

# Cracking old Zip File Passwords with Bkcrack

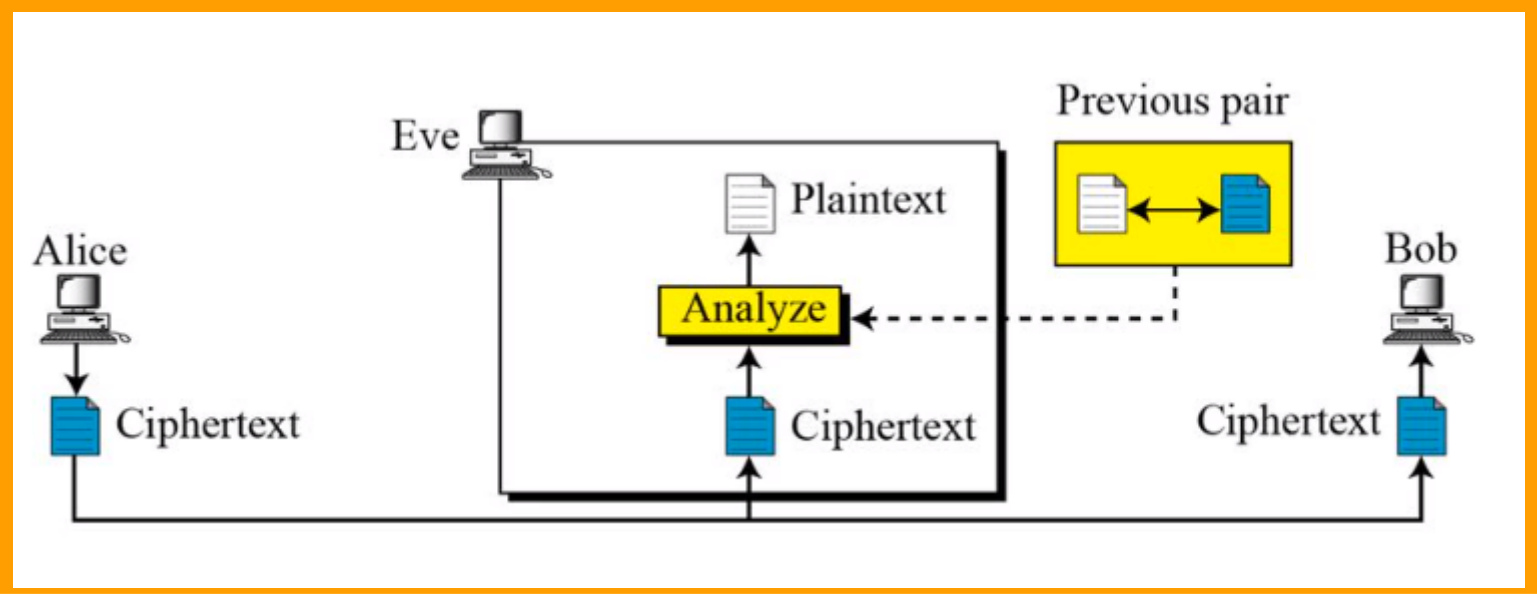
@mmar

# Background

Old Zip Encryption method did not actually encrypt the files and used a method called “store” to save files inside a zip archive. Modern tools like winzip and winrar now use modern methods and you actually have to create this type of archive manually. (But you may come across an old archive created with this type of method)

This is a known plain text attack which means you should know how files look like or what their file content is

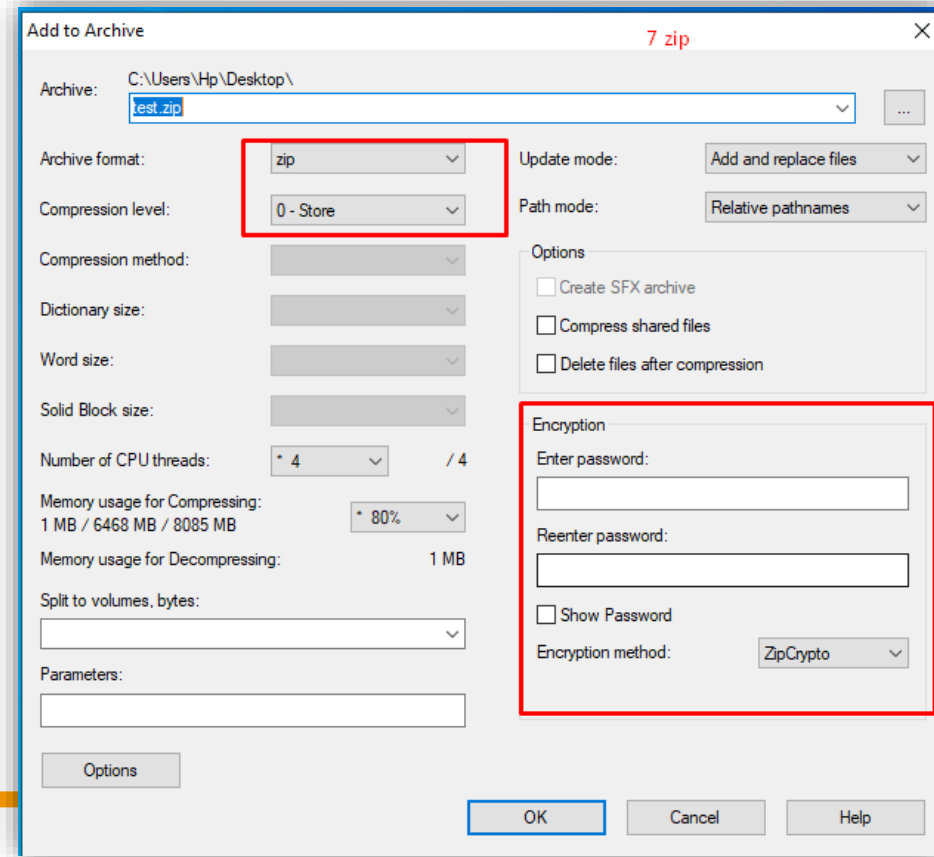
# Known Plain Text Attack



# Creating a Vulnerable Archive

# 7zip Archive

❖ Create an archive with 7zip and set compression level as store

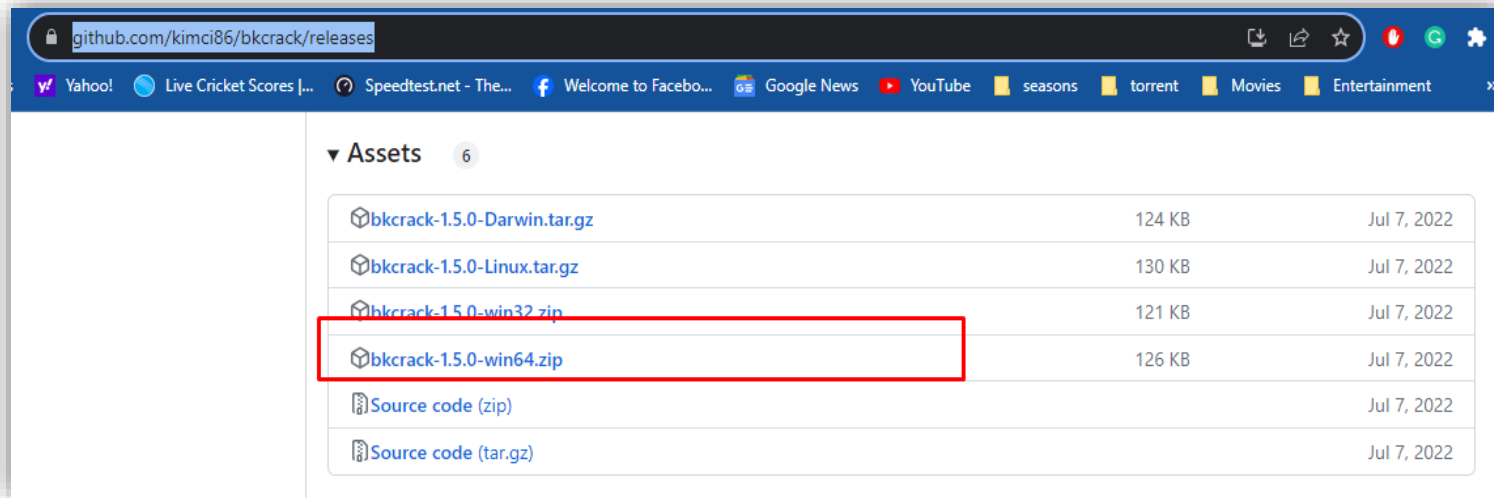


# Breaking the encryption

# Step- 1

- ❖ Download the bkcrack software from github repo

<https://github.com/kimci86/bkcrack/releases>



## Step- 2

- ❖ Copy the archive in the same directory as bkcrack and then use the following command in command prompt to list down the content

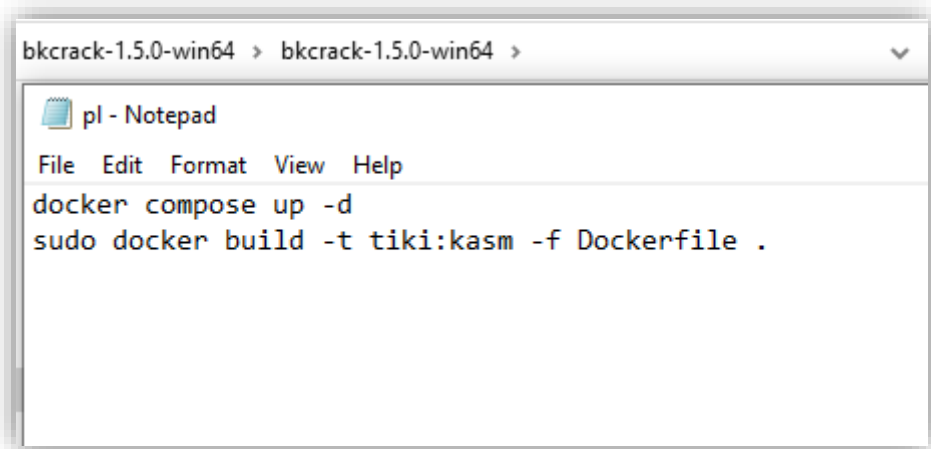
```
bkcrack -L test.zip
```

```
C:\Users\Hp\Desktop\bkcrack-1.5.0-win64\bkcrack-1.5.0-win64>bkcrack.exe -L test.zip
bkcrack 1.5.0 - 2022-07-07
Archive: test.zip
Index Encryption Compression CRC32 Uncompressed Packed size Name
-----
0 ZipCrypto Store d8fefbdf 879 891 test.txt
```



## Step- 3

- ❖ Create a new text file with the content that you know will be present in one of the file

A screenshot of a Notepad window titled "pl - Notepad". The window's title bar shows the path "bkcrack-1.5.0-win64 > bkcrack-1.5.0-win64 >". The text inside the window is:

```
File Edit Format View Help
docker compose up -d
sudo docker build -t tiki:kasm -f Dockerfile .
```

## Step- 4

❖ Now use the following command to recover the key

```
bkcrack -C test.zip -c test.txt -p pl.txt
```

Here :

- test.zip is the encrypted archive
- test is the file you are targeting and have a plain text of
- pl.txt is the plain text file containing some data that you know will be present in the target cipher file

## Step- 4

❖ Now use the following command to recover the key

```
bkcrack -C test.zip -c test.txt -p pl.txt
```

```
C:\Users\Hp\Desktop\bkcrack-1.5.0-win64\bkcrack-1.5.0-win64>bkcrack.exe -C test.zip -c test.txt -p pl.txt
bkcrack 1.5.0 - 2022-07-07
[19:58:44] Z reduction using 13 bytes of known plaintext
100.0 % (13 / 13)
[19:58:44] Attack on 578400 Z values at index 6
Keys: f04945f4 3018d661 edc704a6
9.0 % (52264 / 578400)
[20:01:15] Keys
f04945f4 3018d661 edc704a6
```

## Step- 5

❖ Now we can use the recovered key to extract our files

```
bkcrack -C test.zip -c test.txt -k f04945f4 3018d661 edc704a6 -d decrypt.txt
```

Here :

- decrypt.txt is the output file
- -k flag specifies the recovered key from previous step

## Step- 5

❖ Now we can use the recovered key to extract our files

```
bkcrack -C test.zip -c test.txt -k f04945f4 3018d661 edc704a6 -d decrypt.txt
```

```
C:\Users\Hp\Desktop\bkcrack-1.5.0-win64\bkcrack-1.5.0-win64>bkcrack -C test.zip -c test.txt -k f04945f4 3018d661 edc704a6 -d decrypt.txt
bkcrack 1.5.0 - 2022-07-07
[20:16:44] Writing deciphered data decrypt.txt (maybe compressed)
Wrote deciphered data.
```

# Recovering all files

- ❖ With the key, we can also create a new archive with our own password and then extract all files

```
bkcrack -C test.zip -k f04945f4 3018d661 edc704a6 -U unlocked.zip newpass
```

```
C:\Users\Hp\Desktop\bkcrack-1.5.0-win64\bkcrack-1.5.0-win64>bkcrack -C test.zip -k f04945f4 3018d661 edc704a6 -U unlocked.zip newpass
bkcrack 1.5.0 - 2022-07-07
[20:25:43] Writing unlocked archive unlocked.zip with password "newpass"
100.0 % (1 / 1)
Wrote unlocked archive.
```

DEMO



THANKS