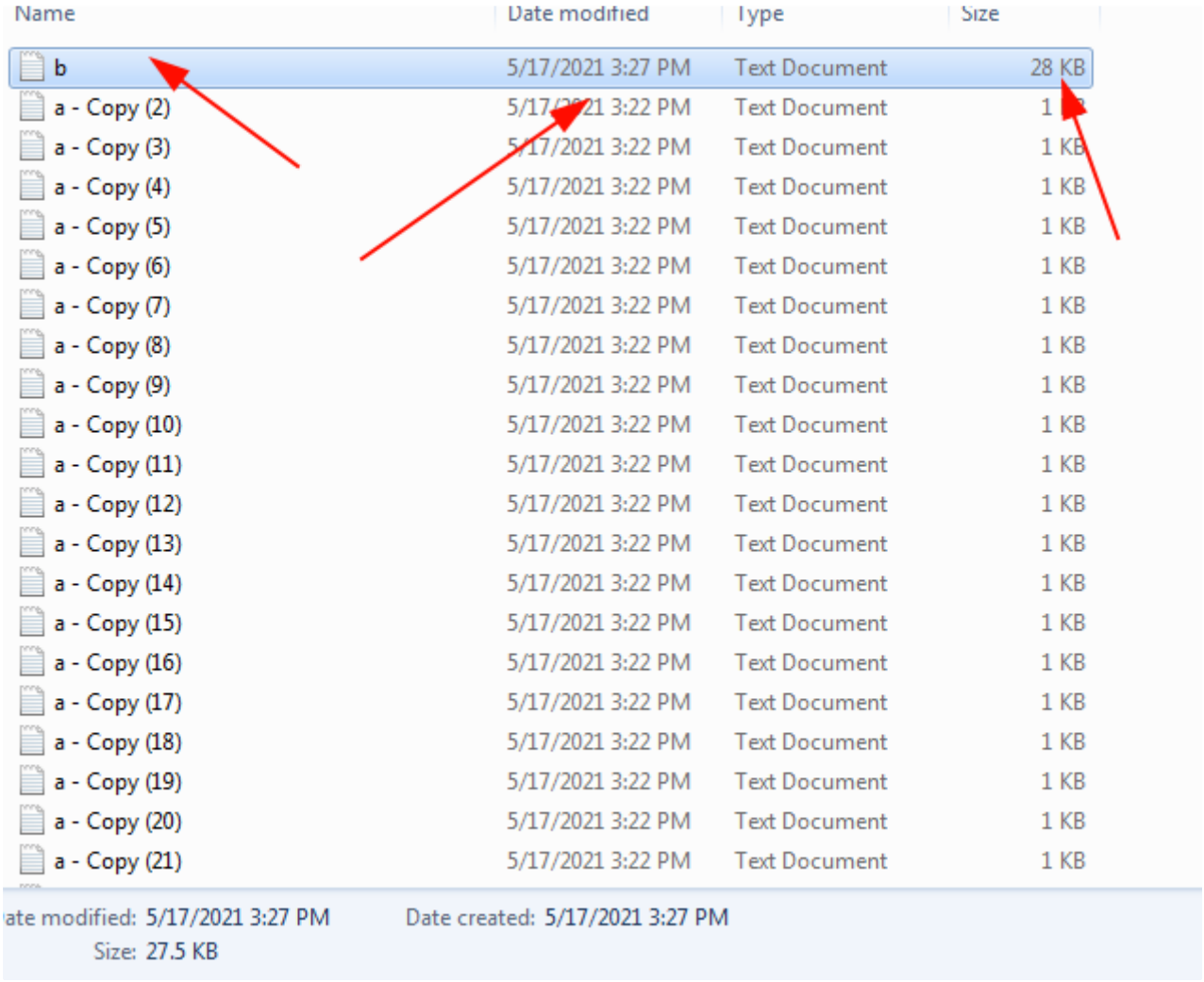
You see ⇒ **1 file<s> copied.** ⇒ This come once we above command

- Step 7 -

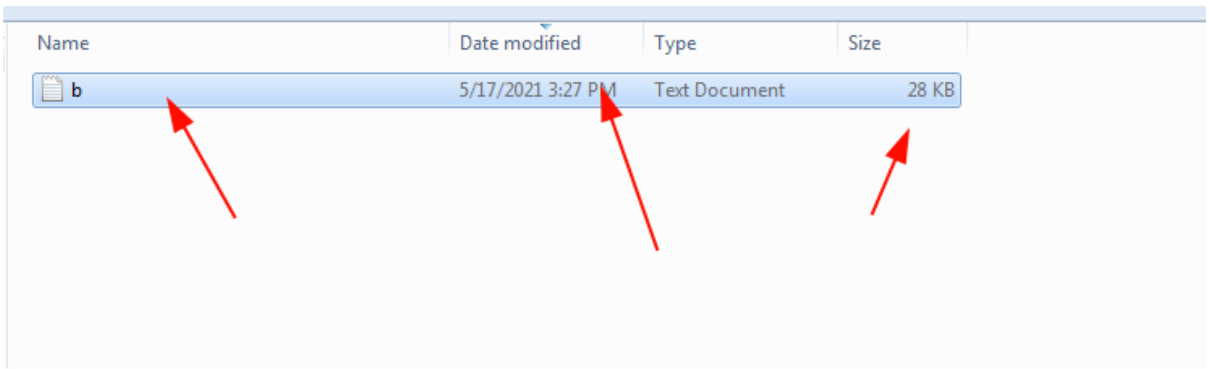
Now, minimize CMD, delete all text files except newly created a.txt file.

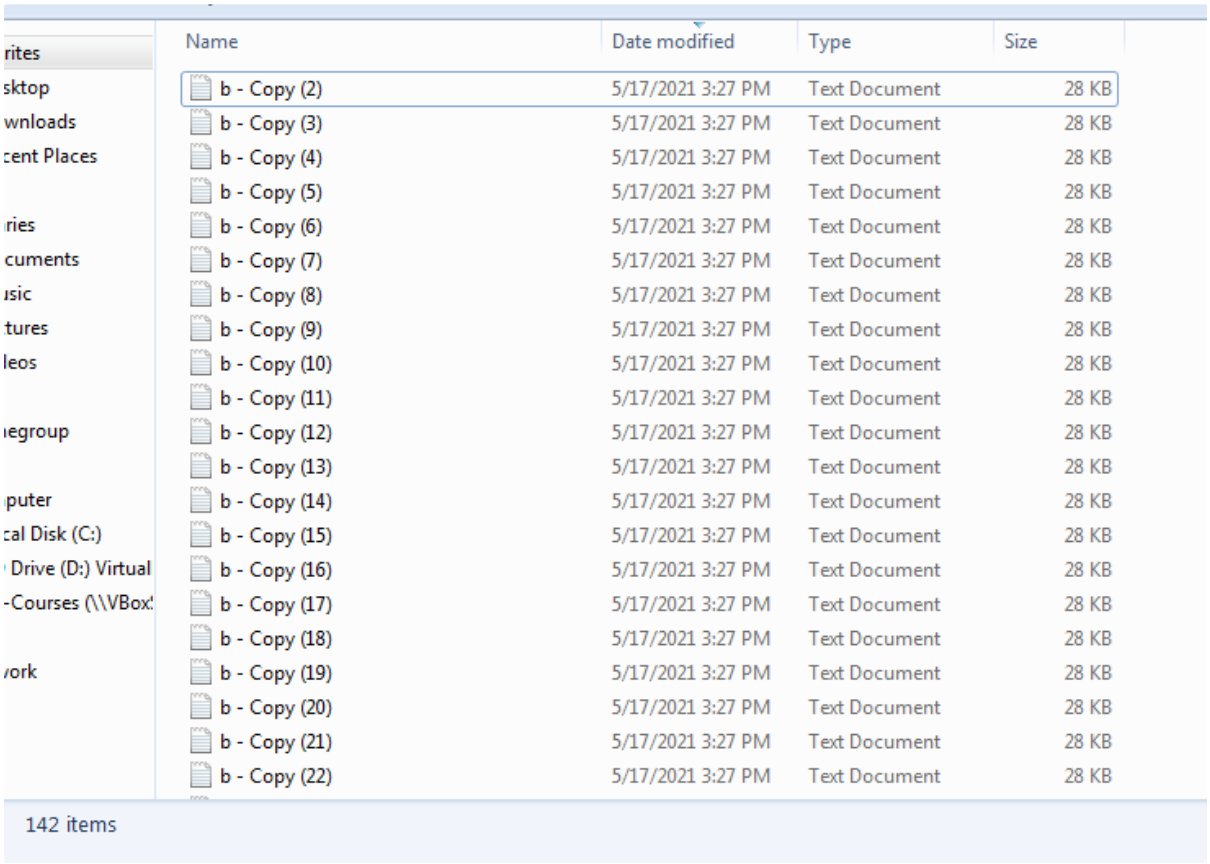
And again make copies of newly created a.txt file and using command prompt copy content of all those files into one file.

Let's say it's named as **c.txt**



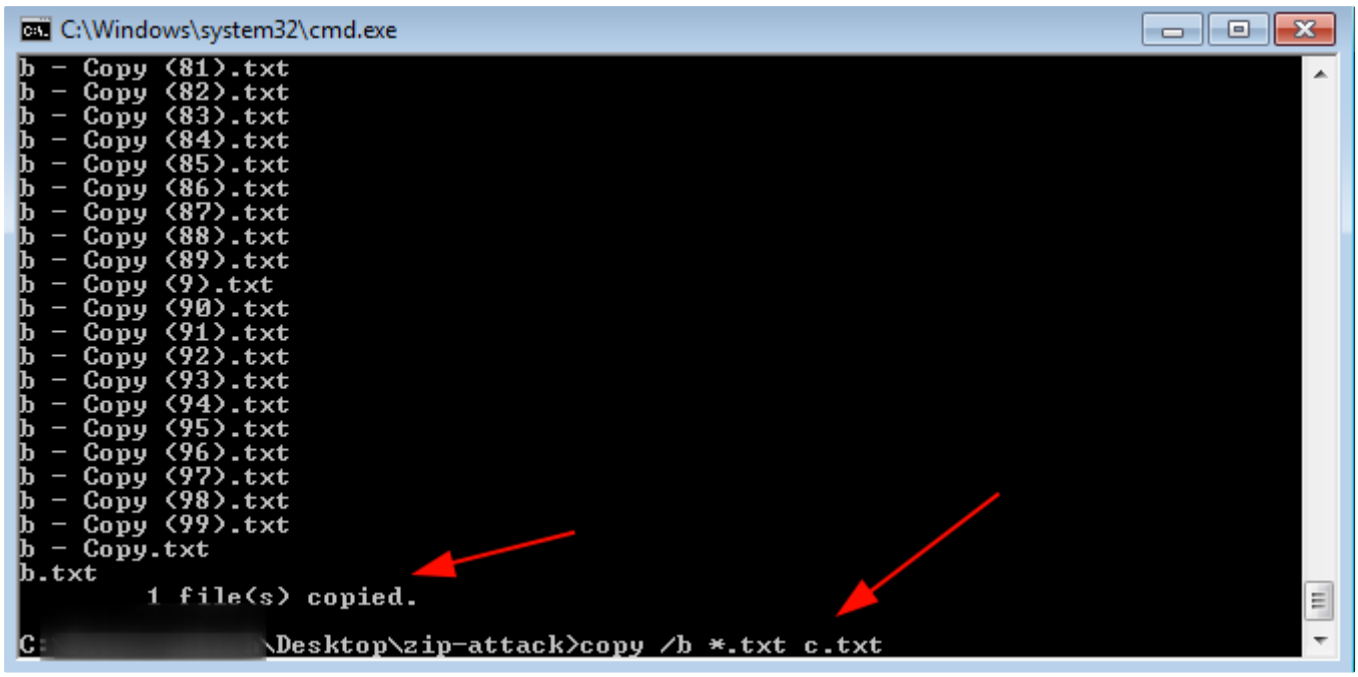
Like above delete all files except the arrow one

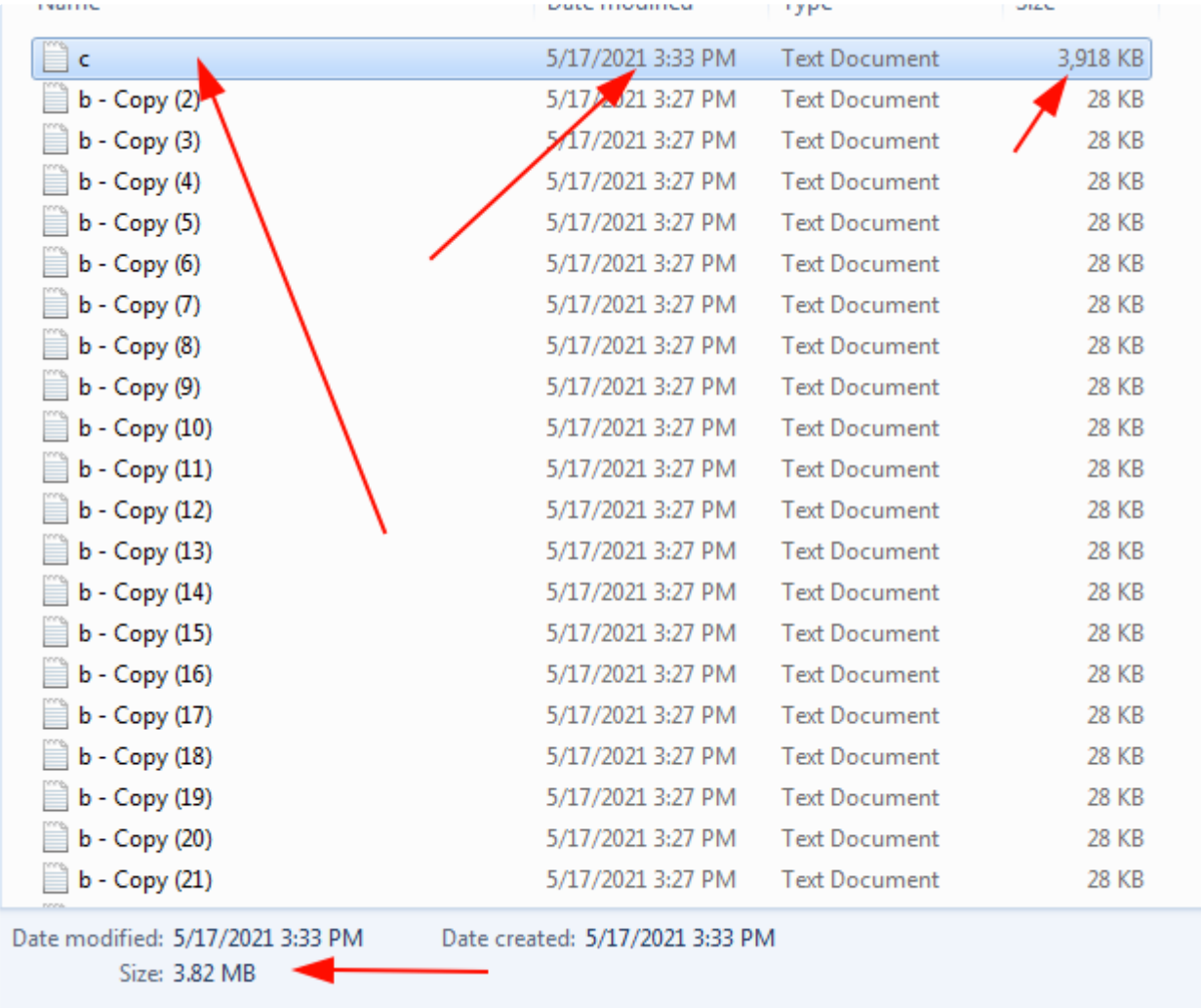




See, we created more txt files.

Again used copy command and this time we make this **c.txt file**



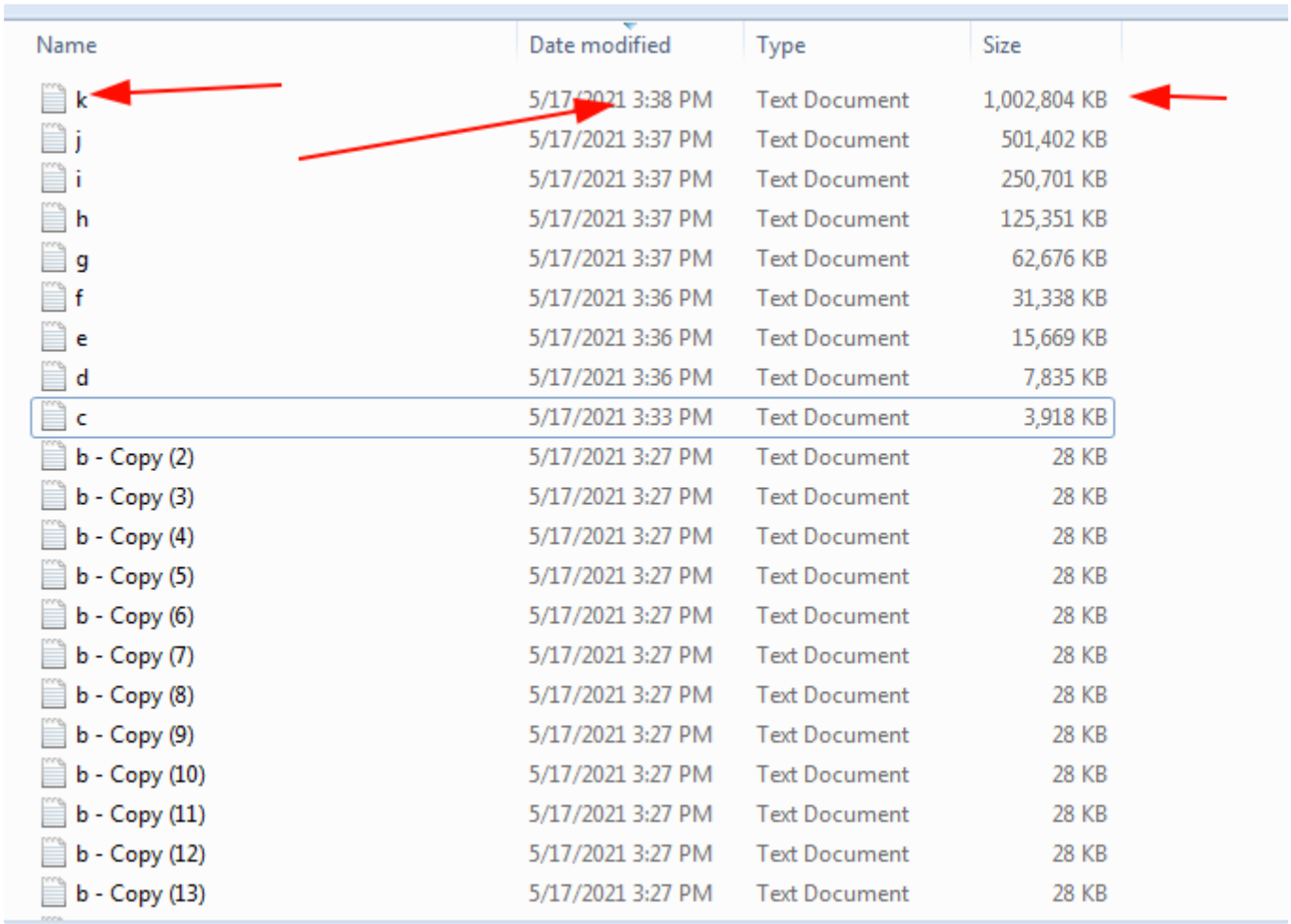


🔥 NOTE ⇒

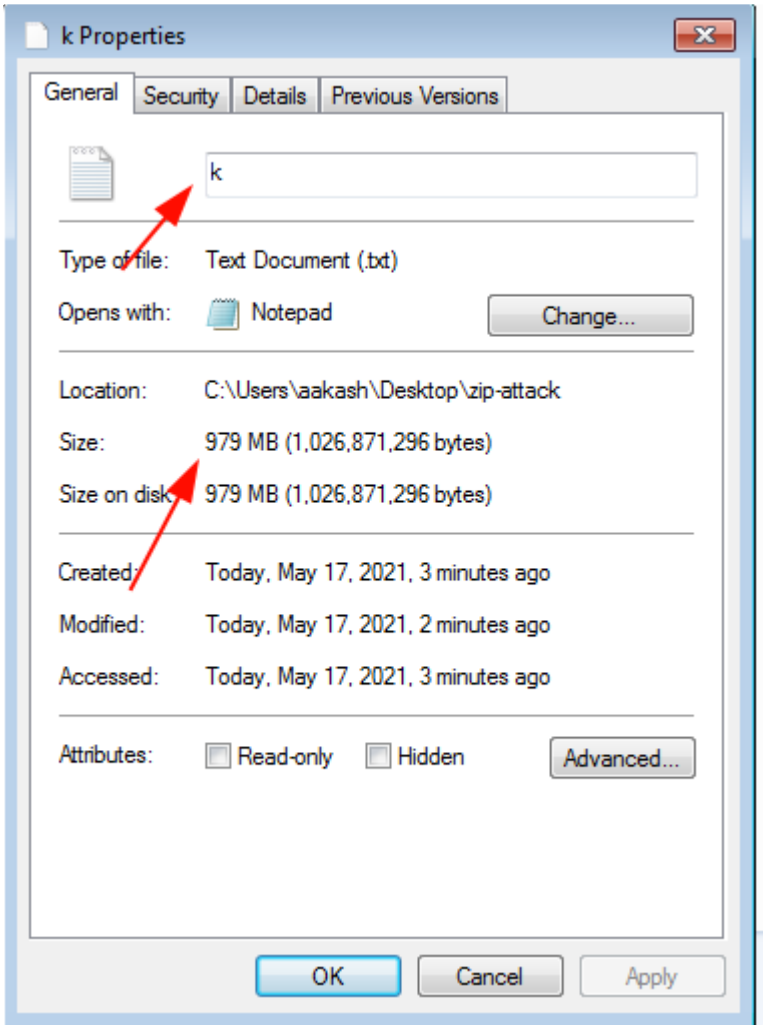
HERE YOU MUST BE CAREFUL! DON'T OPEN THIS TEXT FILE, OTHERWISE YOUR OWN PC MIGHT HANG.

You can make this file even more bigger by repeating this process. YOU MUST NOT OPEN THIS FILE AS IT MAY CRASH YOUR SYSTEM.

Right now file size is 3.82 MB, But, you can make it even more bigger, using above steps as we did already. Let's do this



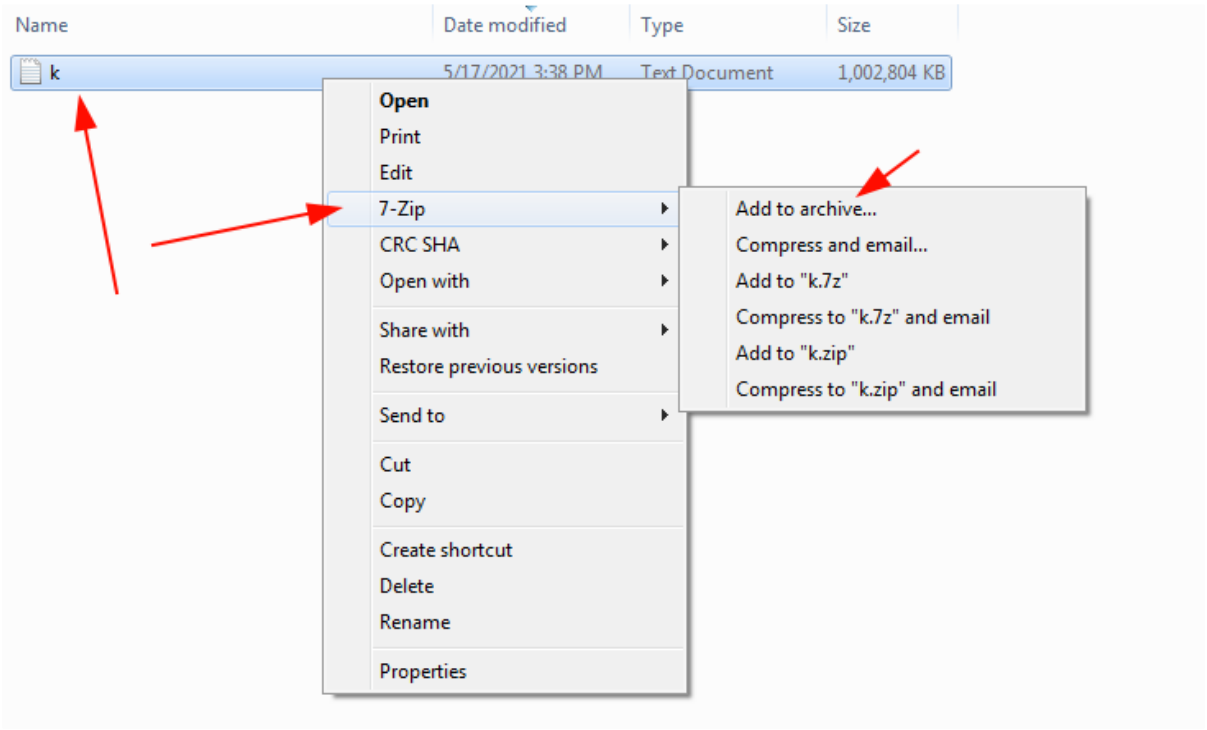
Name	Date modified	Type	Size
k	5/17/2021 3:38 PM	Text Document	1,002,804 KB
j	5/17/2021 3:37 PM	Text Document	501,402 KB
i	5/17/2021 3:37 PM	Text Document	250,701 KB
h	5/17/2021 3:37 PM	Text Document	125,351 KB
g	5/17/2021 3:37 PM	Text Document	62,676 KB
f	5/17/2021 3:36 PM	Text Document	31,338 KB
e	5/17/2021 3:36 PM	Text Document	15,669 KB
d	5/17/2021 3:36 PM	Text Document	7,835 KB
c	5/17/2021 3:33 PM	Text Document	3,918 KB
b - Copy (2)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (3)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (4)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (5)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (6)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (7)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (8)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (9)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (10)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (11)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (12)	5/17/2021 3:27 PM	Text Document	28 KB
b - Copy (13)	5/17/2021 3:27 PM	Text Document	28 KB

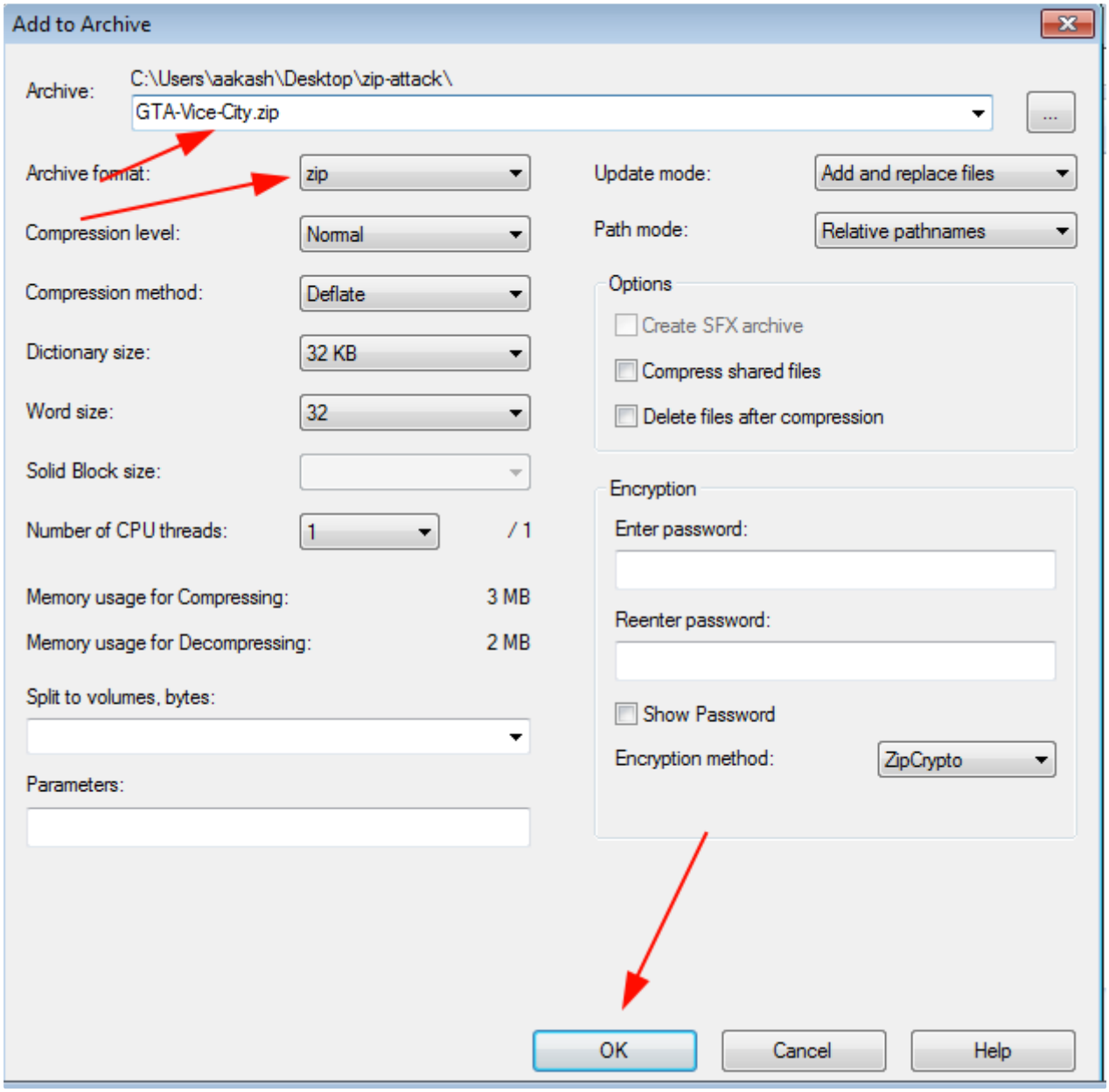


Great, now its size become ⇒ **979 MB**

You can make even larger file if you wish.

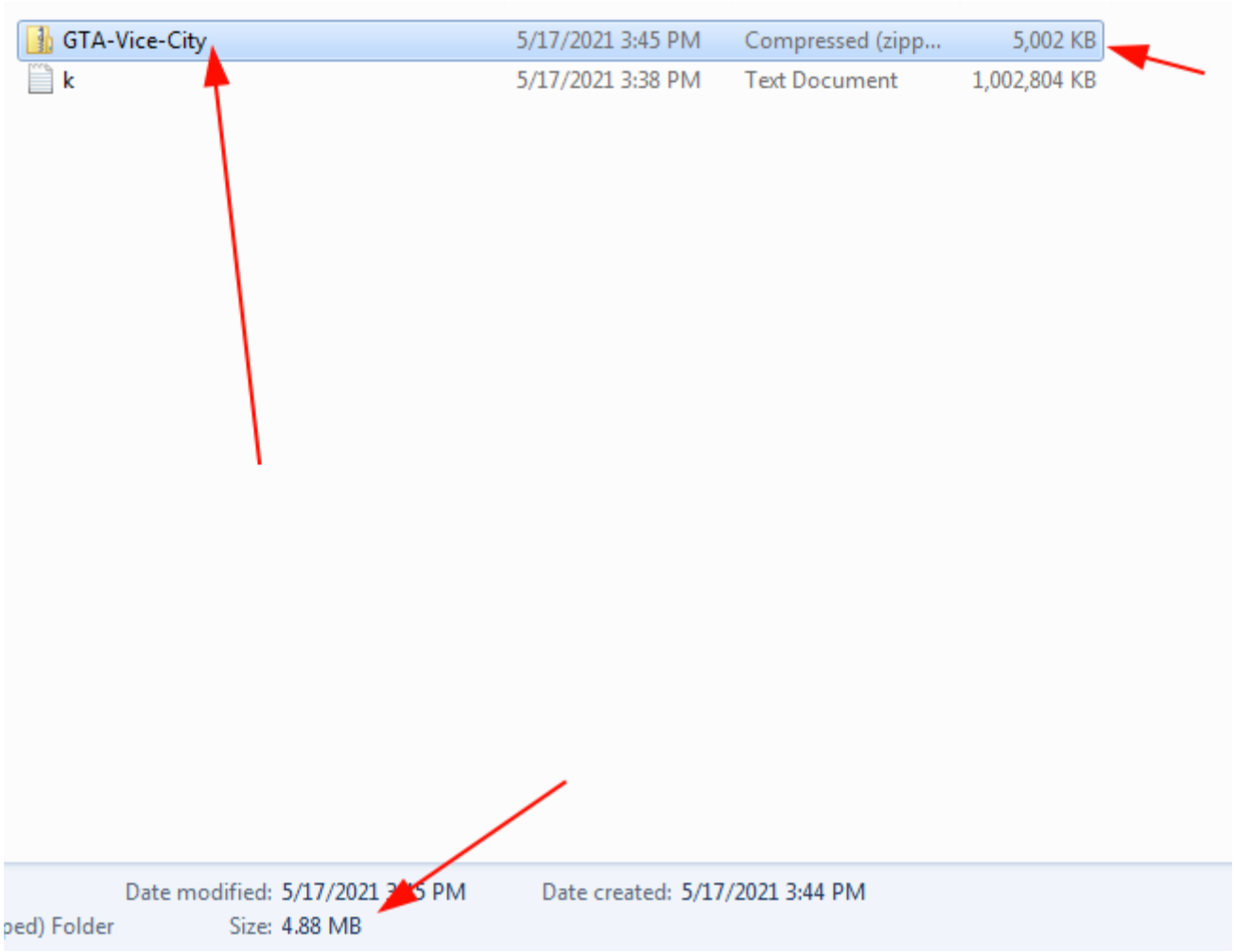
- Step 8 - Time to zip it up. Right-click on k.txt and select **Add to archive...**





Now, check size of newly created zip file, it's amazingly small in size.

You can make size of this archive even more smaller by re-zipping it.



> Now, your Zip Bomb is ready. You must be careful enough not to open it yourself.
>
> You can play prank on your friends. Just send this file to them, in pendrive or by any other means.
>
> You can change the name of text file to some lucrative name that can attract victim to click on it.
>
> Once he clicks on it, it will start extracting and Boom! System will hang and crash!
>
> Be generous to your friends and ask them to save all their work before opening this file.

Practical is Done, But wait, there is one thing more to tell you ⇒ **42.zip**

42.zip ⇒

42.zip is a zip file consisting of 42 kilobytes of compressed data, containing five layers of nested zip files in sets of 16, each bottom-layer archive containing a 4.3-gigabyte (4294967295 bytes; 4 GiB – 1 B) file for a total of 4.5 petabytes (4503599626321920 bytes; 4 PiB – 1 MiB) of uncompressed data

This file is available for download on various websites across the Internet, with much ease for anyone who wants it

In many anti-virus scanners, only a few layers of recursion are performed on archives to help prevent attacks that would cause a buffer overflow, an out-of-memory condition, or exceed an acceptable amount of program execution time.

Zip bombs often (if not always) rely on repetition of identical files to achieve their extreme compression ratios.

Dynamic programming methods can be employed to limit traversal of such files, so that only one file is followed recursively at each level, effectively converting their exponential growth to linear.