SHA512 FAQ

1. Q: What is SHA512?

A: SHA512 is a cryptographic hash. "SHA" is an acronym for "Secure Hash Algorithm". SHA512 is the strongest cryptographic hash in the SHA2 family.

2. Q: How is SHA512 useful?

A: When you download a file, SHA512 can help you verify that the file you receive is exactly the file that was sent. If the file you downloaded from our website has the same SHA512 hash value as the SHA512 hash value we provide for that file, you can be sure that your copy of the file is complete and that the election results did not change during the download.

3. Q: Is using SHA512 required to download files?

A: No. Using SHA512 to verify your downloaded files is entirely optional. The Department provides the SHA512 hash values as an extra measure of assurance that results reports are reliable statements of turnout through time and do not change.

4. Q: Why does the Department of Elections provide SHA512 hash values for some files but not others?

A: The Department is piloting the use of SHA512 and is providing SHA512 hash values for selected files for which members of the public may have significant interest. The Department may expand its use of SHA512 or other cryptographic hashes based on our experience and user feedback associated with this pilot program.

5. Q: If SHA512 helps me verify that my files were correctly downloaded, how do I verify the correctness of the SHA512 hash values that are shown on your website?

A: For the ultimate and direct distribution of a SHA512 hash value, you may visit the Department's office at City Hall, Room 48, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102.

6. Q: How long is a SHA512 hash value?

A: A SHA512 hash value is 512 bits long. The Department represents a SHA512 hash value as a sequence of 128 hexadecimal digits. A comparison of such SHA512 hash values should be case insensitive, since for example an 'a' is considered to be equal to an 'A'.

7. Q: How can I test my ability to verify a download with SHA512?

A: You can start by creating an empty file, a file that has a length of zero bytes, and calculate its SHA512 hash value. The value you calculate should match the value below:

```
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d1
3c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
```

You can also download the following, nearly identical test files and see if you can calculate the given SHA512 hash value for each of the downloaded files:

http://sfelections.org/results/20151103/data/sha512-test-1.pdf
SHA512 hash value:

```
edd6d54109d1b7e3f31a7eee24f59100eabd10d5b26afa3dfd096558d65e925f2dfc6f
a9a0b4aed54eefa97554518d3d2d0cd10968e28310d5251d3a15407308
```

http://sfelections.org/results/20151103/data/sha512-test-2.pdf
SHA512 hash value:

```
5ef1f37554e10f01e164ec76a824e4e17ce62c4a543320d0f90ba38210ef2d9a9ae2a4
ea739f6e551a0da18332c76cc91666d98eef891f81f030ac3b803a096c
```

8. Q: What kind of support does the Department of Elections provide for my use of SHA512?

A: Unfortunately, the Department is not able to provide any support other than providing this FAQ for informational purposes, the related test files, and providing SHA512 hash values on our website and at our office. The Department of Elections does not guarantee any of the information in this FAQ, and is not responsible for the result of any actions you may take based on this information. Information about or links to other websites for particular products do not represent an endorsement of those products.

9. Q: What should I do if I download a file from your website and my SHA512 hash value is different from the one you give for that file?

A: There are several reasons why your SHA512 hash value may be different, such as:

- Your download may have been incorrect because of a temporary problem. Try downloading the file again after first renaming or moving the result of your first download. Check whether the newly downloaded file produces a SHA512 hash value that matches ours and whether it compares equal to the first downloaded file.
- The Department may have updated the file and/or the SHA512 hash value between the time when you downloaded the file and when you retrieved our SHA512 hash value. When we update a file, we try to nearly simultaneously also update the corresponding SHA512 hash value. You should again both download the file and retrieve our SHA512 hash value without a significant interval of time in between. If either has changed since your first download and retrieval and they now both agree, this may have been the problem.
- You may be trying to match the file against the wrong SHA512 hash value. Double check that the SHA512 hash value you retrieve from our website is really for the file that you downloaded and are trying to verify.

- You may be calculating your SHA512 hash value on a file that is different than the one you downloaded. Make sure the name and path of the file that you calculated the SHA512 hash value for are the same as what you used to store the downloaded file.
- You may not be calculating a SHA512 hash value. Make sure that the program you are using to calculate your SHA512 hash value is being correctly directed to calculate a SHA512 hash value and is not instead calculating some other kind of cryptographic hash. Verify that the hash value you produce is displayed with exactly 128 characters consisting only of hexadecimal digits.
- You may not be correctly calculating a SHA512 hash value. You can test how you are calculating SHA512 hash values by uploading any file to an online service that calculates SHA512 hash values and comparing your value against the value produced by the online service. Do not use a file that contains sensitive information. One such online service is at:
  http://hash.online-convert.com/sha512-generator
- If you are experiencing problems not listed here, check whether the same problem occurs when using a different computer.

Use our email contact form to share your experiences using these tools. We want to identify and correct any problems with our site or information as quickly as possible and the information you provide can help us do so more effectively.

10. Q: How do I calculate the SHA512 hash value for a file that is on my computer?

A: It depends on which operating system your computer is using. See the related questions that follow for additional information about Microsoft Windows, Apple OS X, and Linux/Unix.

11. Q: How do I calculate the SHA512 hash value for a file on my Windows computer?

A: There are several ways you might be able to calculate SHA512 hash values on Windows. You might have a version of PowerShell that supports calculation of SHA512 hash values either with a Microsoft command, Get-FileHash, or with third-party scripts, some of which are also named Get-FileHash. There are also other third-party programs for Windows that calculate a SHA512 hash value.

12. Q: Under what circumstances can I use PowerShell run Microsoft's command or third-party scripts?

A: It depends in part on which version of Windows you are using:
- If you are running Windows 8.1 or later, the Get-FileHash PowerShell command should be available for use.
- If you are running Windows 8.0, you can upgrade to Windows 8.1 and then use the Get-FileHash PowerShell command. Microsoft does not provide a way in Windows 8 to only upgrade PowerShell to version 4.0.
- If you are running Windows 7, you can upgrade to PowerShell 4.0, which then allows you to use the Get-FileHash command.
- If you are running Windows Vista or later with .Net Framework version 4.5 or later, you may be able to use third-party scripts in PowerShell. For example, see:
  http://learn-powershell.net/2013/03/25/use-powershell-to-calculate-the-hash-of-a-file/
  https://gallery.technet.microsoft.com/scriptcenter/Get-FileHash-83ab0189

13. Q: How do I upgrade to PowerShell 4.0 on my Windows 7 computer?

A: One guide for doing this upgrade is at:
http://blogs.technet.com/b/heyscriptingguy/archive/2014/11/09/weekend-scripter-install-powershell-4-0-in-windows-7.aspx

Be sure to read this and related information carefully. Be aware that there is a prerequisite that Windows 7 is using .Net Framework 4.5 or later, but that the upgrade process may not enforce that prerequisite and may fail less than gracefully if you do not ensure it is satisfied.

14. Q: What are third-party programs for calculating SHA512 hash values on Windows?

A: Some options include:

- http://sourceforge.net/projects/quickhash/
- http://implbits.com/products/hashtab/
- https://addons.mozilla.org/en-US/firefox/addon/md5-reborned-hasher/

15. Q: How do I use the Microsoft-provided Get-FileHash Powershell command?

A: Start a PowerShell or PowerShell ISC console. In PowerShell, you can use the command:

```
> help get-filehash
```

to get a synopsis of the command. Navigate to the folder where the file exists (for example using cd and dir commands or using Set-Location and Get-ChildItem commands).

One basic use of the Get-FileHash command for the file downloaded-1.txt is:

```
> get-filehash -path downloaded-1.txt -algorithm sha512
```

However this does not print the full SHA512 hash value. To see the full hash value, you could try:

```
> get-filehash -path downloaded-1.txt -algorithm sha512 | select-object hash
```

You could also store into a CSV file named sha512.csv the SHA512 files for all PDF files in the current folder with:

```
> get-filehash -path *.pdf -algorithm sha512 | export-csv sha512.csv
```

16. Q: How do I calculate a SHA512 hash value for a file on my Apple computer running OS X?

A: Launch a Terminal from the Applications and Utilities folders, and at the command prompt enter a command of the form:

```
> shasum -a 512 path/to/file
```

17. Q: How do I calculate a SHA512 hash value for a file on my Linux/Unix computer?

A: Look for a command such as sha512sum, sha512, shasum, or something similar. Running the command:

> apropos sha512

may help you identify the appropriate command.

FAQ originally written by David Cary for the San Francisco Department of Elections