Can a ZIP archive have 2 passwords? Why is that?

Did you know that a ZIP file can have up to 2 correct passwords and both produce the same result when the ZIP file is unzipped?

Password-protected ZIP archives are a popular method for securely compressing and sharing files ranging from sensitive data to malicious code.

However, did you know that a ZIP file can have up to 2 correct passwords and both produce the same result when the ZIP file is unzipped?

Can a ZIP file have two passwords?

Arseniy Sharoglazov, a cybersecurity researcher at Positive Technologies, shared over the weekend a seemingly simple yet magical experiment. In it, he created a password-protected ZIP file named x.zip.

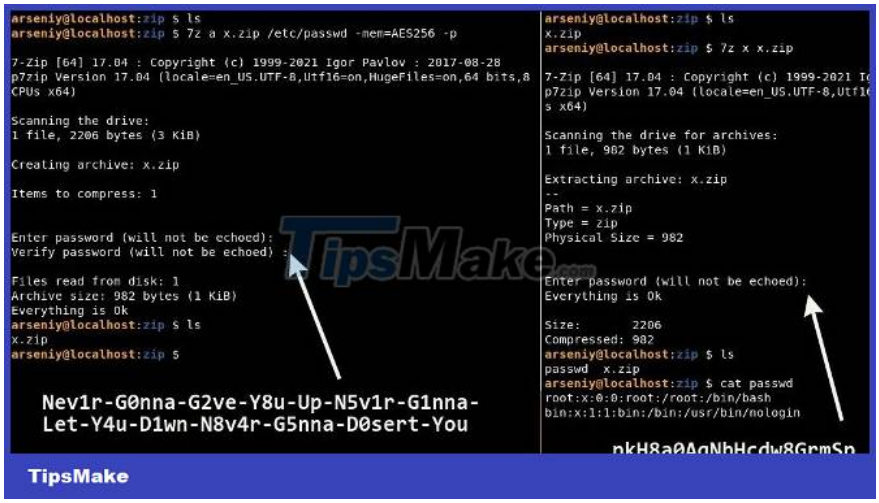
The password that Sharoglazov chose to encrypt the ZIP file was a pun on Rick Astley's 1987 hit Never Gonna Give You Up, which became a popular meme in the tech world:

```
Nev1r-G0nna-G2ve-Y8u-Up-N5v1r-G1nna-Let-Y4u-D1wn-N8v4r-G5nna-D0sert-You
```

But the researcher also proved that when extracting the x.zip file with a completely different password, he did not encounter any errors.

In fact, using a different password allows to successfully extract the ZIP file, the original content is intact:

```
pkH8a0AqNbHcdw8GrmSp
```



How does this happen?

How can Sharoglazov use two passwords for a ZIP file? Twitter user Unblvr explains: When creating a ZIP file with a password with AES-256 mode enabled, the ZIP format uses the PBKDF2 algorithm and hashes the user-supplied password, if the password is too long. . Passwords over 64 bytes (characters) will be too long.

Then, instead of the user's chosen password (in this case "Nev1r-G0nna-G2ve-."), the newly computed hash becomes the actual password of the file.

When the user unzips the file and enters a password longer than 64 bytes ("Nev1r-G0nna-G2ve-."), what the user enters again will be hashed by the ZIP application and compared again with the correct password (the password is now a hash). The comparison results match so the file extraction is successful.

The alternate password used in this case ("pkH8a0AqNbHcdw8GrmSp") is in fact the ASCII representation of the SHA-1 hash of the long password ("Nev1r-G0nna-G2ve-.").

Checksum SHA-1 of "Nev1r-G0nna-G2ve-." = 706b4838613041714e6248636773847726d5370.

This checksum, after being converted to ASCII, will produce: pkH8a0AqNbHcdw8GrmSp.

However, you should keep in mind that when encrypting or decrypting a file, hashing occurs only if the length of the password is greater than 64 characters.

In other words, shorter passwords will not be hashed at both the compression and decompression stages of the ZIP file.

It should be noted, though, that the ASCII representation of the SHA-1 hash of a long password is not always a string of characters and numbers. Sometimes it creates a meaningless set of bytes, which cannot be entered in the password box.

Sharoglazov himself also had to use an open source password recovery tool hashcat with slight modification to find the password with a reasonable ASCII representation. He tried variations of "Nev0r, Nev1r, Nev2r." until he came up with a clean password consisting of only letters and numbers (pkH8a0AqNbHcdw8GrmSp).

For ordinary users, using a ZIP file with a password is guaranteed to be safe. However, this test gives you a glimpse into one of the mysteries surrounding encrypted ZIP files as well as how to get 2 passwords for your ZIP files.