Steps to verify digital signatures

1) Install GnuPG. Depending on the operating system, install the GnuPG key management software (Windows, Mac OS) or ensure it is pre-installed on GNU/Linux.

2) Import the Tor Developers signing key (0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290) by opening GnuPG and entering the following:

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

3) Save the key to a file by typing in the following. The Tor Developers key should be saved in the same folder as the key that needs verification.

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

4) Verify the signature. Compare the downloaded *.asc* file against the Tor browser installer to ensure its integrity and authenticity.

- **For Windows users**, in the Command terminal (cmd.exe), type:
  ```
  gpgv --keyring .\tor.keyring Downloads\torbrowser-install-win64-13.0.13.exe.asc
  Downloads\torbrowser-install-win64-13.0.13.exe
  ```

- **For macOS users**, in the Terminal (under "Applications"), type:
  ```
  gpgv --keyring ./tor.keyring ~/Downloads/Torbrowser-13.0.13-osx64_en-US.dmg.asc
  ~/Downloads/Torbrowser-13.0.13-osx64.dmg
  ```

- **For GNU/Linux users** (change 64 to 32 if you have the 32-bit package), in a terminal window, type:
  ```
  gpgv --keyring ./tor.keyring
  ~/Downloads/tor-browser-linux64-13.0.13.tar.xz.asc
  ~/Downloads/tor-browser-linux64-13.0.13.tar.xz$
  ```

5) Check the positive result. The display result should produce the following result (date and time change according to each person):

```
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>"
```