|  |
| --- |
| https://www.onlinehashcrack.com/tools-zip-rar-7z-archive-hash-extractor.php |
| |  | | --- | |  | | $pkzip2$1\*1\*2\*0\*207\*38e\*6d925e42\*0\*2b\*8\*207\*6d92\*aae6\*\*$/pkzip2$ |   **Notes**   * Uploaded files will be deleted immediately. We do **NOT** store your files. * This site is using rar2john and zip2john and 7z2john from JohnTheRipper tools to extract the hash * The goal of this page is to make it very easy to convert your ZIP / RAR / 7zip archive files (.rar, .zip, .7z) to "hashes" which hashcat/john can crack * We can also attempt to recover its password: send your file on our [homepage](https://www.onlinehashcrack.com/index.php)   **How to use?**  More than easy, just select and upload your **ZIP / RAR / 7zip archive file (Max size: 200 Mb)**. The hash will be computed in the "Output" part. ZIP Archive **ZIP Archive hashcat mode is 13600 (WinZip)** and can output 2 formats, which look like:  $zip2$\*0\*3\*0\*b5d2b7bf57ad5e86a55c400509c672bd\*d218\*0\*\*ca3d736d03a34165cfa9\*$/zip2$  or  $pkzip2$2\*1\*1\*0\*8\*24\*8058\*9125\*1b9e7c93b129bd495fe107c89ffbf222bc39303ae92ab534e5cb5013db97bb538945fcb1\*2\*0\*188\*2dc\*33d1d8af\*3c1\*2c\*8\*188\*33d1\*90ed\*.....\*$/pkzip2$::::  **zip2** stands for [AES-256](https://www.winzip.com/aes_info.htm), which provides a stronger encryption. Used in modern zip manager (7-zip, WinZip, etc.)  **pkzip2** stands for ZipCrypto, which is an old/legacy encryption. |

|  |
| --- |
| https://dfir.science/2014/07/how-to-cracking-zip-and-rar-protected.html |
| How-to - Cracking ZIP and RAR protected files with John the Ripper **Updated:** 2014-07-31 3 minute read  After seeing how to [compile John the Ripper to use all your computer's processors](https://DFIR.Science/2014/07/how-to-compiling-john-ripper-to-use-all.html) now we can use it for some tasks that may be useful to digital forensic investigators: getting around passwords. Today we will focus on cracking passwords for ZIP and RAR archive files. Luckily, the JtR community has done most of the hard work for us. For this to work you need to have built the community version of John the Ripper since it has extra utilities for ZIP and RAR files.  For this exercise I have created password protected RAR and ZIP files, that each contain two files.  test.rar: RAR archive data, v1d, os: Unix   test.zip: Zip archive data, at least v1.0 to extract   * The password for the rar file is 'test1234' * the password for the zip file is 'test4321'.   In the 'run' folder of John the Ripper community version (I am using John-1.7.9-jumbo-7), there are two programs called 'zip2john' and 'rar2john'. Run them against their respective file types to extract the password hashes:  ./zip2john ../test.zip > ../zip.hashes ./rar2john ../test.rar > ../rar.hashes  This will give you files that contain the password hashes to be cracked... something like this:  ../test.zip:$pkzip$2\*2\*1\*0\*0\*1b\*a80c\*95e4e9547dcfcde4b8b2f05a80aaeb9d15dd76e7526b81803c8bf7\*2\*0\*1b\*f\*72051312\*0\*44\*0\*1b\*a808\*cbafdd390bf49ea54064ab3ff9f486e6260b9854e37d1ee3a41c54\*$/pkzip$  After, that you can run John the Ripper directly on the password hash files:  ./john ../zip.hashes  You should get a message like: Loaded 1 password hash (PKZIP [32/64]). By using John with no options it will use its default order of cracking modes. See the [examples page](https://www.openwall.com/john/doc/EXAMPLES.shtml) for more information on modes.  Notice, in this case we are not using explicit dictionaries. You could potentially speed the cracking process up if you have an idea what the password may be. If you look at your processor usage, if only one is maxed out, then you did not enable OpenMP when building. If you have a multi-processor system, it will greatly speed up the cracking process.  Now sit back and wait for the cracking to finish. On a 64bit quad-core i7 system, without using GPU, and while doing some other CPU-intensive tasks, the password was cracked in 6.5 hours.  Loaded 1 password hash (PKZIP [32/64])  guesses: 0 time: 0:00:40:29 0.00% (3) c/s: 2278K trying: eDTvw - ekTsl guesses: 0 time: 0:01:25:10 0.00% (3) c/s: 1248K trying: ctshm#ni - ctshfon9 guesses: 0 time: 0:02:56:40 0.00% (3) c/s: 1499K trying: BR489a - BR48jf guesses: 0 time: 0:03:56:04 0.00% (3) c/s: 1703K trying: fjmis5od - fjmidia0 guesses: 0 time: 0:04:46:09 0.00% (3) c/s: 1748K trying: Difg1ek - DifgbpS guesses: 0 time: 0:05:21:22 0.00% (3) c/s: 1855K trying: btkululp - btkulene guesses: 0 time: 0:06:02:43 0.00% (3) c/s: 1857K trying: ghmnymik - ghmnyasd test4321 (../test.zip) guesses: 1 time: 0:06:32:34 DONE (Mon Jul 28 17:50:22 2014) c/s: 1895K trying: telkuwhy – test43ac  Now if you want to see the cracked passwords give john the following arguments:  ./john ../zip.hashes --show  It should output something like:  ../test.zip:test4321  1 password hash cracked, 0 left |