How do I verify the checksum of a file on Debathena?

Q: How do I verify the checksum of a file on Debathena?

- How do I verify the md5sum of a file?
- How do I verify the sha256sum of a file?

Context

- You have downloaded a file from a website, and the site offers a checksum (e.g. a sha256sum or an md5sum) of the file for verification.

Answer

When downloading software that you intend to run, it's important to verify that it's from a trusted source. The easiest way to do this is to download the software over a secure connection (e.g. from a URL that begins with `https://`), but if you cannot do that, you can also verify the checksum.

1. Obtain the checksum file. Typically, the site will have a link to the checksum file. Ensure that you're download it over a secure connection, otherwise you have no guarantee that the checksum itself hasn't also been tampered with.

2. Determine the checksum type. Typically, the site will indicate this either in text, or in the filename of the checksum. The two most common checksums are SHA256 and MD5.

   - If you aren't sure, consult the file itself. The file will typically have a long string of hexadecimal digits (0-9 and a-f). If the string is 32 characters long, it's likely an MD5 checksum. If the string is 64 characters long, it's likely SHA256. However, other checksum algorithms can produce similar values, so consult the software's website for the correct checksum type.

3. Verify that you have the correct utility to compute the checksum:

   - SHA256: `sha256sum` (Linux), `shasum -a 256` (Mac OS)
   - MD5: `md5sum` (Linux), `md5` (Mac OS)

4. Verify the checksum. You can do this automatically, or manually.

Automatic verification: If the checksum file is in the correct format (each line has a checksum, followed by a filename) and the name of the file to be verified matches the file you downloaded, you can run the following command:
Linux: `sha256sum -c` *`name-of-checksum-file`*
Mac OS: `shasum -a 256 -c` *`name-of-checksum-file`*

Manual verification: You can run the checksum command to generate a checksum for the file you downloaded, and confirm (by visual inspection) that it matches the expected checksum. It can be difficult to compare 64-character values visually, so we recommend this method only as a last resort.
Linux: `sha256sum` *`name_of_file_to_verify`*
Mac OS: `shasum -a 256 -c` *`name_of_file_to_verify`*

Example:

Verifying the checksum of the Debathena installer:

1. Obtain the installer (https://debathena.mit.edu/install-debathena.sh) and save it in your home directory.

2. Obtain the checksum file (https://debathena.mit.edu/install-debathena.sh.sha256sum) and save it in your home directory.

3. Determine the checksum type: Since "sha256sum" is in the filename, we know it's a SHA256 checksum. We can also inspect the contents of the file and see that the checksum value is 64 characters long:

```
$ cat install-debathena.sh.sha256sum
282662a5ac19fb6bb61928fb99d1020b515820a19b6da29df121775bab4adbd2  install-debathena.sh
$
```

4. Calculate the checksum automatically:

```
$ sha256sum -c install-debathena.sh.sha256sum
install-debathena.sh: OK
```

Or we can calculate it manually:

```
$ sha256sum install-debathena.sh
282662a5ac19fb6bb61928fb99d1020b515820a19b6da29df121775bab4adbd2  install-debathena.sh
$
```

and verify that the checksum displays matches the one in the checksum file (install-debathena.sh.sha256sum)