applied cryptography

**Hash Functions**

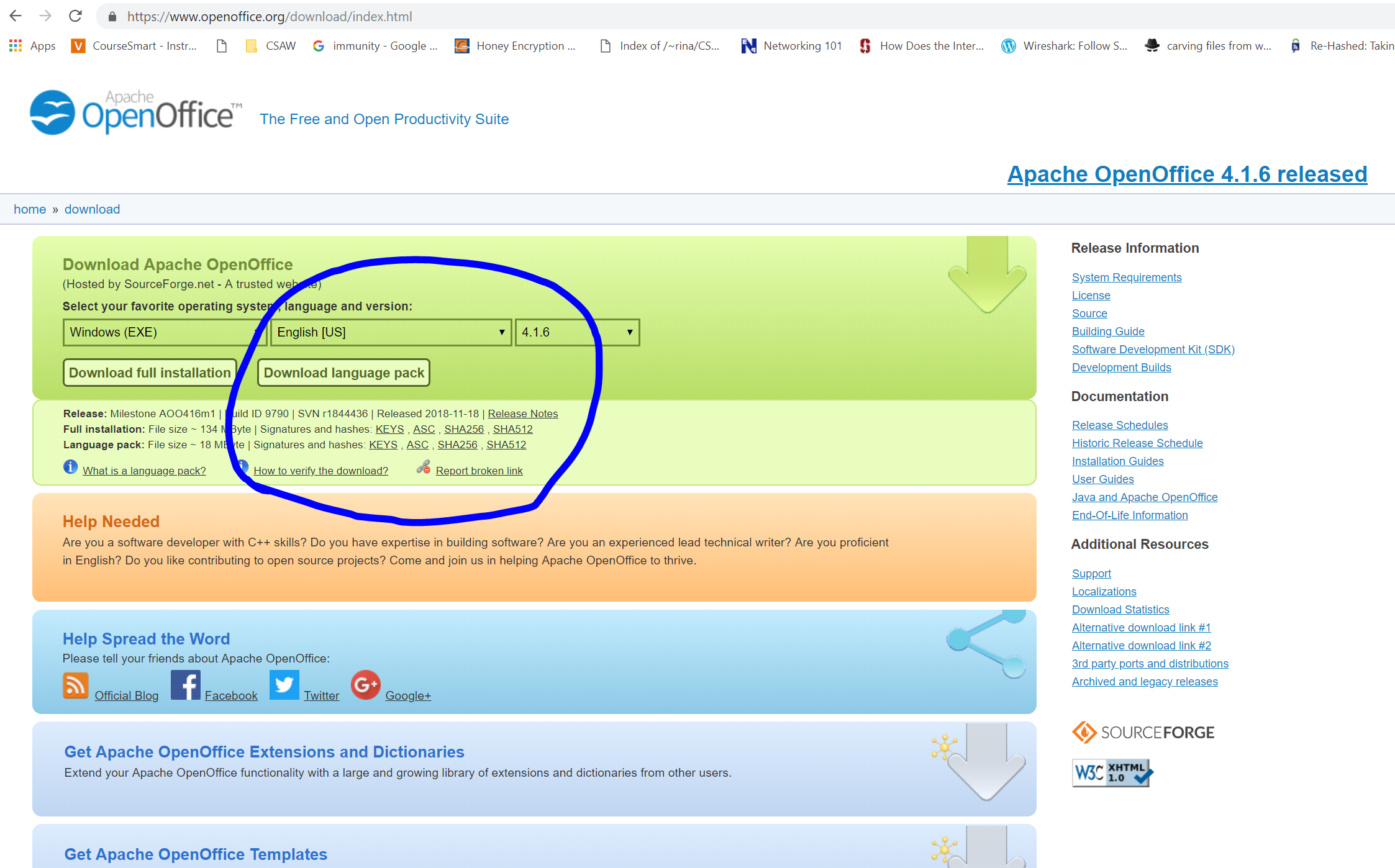
# lab 5: Verifying Integrity of a Download

In this assignment you will verify that a file you download has not been changed during download.

Go to the site <https://www.openoffice.org/download/index.html>.

Note that there two download options: “Download full installation” and “Download language pack.” Download the language pack only and do NOT install it.

Note that two hash values are given for the language pack on the site: SHA 256 and SHA512. Copy and paste these values in this document.



Use an online hash calculator to calculate the SHA256 and SHA512 hashes for the downloaded file. You can use <https://md5file.com/calculator>.

Insert screenshots of these values in this document as well.

## what to submit

Insert screenshots from above steps.

In the Word file, include your answers to the following questions:

1. Compare these hash values on the site with the hash values you have calculated. Are they the same? Explain.
2. What is your conclusion if the SHA256 hash value provided on the site is the same as the one you calculated?
3. What is your conclusion if the SHA256 hash value provided on the site is different from the one you calculated?
4. If the provided hash value is the same as the one you calculated, does that mean that this is absolutely the right file that delivers what it promises, or could it be malicious? Explain.
5. How could a second hash value (such as SHA512, in this case) help to verify the integrity of the download? Explain.

## grading rubric

|  |  |
| --- | --- |
|  | Max. Points |
| Screenshots of four hash values | 50 |
| Answers to questions about hash functions | 50 |
| Total | 100 |

256

ffa7ca39e5e0dced46f2e68ff22331cdd90d304674395f47127458bab038e51a

512

3c472e2c9e784570dcf82abf0b4e8eb8c49546f2baf2d784dc04bea71dccb6821ddf9094019611dfd0f34f77e4f3f7aef4f5223b103fa0ed1cee75ca8726cd0d

