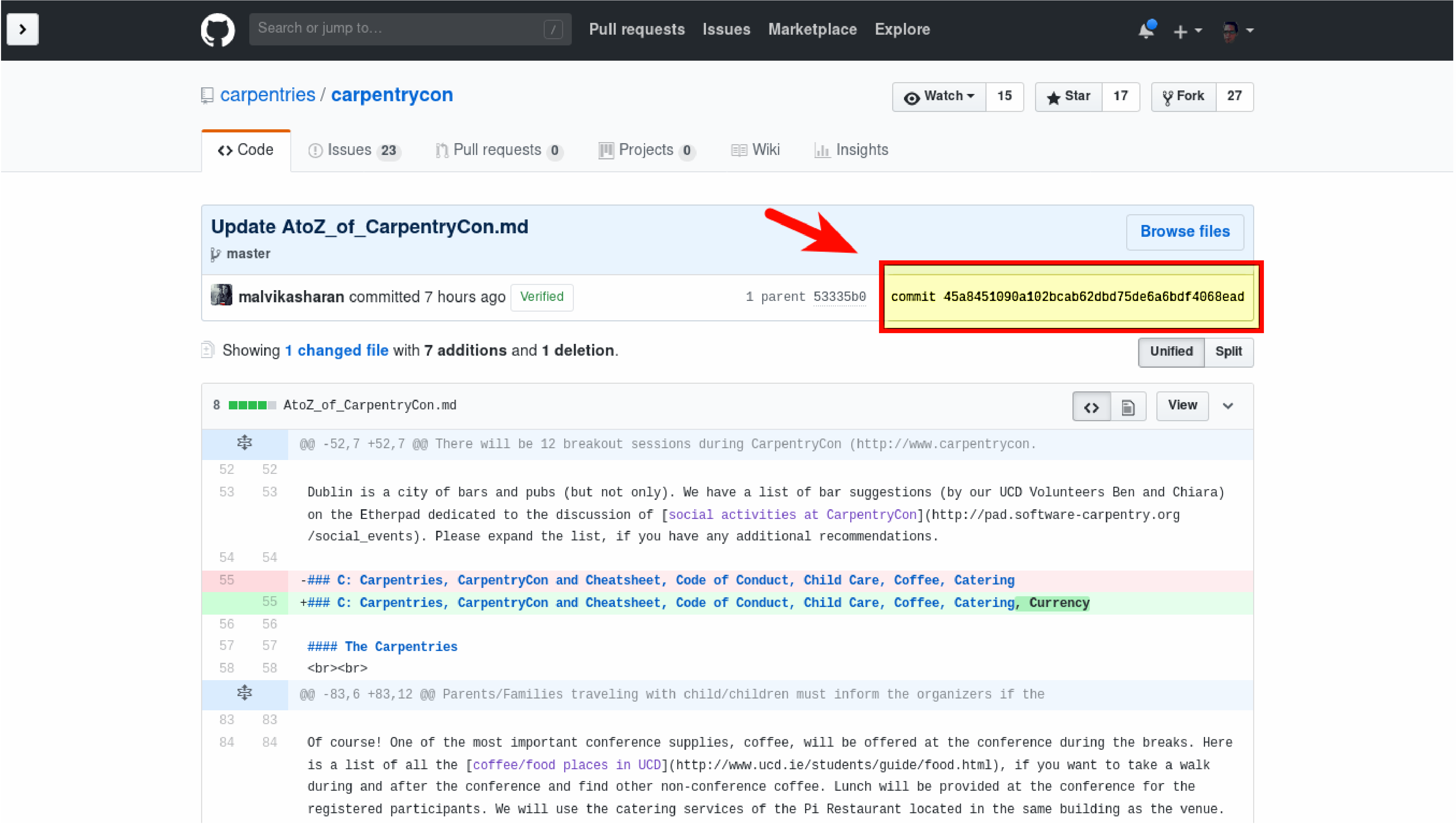
Criptography Essentials for Carpentries Curriculum

Francisco Palm

Pecha Kuc~~ha~~ Style



Update AtoZ_of_CarpentryCon.md

master

malvikasharan committed 7 hours ago

1 parent 53335b0

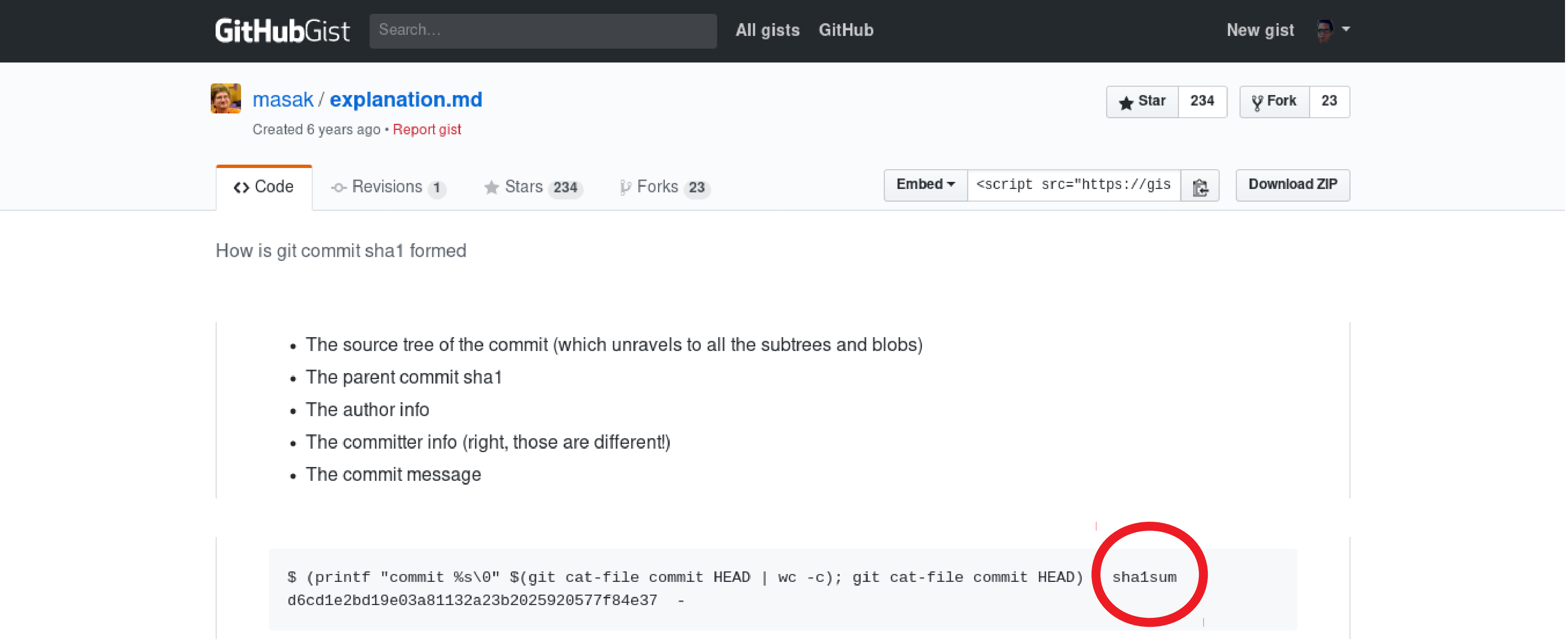
commit 45a8451090a102bcab62dbd75de6a6bdf4068ead

Showing 1 changed file with 7 additions and 1 deletion.

8 AtoZ_of_CarpentryCon.md

```
@@ -52,7 +52,7 @@ There will be 12 breakout sessions during CarpentryCon (http://www.carpentrycon.
52  52
53  53   Dublin is a city of bars and pubs (but not only). We have a list of bar suggestions (by our UCD Volunteers Ben and Chiara)
         on the Etherpad dedicated to the discussion of [social activities at CarpentryCon](http://pad.software-carpentry.org
         /social_events). Please expand the list, if you have any additional recommendations.
54  54
55      -### C: Carpentries, CarpentryCon and Cheatsheet, Code of Conduct, Child Care, Coffee, Catering
    55  +### C: Carpentries, CarpentryCon and Cheatsheet, Code of Conduct, Child Care, Coffee, Catering, Currency
56  56
57  57   #### The Carpentries
58  58   <br><br>
@@ -83,6 +83,12 @@ Parents/Families traveling with child/children must inform the organizers if the
83  83
84  84   Of course! One of the most important conference supplies, coffee, will be offered at the conference during the breaks. Here
         is a list of all the [coffee/food places in UCD](http://www.ucd.ie/students/guide/food.html), if you want to take a walk
         during and after the conference and find other non-conference coffee. Lunch will be provided at the conference for the
         registered participants. We will use the catering services of the Pi Restaurant located in the same building as the venue.
```

What is a commit hash?



How is git commit sha1 formed

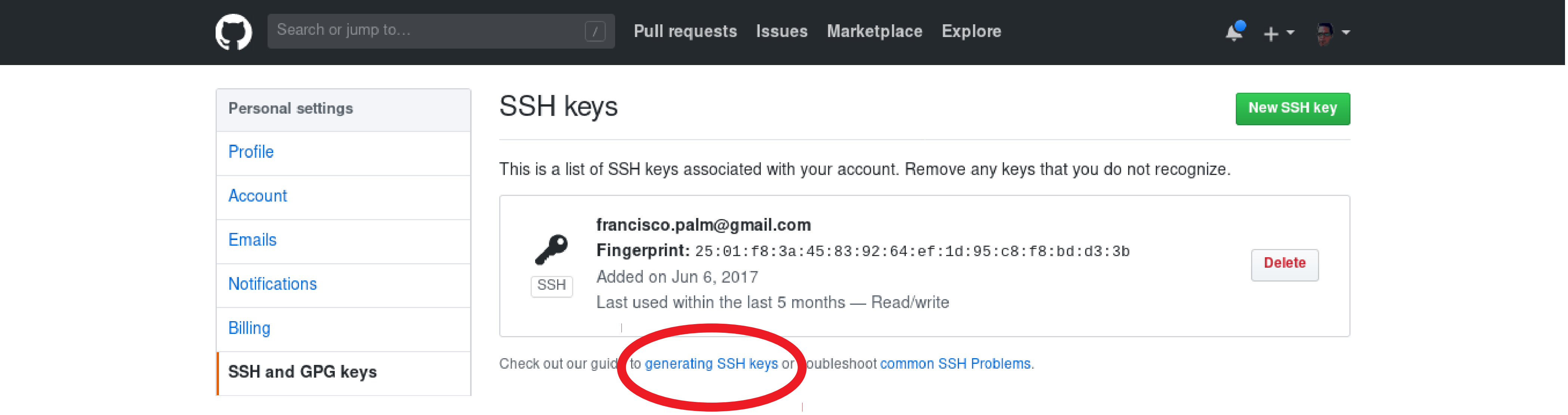
- The source tree of the commit (which unravels to all the subtrees and blobs)
- The parent commit sha1
- The author info
- The committer info (right, those are different!)
- The commit message

```
$ (printf "commit %s\0" $(git cat-file commit HEAD | wc -c); git cat-file commit HEAD) sha1sum
d6cd1e2bd19e03a81132a23b2025920577f84e37  -
```

What is a sha1sum?

For Git “It's purely a consistency check. The security parts are elsewhere”. Linus Torvalds

https://gist.github.com/masak/2415865



SSH keys

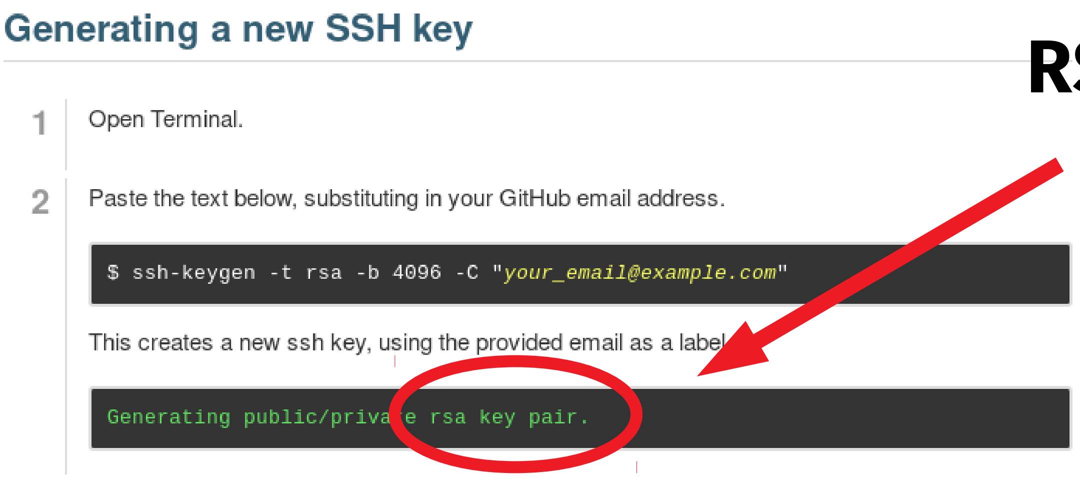
This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.

francisco.palm@gmail.com
Fingerprint: `25:01:f8:3a:45:83:92:64:ef:1d:95:c8:f8:bd:d3:3b`
Added on Jun 6, 2017
Last used within the last 5 months — Read/write

Check out our guide to generating SSH keys or troubleshoot common SSH Problems.

The security parts...

What happen when SSH or GPG keys are generated?



Generating a new SSH key

1 Open Terminal.

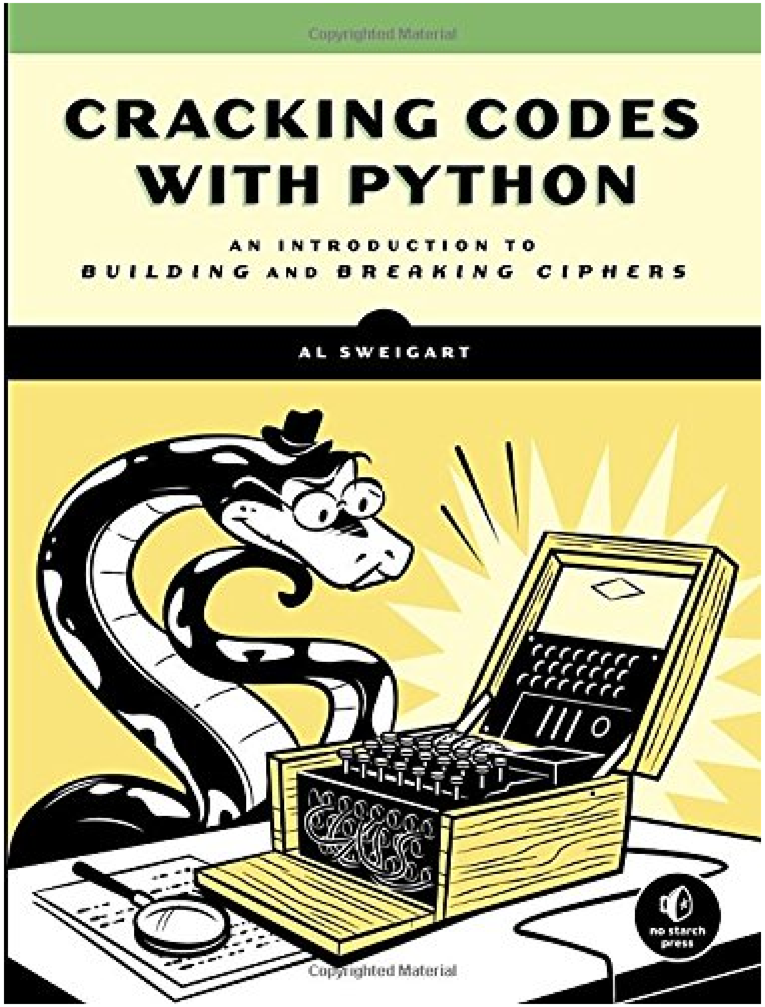
2 Paste the text below, substituting in your GitHub email address.

```
$ ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

This creates a new ssh key, using the provided email as a label.

```
Generating public/private rsa key pair.
```

RSA Key pair?

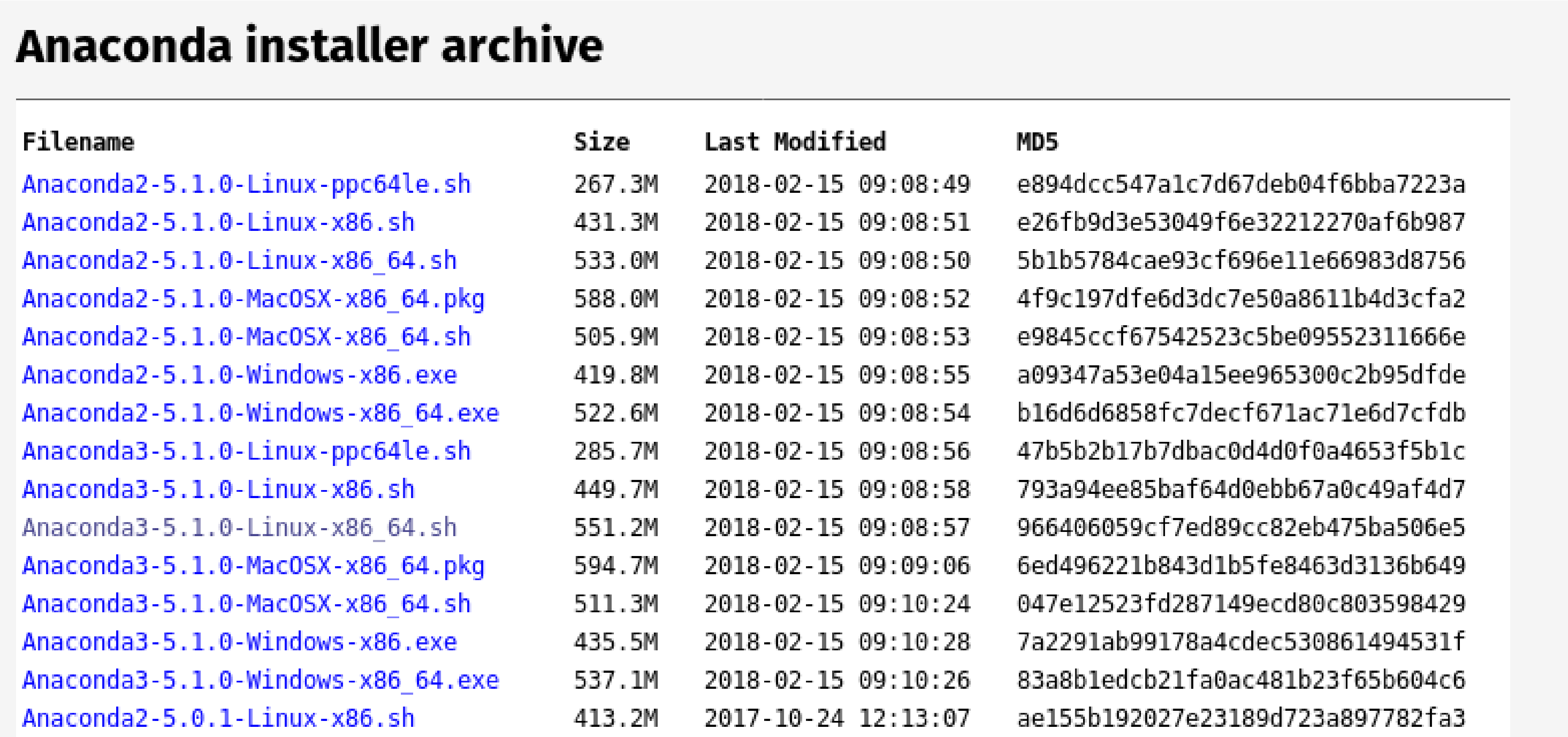

Copyrighted Material
CRACKING CODES WITH PYTHON
AN INTRODUCTION TO BUILDING AND BREAKING CIPHERS
AL SWEIGART
no starch press
Copyrighted Material

Cracking Codes with Python teaches complete beginners how to program in the Python programming language.

…

The final chapters cover the modern RSA cipher and public key cryptography.

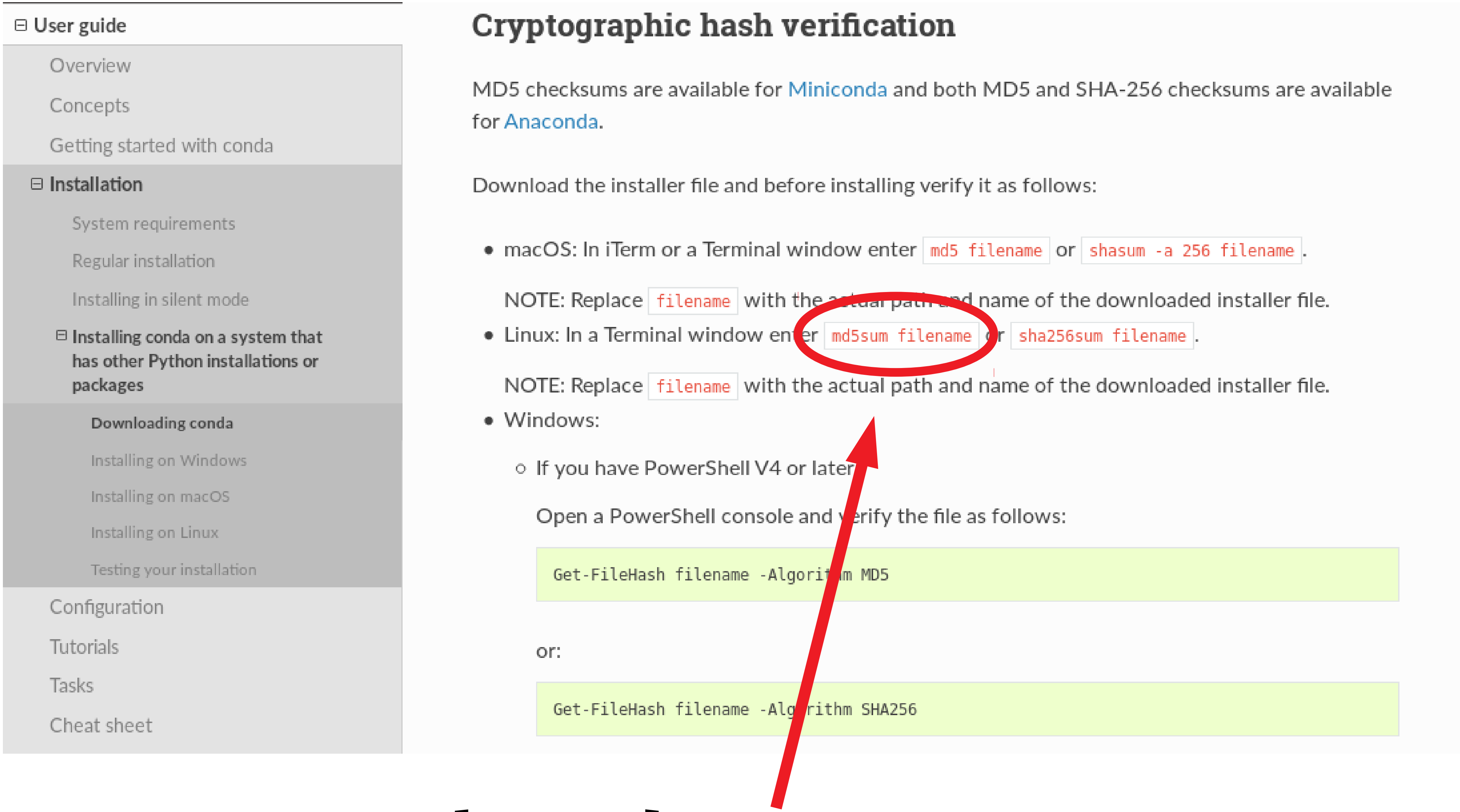
Black magic or accessible content?



Anaconda installer archive

Filename	Size	Last Modified	MD5
Anaconda2-5.1.0-Linux-ppc64le.sh	267.3M	2018-02-15 09:08:49	e894dcc547a1c7d67deb04f6bba7223a
Anaconda2-5.1.0-Linux-x86.sh	431.3M	2018-02-15 09:08:51	e26fb9d3e53049f6e32212270af6b987
Anaconda2-5.1.0-Linux-x86_64.sh	533.0M	2018-02-15 09:08:50	5b1b5784cae93cf696e11e66983d8756
Anaconda2-5.1.0-MacOSX-x86_64.pkg	588.0M	2018-02-15 09:08:52	4f9c197dfe6d3dc7e50a8611b4d3cfa2
Anaconda2-5.1.0-MacOSX-x86_64.sh	505.9M	2018-02-15 09:08:53	e9845ccf67542523c5be09552311666e
Anaconda2-5.1.0-Windows-x86.exe	419.8M	2018-02-15 09:08:55	a09347a53e04a15ee965300c2b95dfde
Anaconda2-5.1.0-Windows-x86_64.exe	522.6M	2018-02-15 09:08:54	b16d6d6858fc7decf671ac71e6d7cfdb
Anaconda3-5.1.0-Linux-ppc64le.sh	285.7M	2018-02-15 09:08:56	47b5b2b17b7dbac0d4d0f0a4653f5b1c
Anaconda3-5.1.0-Linux-x86.sh	449.7M	2018-02-15 09:08:58	793a94ee85baf64d0ebb67a0c49af4d7
Anaconda3-5.1.0-Linux-x86_64.sh	551.2M	2018-02-15 09:08:57	966406059cf7ed89cc82eb475ba506e5
Anaconda3-5.1.0-MacOSX-x86_64.pkg	594.7M	2018-02-15 09:09:06	6ed496221b843d1b5fe8463d3136b649
Anaconda3-5.1.0-MacOSX-x86_64.sh	511.3M	2018-02-15 09:10:24	047e12523fd287149ecd80c803598429
Anaconda3-5.1.0-Windows-x86.exe	435.5M	2018-02-15 09:10:28	7a2291ab99178a4cdec530861494531f
Anaconda3-5.1.0-Windows-x86_64.exe	537.1M	2018-02-15 09:10:26	83a8b1edcb21fa0ac481b23f65b604c6
Anaconda2-5.0.1-Linux-x86.sh	413.2M	2017-10-24 12:13:07	ae155b192027e23189d723a897782fa3

How to use this information?
Is important?



Cryptographic hash verification

MD5 checksums are available for Miniconda and both MD5 and SHA-256 checksums are available for Anaconda.

Download the installer file and before installing verify it as follows:

- macOS: In iTerm or a Terminal window enter `md5 filename` or `shasum -a 256 filename`.

  NOTE: Replace `filename` with the actual path and name of the downloaded installer file.
- Linux: In a Terminal window enter `md5sum filename` or `sha256sum filename`.

  NOTE: Replace `filename` with the actual path and name of the downloaded installer file.
- Windows:
  - If you have PowerShell V4 or later:

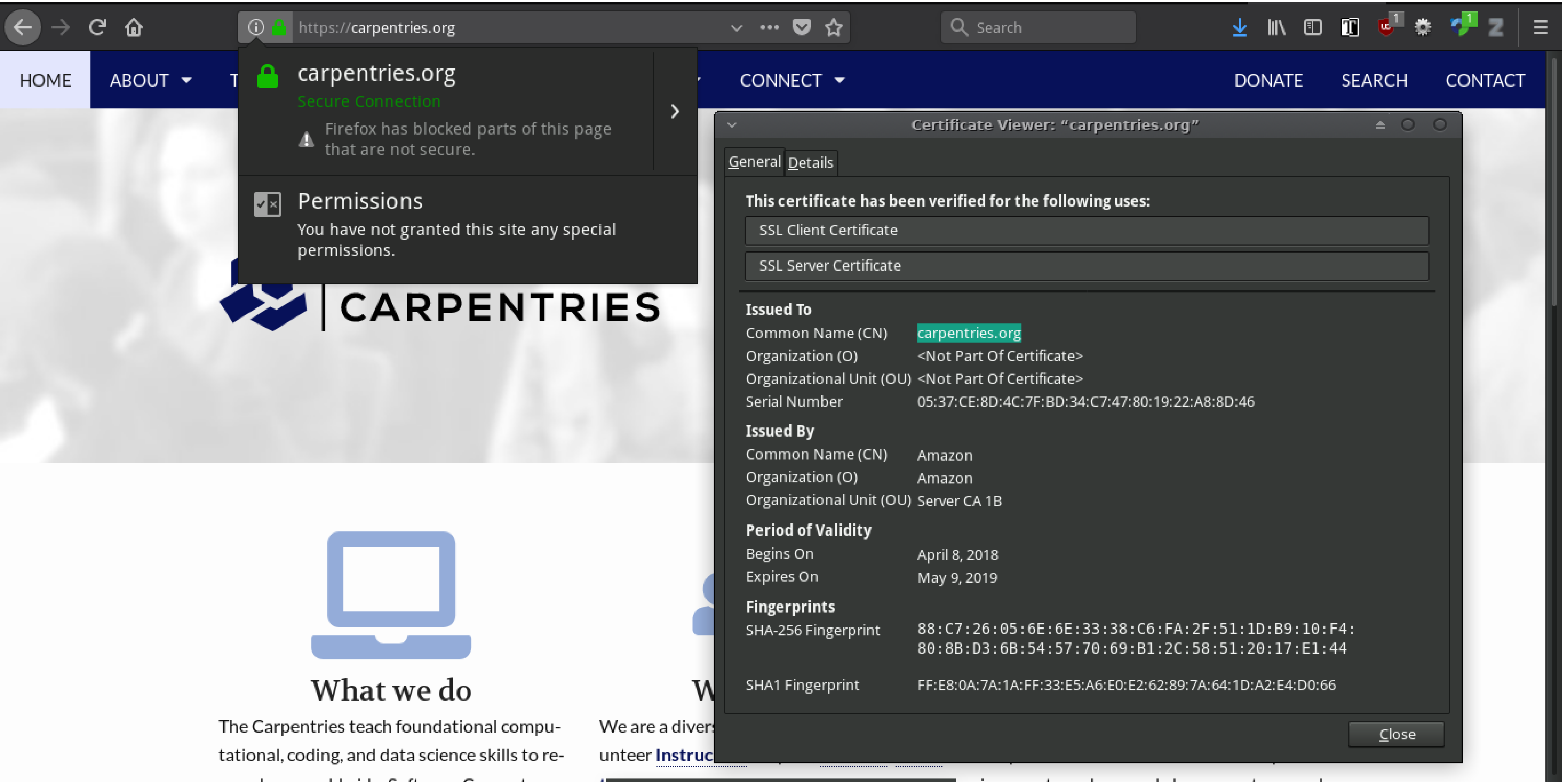
    Open a PowerShell console and verify the file as follows:

    ```
    Get-FileHash filename -Algorithm MD5
    ```

    or:

    ```
    Get-FileHash filename -Algorithm SHA256
    ```

Enough and comprehensive?



carpentries.org

Secure Connection

Firefox has blocked parts of this page that are not secure.

Permissions

You have not granted this site any special permissions.

Certificate Viewer: “carpentries.org”

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To	
Common Name (CN)	carpentries.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	05:37:CE:8D:4C:7F:BD:34:C7:47:80:19:22:A8:8D:46
Issued By	
Common Name (CN)	Amazon
Organization (O)	Amazon
Organizational Unit (OU)	Server CA 1B
Period of Validity	
Begins On	April 8, 2018
Expires On	May 9, 2019
Fingerprints	
SHA-256 Fingerprint	88:C7:26:05:6E:6E:33:38:C6:FA:2F:51:1D:B9:10:F4: 80:8B:D3:6B:54:57:70:69:B1:2C:58:51:20:17:E1:44
SHA1 Fingerprint	FF:E8:0A:7A:1A:FF:33:E5:A6:E0:E2:62:89:7A:64:1D:A2:E4:D0:66

What we do

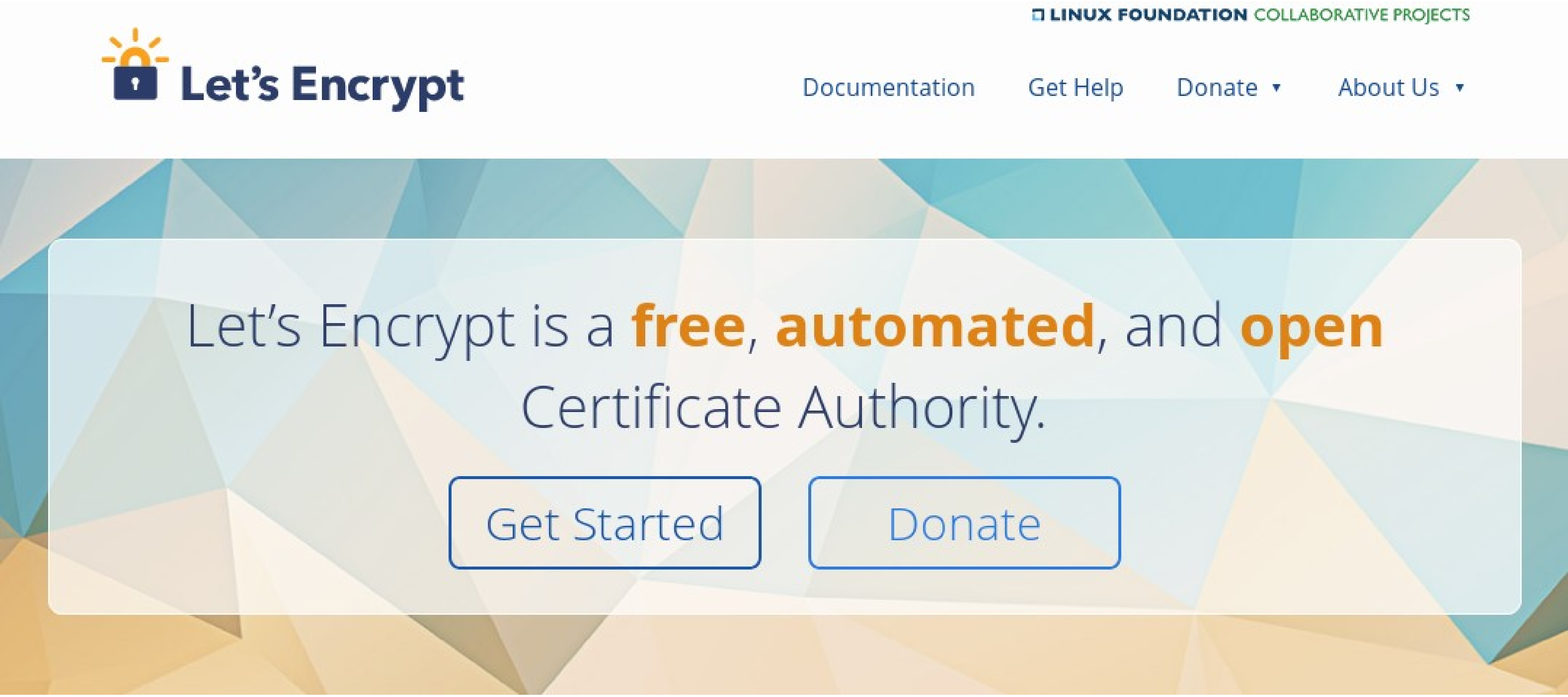
The Carpentries teach foundational computational, coding, and data science skills to re-

We are a divers

unteer Instruc

Certificates are important?

Do you use bank services on-line?



LINUX FOUNDATION COLLABORATIVE PROJECTS

Let's Encrypt

Let's Encrypt is a **free**, **automated**, and **open** Certificate Authority.

Do you know that now is easy and cheap to obtain certificates?

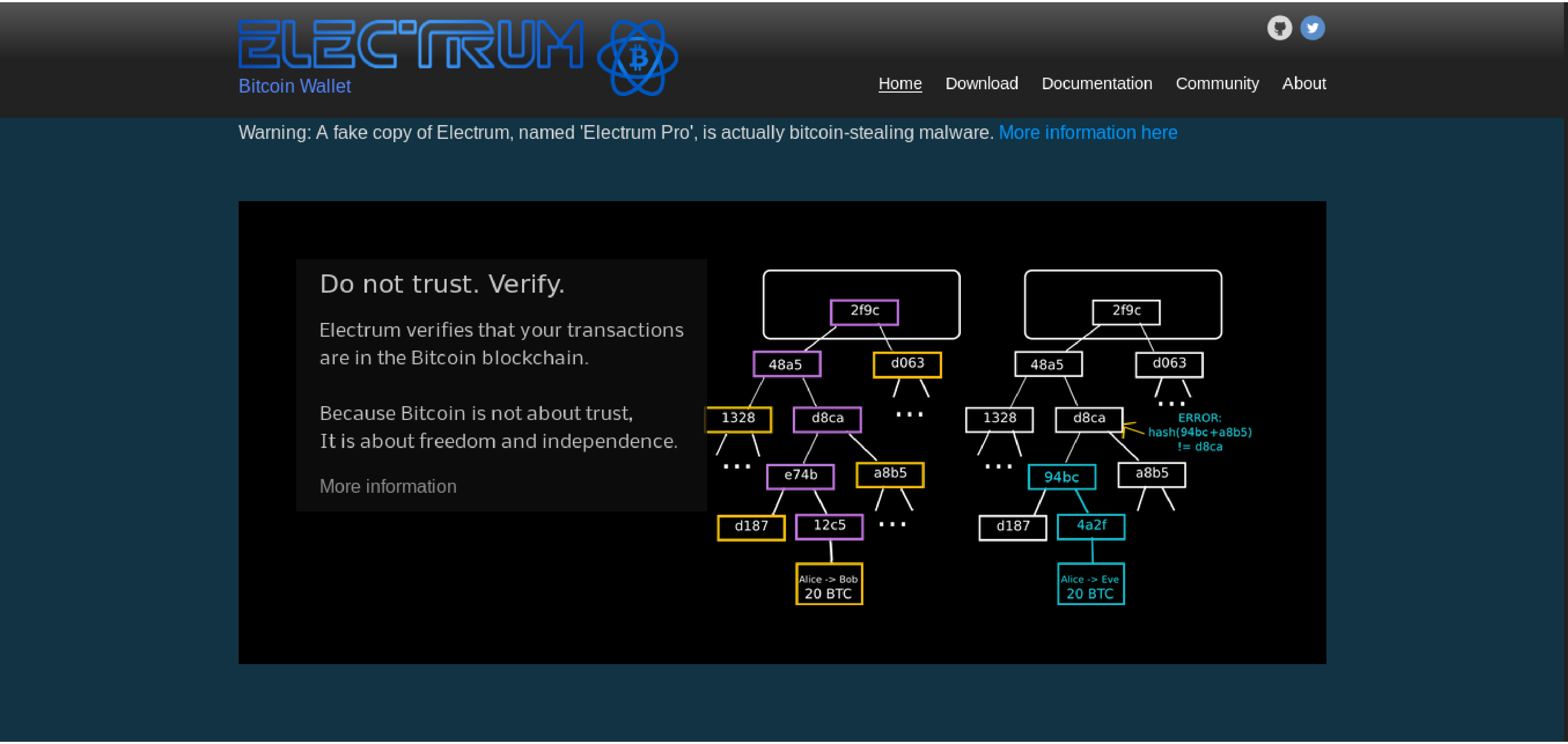
Automatically enable HTTPS on your website with EFF's Certbot, deploying Let's Encrypt certificates.

I'm using Software on System

Very easy!

```
$ sudo certbot –apache
```

```
0 0,12 * * * python -c 'import random; import time;
time.sleep(random.random() * 3600)' && certbot renew
```



ELECTRUM

Bitcoin Wallet

Home Download Documentation Community About

Warning: A fake copy of Electrum, named 'Electrum Pro', is actually bitcoin-stealing malware. More information here

Do not trust. Verify.

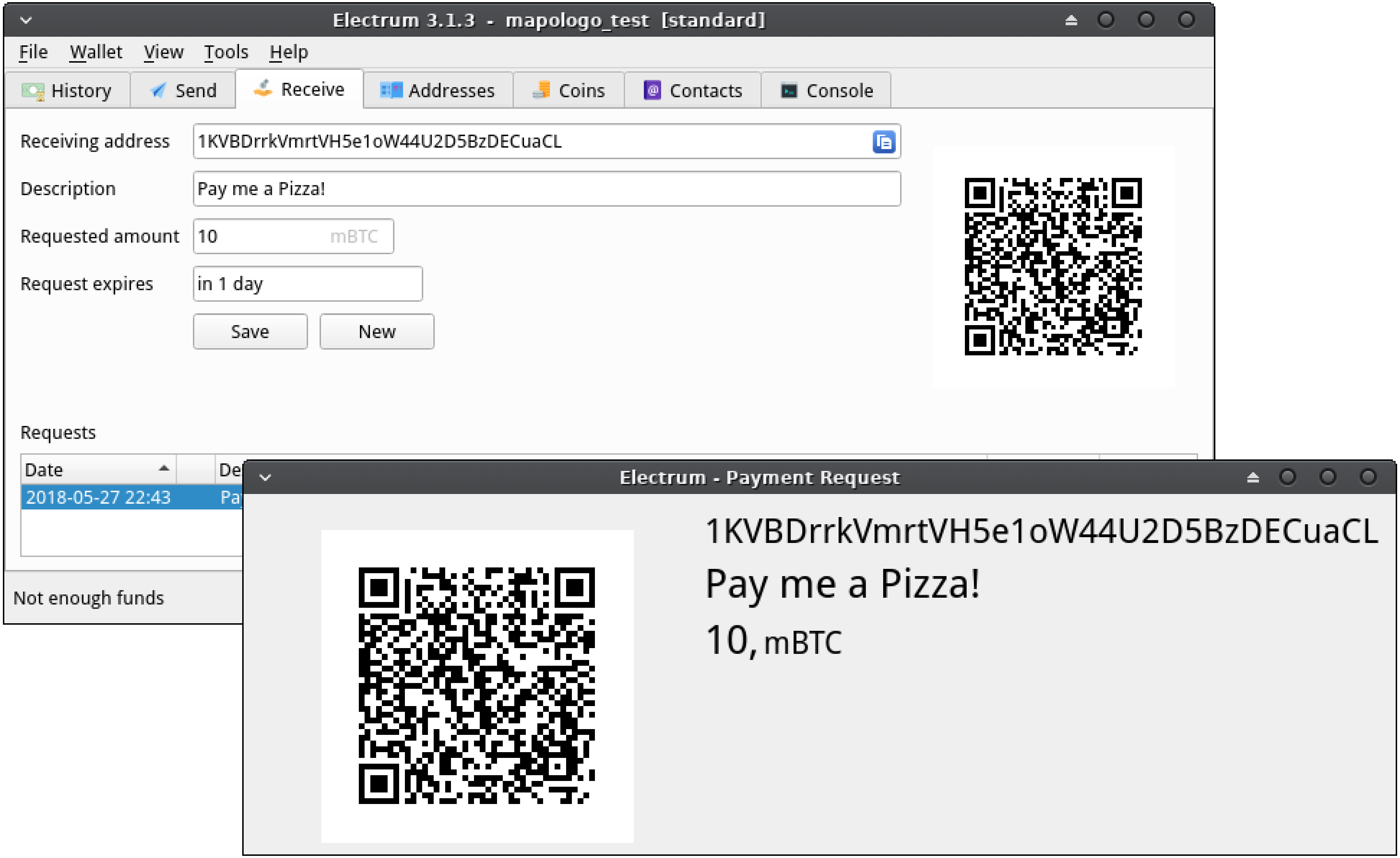
Electrum verifies that your transactions are in the Bitcoin blockchain.

Because Bitcoin is not about trust,
It is about freedom and independence.

More information

Is also very easy create a Bitcoin wallet

to understand public key cryptography



Receiving address: 1KVBDrrkVmrtVH5e1oW44U2D5BzDECuaCL

Description: Pay me a Pizza!

Requested amount: 10 mBTC

Request expires: in 1 day

Requests

Date	De
2018-05-27 22:43	Pa

Not enough funds

1KVBDrrkVmrtVH5e1oW44U2D5BzDECuaCL

Pay me a Pizza!

10, mBTC

And receive payments!

In case of doubt use testbeds

Get your encrypted mailbox for free.

And install our app:

Why you may need to encrypt your emails? How?

How to digitally sign a LibreOffice 6 document with GnuPG

With the release of LibreOffice 6 comes a much more user-friendly means of digitally signing a document. Jack Wallen shows you how.

By Jack Wallen | February 15, 2018, 8:02 AM PST

The new commute: How driverless cars, hyperloop, and drones will change our

Exomedicine arrives: How labs in space could pave the way for healthcare

Why you would need to sign digitally a document?

We really need it?

How to prioritize it?

How we can implement it?

Which approach would be useful?