HowTo: Extract Archives [tar|gz|bz2|rar|zip|7z|tbz2|tgz|Z]

Posted on Tuesday December 27th, 2016 (https://www.shellhacks.com/extract-archive-tar-gz-bz2-rar-zip-7z-tbz2-tgz-z/) by admin (https://www.shellhacks.com/author/admin/)

(https://www.shellhacks.com/extract-archive-tar-gz-bz2-rar-zip-7z-tbz2-tgz-z/)

A small note about how to unpack and uncompress the most popular types of archives from the Linux command line.

Unpack [tar|tar.gz|tgz|tar.bz2|tbz2] Files in Linux

Use the following commands to extract **TAR** archives compressed with **GZIP** and **BZIP2**:

```
$ tar xvf file.tar
$ tar xvzf file.tar.gz
$ tar xvzf file.tar.tgz
$ tar xvjf file.tar.bz2
$ tar xvjf file.tar.tbz2
```

Uncompress [zip|rar|bz2|gz|Z|7z] Files in Linux

Use the following commands to uncompress archives or files, compressed with **ZIP**, **GUNZIP**, **RAR**, **BUNZIP2**, **COMPRESS** and **7Z** programs:

```
$ unzip file.zip
$ gunzip file.gz
$ unrar x file.rar
$ bunzip2 file.bz2
$ uncompress file.Z
$ 7z x file.7z
```

Extract Archives with Shell Function

You can create a bash shell function as follows (add to your ~/.bashrc):

```
function extract {
 if [ -z "$1" ]; then
    # display usage if no parameters given
    echo "Usage: extract ."
 else
if [ -f $1 ] ; then
        # NAME=${1%.*}
        # mkdir $NAME && cd $NAME
        case $1 in
          *.tar.bz2) tar xvjf ../$1 ;;
          *.tar.gz) tar xvzf ../$1 ;;
          *.tar.xz) tar xvJf ../$1 ;;
          *.lzma) unlzma ../$1 ;;
          *.bz2) bunzip2 ../$1 ;;
          *.rar) unrar x -ad ../$1 ;;
          *.gz) gunzip ../$1 ;;
          *.tar) tar xvf ../$1 ;;
          *.tbz2) tar xvjf ../$1 ;;
          *.tgz) tar xvzf ../$1 ;;
          *.zip) unzip ../$1 ;;
          *.Z) uncompress ../$1 ;;
          *.7z) 7z x ../$1 ;;
          *.xz) unxz ../$1 ;;
          *.exe) cabextract ../$1 ;;
          *) echo "extract: '$1' - unknown archive method" ;;
        esac

else
echo "$1 - file does not exist"
    fi
fi
}
```

Source: https://github.com/xvoland/Extract (https://github.com/xvoland/Extract)

Reload .bashrc file.

```
$ . ~/.bashrc
```

Now use **extract** command for unpacking and uncompressing the most popular archive types:

```
$ extract file.rar
$ extract file.tar.gz2
$ extract file.7z
```

Comment (1) (https://www.shellhacks.com/extract-archive-tar-gz-bz2-rar-zip-7z-tbz2-tgz-z/#comments)

ONE REPLY TO “HOWTO: EXTRACT ARCHIVES [TAR|GZ|BZ2|RAR|ZIP|7Z|TBZ2|TGZ|Z]”

ALESHKA REPLY

Saturday November 17th, 2018 at 02:03 AM (https://www.shellhacks.com/extract-archive-tar-gz-bz2-rar-zip-7z-tbz2-tgz-z/#comment-7267)

Для zsh

```
function extract {
 if [ -z "$1" ]; then
    # display usage if no parameters given
    echo "Usage: extract ."
 else
if [ -f $1 ] ; then
        # NAME=${1%.*}
        # mkdir $NAME && cd $NAME
        case $1 in
          *.tar.bz2) tar xvjf $1 ;;
          *.tar.gz) tar xvzf $1 ;;
          *.tar.xz) tar xvJf $1 ;;
          *.lzma) unlzma $1 ;;
          *.bz2) bunzip2 $1 ;;
          *.rar) unrar x -ad $1 ;;
          *.gz) gunzip $1 ;;
          *.tar) tar xvf $1 ;;
          *.tbz2) tar xvjf $1 ;;
          *.tgz) tar xvzf $1 ;;
          *.zip) unzip $1 ;;
          *.Z) uncompress $1 ;;
          *.7z) 7z x $1 ;;
          *.xz) unxz $1 ;;
          *.exe) cabextract $1 ;;
          *) echo "extract: '$1' - unknown archive method" ;;
        esac
else
echo "$1 - file does not exist"
    fi
fi
}
```

LEAVE A REPLY

Comment

Name

Email

POST REPLY

‹ CASE STATEMENT IN BASH [EXAMPLE] (HTTPS://WWW.SHELLHACKS.COM/CASE-STATEMENT-BASH-EXAMPLE/)

HOWTO: FIND OUT TOP PROCESSES BY MEMORY USAGE IN LINUX › (HTTPS://WWW.SHELLHACKS.COM/FIND-TOP-PROCESSES-MEMORY-USAGE-LINUX/)

TAGS

ACCESS-CONTROL (HTTPS://WWW.SHELLHACKS.COM/TAG/ACCESS-CONTROL/)

AIRCRACK-NG (HTTPS://WWW.SHELLHACKS.COM/TAG/AIRCRACK-NG/)

ANONYMITY (HTTPS://WWW.SHELLHACKS.COM/TAG/ANONYMITY/)

APACHE (HTTPS://WWW.SHELLHACKS.COM/TAG/APACHE/)

ARCHIVE (HTTPS://WWW.SHELLHACKS.COM/TAG/ARCHIVE/) BASH (HTTPS://WWW.SHELLHACKS.COM/TAG/BASH/)

BOOT (HTTPS://WWW.SHELLHACKS.COM/TAG/BOOT/) CISCO (HTTPS://WWW.SHELLHACKS.COM/TAG/CISCO/)

COMMAND-LINE (HTTPS://WWW.SHELLHACKS.COM/TAG/COMMAND-LINE/)

CURL (HTTPS://WWW.SHELLHACKS.COM/TAG/CURL/) DNS (HTTPS://WWW.SHELLHACKS.COM/TAG/DNS/)

DOCKER (HTTPS://WWW.SHELLHACKS.COM/TAG/DOCKER/)

ENCODING (HTTPS://WWW.SHELLHACKS.COM/TAG/ENCODING/)

ENCRYPTION (HTTPS://WWW.SHELLHACKS.COM/TAG/ENCRYPTION/)

FTP (HTTPS://WWW.SHELLHACKS.COM/TAG/FTP/) GIT (HTTPS://WWW.SHELLHACKS.COM/TAG/GIT/)

HISTORY (HTTPS://WWW.SHELLHACKS.COM/TAG/HISTORY/) ISO (HTTPS://WWW.SHELLHACKS.COM/TAG/ISO/)

JOHN-THE-RIPPER (HTTPS://WWW.SHELLHACKS.COM/TAG/JOHN-THE-RIPPER/)

MAIL (HTTPS://WWW.SHELLHACKS.COM/TAG/MAIL/)

MOD-WSGI (HTTPS://WWW.SHELLHACKS.COM/TAG/MOD-WSGI/)

MONGODB (HTTPS://WWW.SHELLHACKS.COM/TAG/MONGODB/)

MONITORING (HTTPS://WWW.SHELLHACKS.COM/TAG/MONITORING/)

MOUNT (HTTPS://WWW.SHELLHACKS.COM/TAG/MOUNT/) MYSQL (HTTPS://WWW.SHELLHACKS.COM/TAG/MYSQL/)

NETWORK (HTTPS://WWW.SHELLHACKS.COM/TAG/NETWORK/)

NMAP (HTTPS://WWW.SHELLHACKS.COM/TAG/NMAP/)

OPENSSL (HTTPS://WWW.SHELLHACKS.COM/TAG/OPENSSL/)

PASSWORD (HTTPS://WWW.SHELLHACKS.COM/TAG/PASSWORD/)

PDF (HTTPS://WWW.SHELLHACKS.COM/TAG/PDF/)

PERFORMANCE (HTTPS://WWW.SHELLHACKS.COM/TAG/PERFORMANCE/)

PROMETHEUS (HTTPS://WWW.SHELLHACKS.COM/TAG/PROMETHEUS/)

PROXY (HTTPS://WWW.SHELLHACKS.COM/TAG/PROXY/)

PYTHON (HTTPS://WWW.SHELLHACKS.COM/TAG/PYTHON/) REDIS (HTTPS://WWW.SHELLHACKS.COM/TAG/REDIS/)

REGEX (HTTPS://WWW.SHELLHACKS.COM/TAG/REGEX/)

REPOSITORY (HTTPS://WWW.SHELLHACKS.COM/TAG/REPOSITORY/)

SALT-STACK (HTTPS://WWW.SHELLHACKS.COM/TAG/SALT-STACK/)

SSH (HTTPS://WWW.SHELLHACKS.COM/TAG/SSH/) TELNET (HTTPS://WWW.SHELLHACKS.COM/TAG/TELNET/)

TEXT-PROCESSING (HTTPS://WWW.SHELLHACKS.COM/TAG/TEXT-PROCESSING/)

TOR (HTTPS://WWW.SHELLHACKS.COM/TAG/TOR/) TSM (HTTPS://WWW.SHELLHACKS.COM/TAG/TSM/)

WGET (HTTPS://WWW.SHELLHACKS.COM/TAG/WGET/) YUM (HTTPS://WWW.SHELLHACKS.COM/TAG/YUM/)