[How can I verify Tor Browser's signature?](https://support.torproject.org/tbb/how-to-verify-signature/#how-to-verify-signature)

Digital signature is a process ensuring that a certain package was generated by its developers and has not been tampered with. Below we explain why it is important and how to verify that the Tor program you download is the one we have created and has not been modified by some attacker.

Each file on our [download page](https://www.torproject.org/download/) is accompanied by a file with the same name as the package and the extension ".asc". These .asc files are OpenPGP signatures. They allow you to verify the file you've downloaded is exactly the one that we intended you to get.

For example, torbrowser-install-win64-9.0\_en-US.exe is accompanied by torbrowser-install-win64-9.0\_en-US.exe.asc. These are example file names and will not exactly match the file names that you download.

We now show how you can verify the downloaded file's digital signature on different operating systems. Please notice that a signature is dated the moment the package has been signed. Therefore every time a new file is uploaded a new signature is generated with a different date. As long as you have verified the signature you should not worry that the reported date may vary.

Installing GnuPG

First of all you need to have GnuPG installed before you can verify signatures.

For Windows users:

If you run Windows, [download Gpg4win](https://gpg4win.org/download.html) and run its installer.

In order to verify the signature you will need to type a few commands in windows command-line, cmd.exe.

For macOS users:

If you are using macOS, you can [install GPGTools](https://www.gpgtools.org/).

In order to verify the signature you will need to type a few commands in the Terminal (under "Applications").

For GNU/Linux users:

If you are using GNU/Linux, then you probably already have GnuPG in your system, as most GNU/Linux distributions come with it preinstalled.

In order to verify the signature you will need to type a few commands in a terminal window. How to do this will vary depending on your distribution.

Fetching the Tor Developers key

The Tor Browser team signs Tor Browser releases. Import the Tor Browser Developers signing key (0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290):

gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org

This should show you something like:

gpg: key 4E2C6E8793298290: public key "Tor Browser Developers (signing key) <torbrowser@torproject.org>" imported

gpg: Total number processed: 1

gpg: imported: 1

pub rsa4096 2014-12-15 [C] [expires: 2020-08-24]

EF6E286DDA85EA2A4BA7DE684E2C6E8793298290

uid [ unknown] Tor Browser Developers (signing key) <torbrowser@torproject.org>

sub rsa4096 2018-05-26 [S] [expires: 2020-09-12]

If you get an error message, something has gone wrong and you cannot continue until you've figured out why this didn't work. You might be able to import the key using the **Workaround (using a public key)** section instead.

After importing the key, you can save it to a file (identifying it by fingerprint here):

gpg --output ./tor.keyring --export 0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290

If ./tor.keyring doesn't exist after running this command, something has gone wrong and you cannot continue until you've figured out why this didn't work.

Verifying the signature

To verify the signature of the package you downloaded, you will need to download the corresponding ".asc" signature file as well as the installer file itself, and verify it with a command that asks GnuPG to verify the file that you downloaded.

The examples below assume that you downloaded these two files to your "Downloads" folder. Note that these commands use example file names and yours will be different: you will have downloaded a different version than 9.0 and you may not have chosen the English (en-US) version.

For Windows users:

gpgv --keyring .\tor.keyring Downloads\torbrowser-install-win64-9.0\_en-US.exe.asc Downloads\torbrowser-install-win64-9.0\_en-US.exe

For macOS users:

gpgv --keyring ./tor.keyring ~/Downloads/TorBrowser-9.0-osx64\_en-US.dmg.asc ~/Downloads/TorBrowser-9.0-osx64\_en-US.dmg

For GNU/Linux users (change 64 to 32 if you have the 32-bit package):

gpgv --keyring ./tor.keyring ~/Downloads/tor-browser-linux64-9.0\_en-US.tar.xz.asc ~/Downloads/tor-browser-linux64-9.0\_en-US.tar.xz

The result of the command should produce something like this:

gpgv: Signature made 07/08/19 04:03:49 Pacific Daylight Time

gpgv: using RSA key EB774491D9FF06E2

gpgv: Good signature from "Tor Browser Developers (signing key) <torbrowser@torproject.org>"

If you get error messages containing 'No such file or directory', either something went wrong with one of the previous steps, or you forgot that these commands use example file names and yours will be a little different.

Workaround (using a public key)

If you encounter errors you cannot fix, feel free to [download and use this public key](https://openpgpkey.torproject.org/.well-known/openpgpkey/torproject.org/hu/kounek7zrdx745qydx6p59t9mqjpuhdf) instead. Alternatively, you may use the following command:

curl -s https://openpgpkey.torproject.org/.well-known/openpgpkey/torproject.org/hu/kounek7zrdx745qydx6p59t9mqjpuhdf |gpg --import -

You may also want to [learn more about GnuPG](https://www.gnupg.org/documentation/).