Deep Dive into Let’s Encrypt

Slides and follow-up available on joind.in at
https://joind.in/talk/c5643

- Full-stack developer, architect, consultant since 1997
- Cypherpunk since 1992 - Focus on security and privacy
- Financial/Payment, Healthcare, VPN-of-Things
- Ran a hosting farm for 10 years
- Not a representative of Let’s Encrypt or ISRG

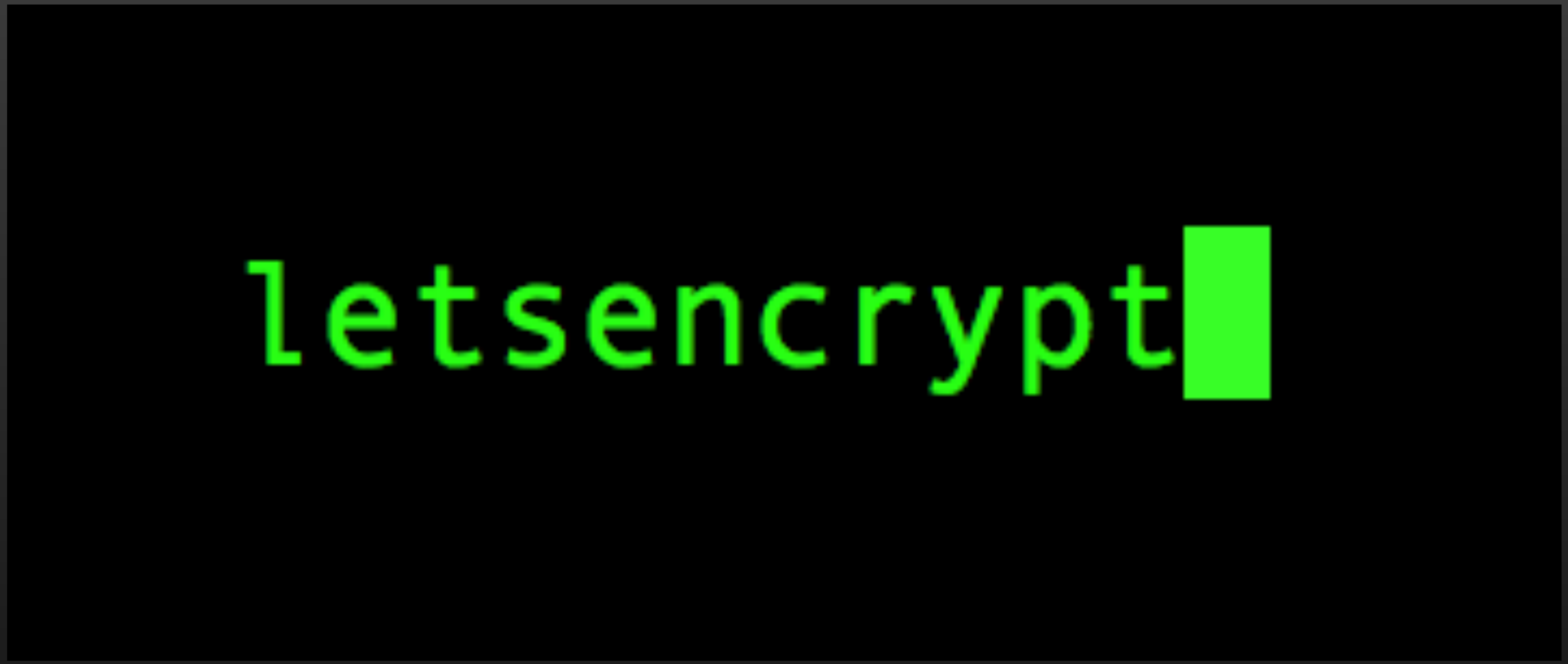
In case you are unfamiliar with Let’s Encrypt…

- Certificate Authority - Free, automated
- Product of the Internet Security Research Group, with funding from EFF and others.
- Wide browser acceptance due to IdenTrust’s cross-signature. (XP SP3, FF2.0)
- Automated issuance with ACME protocol

From 1993 to 2015, the HTTPS Procedure was…

- Execute a series of OpenSSL incantations maybe only 200 people really understand to create a Certificate Signing Request (CSR)
- Pay an average of $150 a year to a company that was in the right place at the right time a decade ago.
- Perform a sacred email authentication ceremony.
- Wait
- Give the correct configuration to your web server.

The Goal of Let’s Encrypt:



```
letsencrypt
```

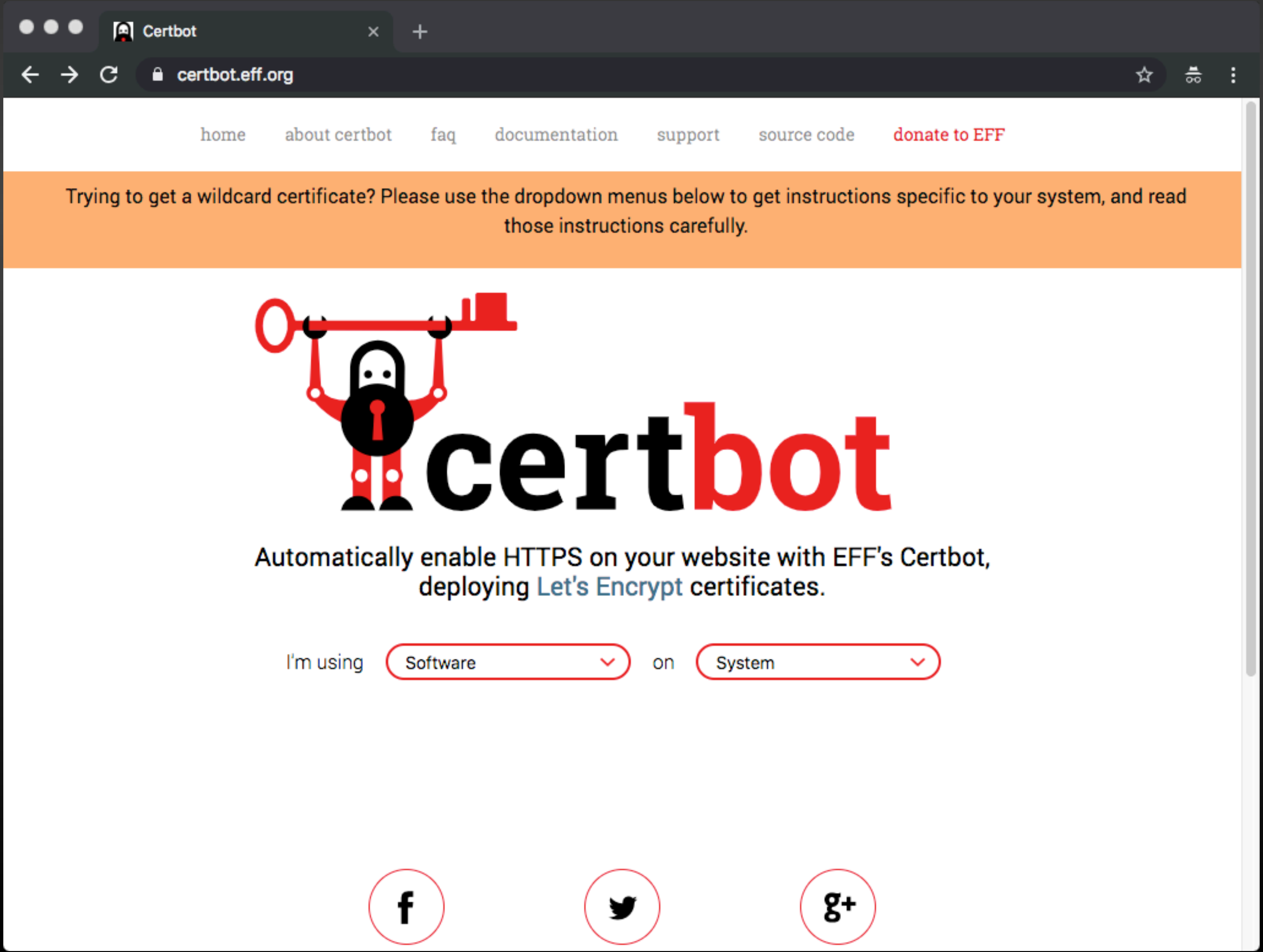
Free, open, automatic, everywhere

Why?

- Fire sheep, rogue access points and cell towers, malware snooping, Snowden NSA revelations (confirmations), ISPs tryng to sell your traffic to marketers, etc.
- Falling certificate prices haven't enabled the web to "go dark"

ACME != Rocket Sleds

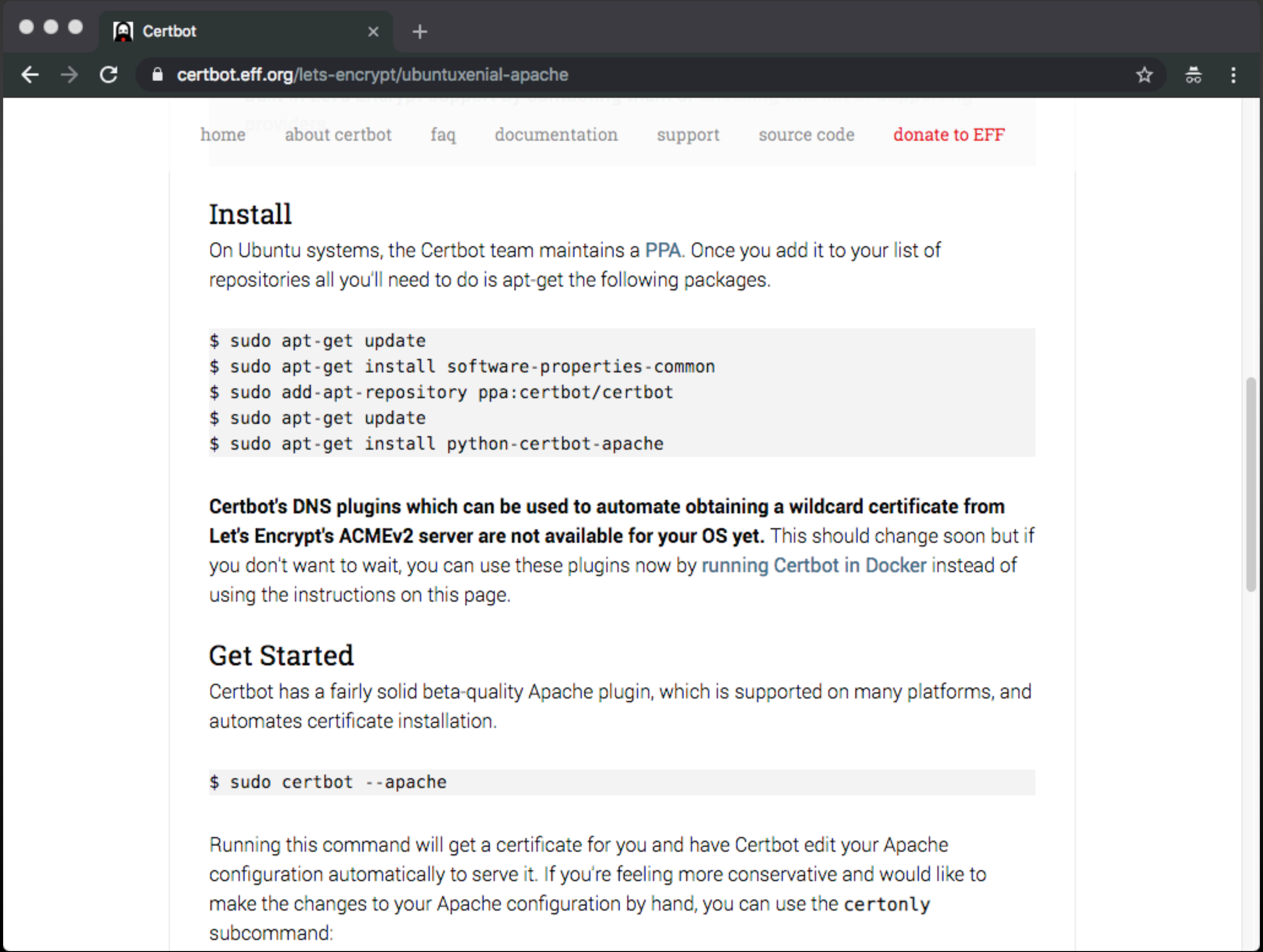
- “Automated Certificate Management Environment”
- IETF Standards track
- https://github.com/ietf-wg-acme/acme/
- Prototype server “boulder” (Go) / prototype client “certbot” (python)
- Uses proof-of-control to verify authority:
- Typically a nonce at http://site.tld/.well-known/acme-challence/nonce



Trying to get a wildcard certificate? Please use the dropdown menus below to get instructions specific to your system, and read those instructions carefully.

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

I'm using Software on System



Install

On Ubuntu systems, the Certbot team maintains a PPA. Once you add it to your list of repositories all you'll need to do is apt-get the following packages.

```
$ sudo apt-get update
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository ppa:certbot/certbot
$ sudo apt-get update
$ sudo apt-get install python-certbot-apache
```

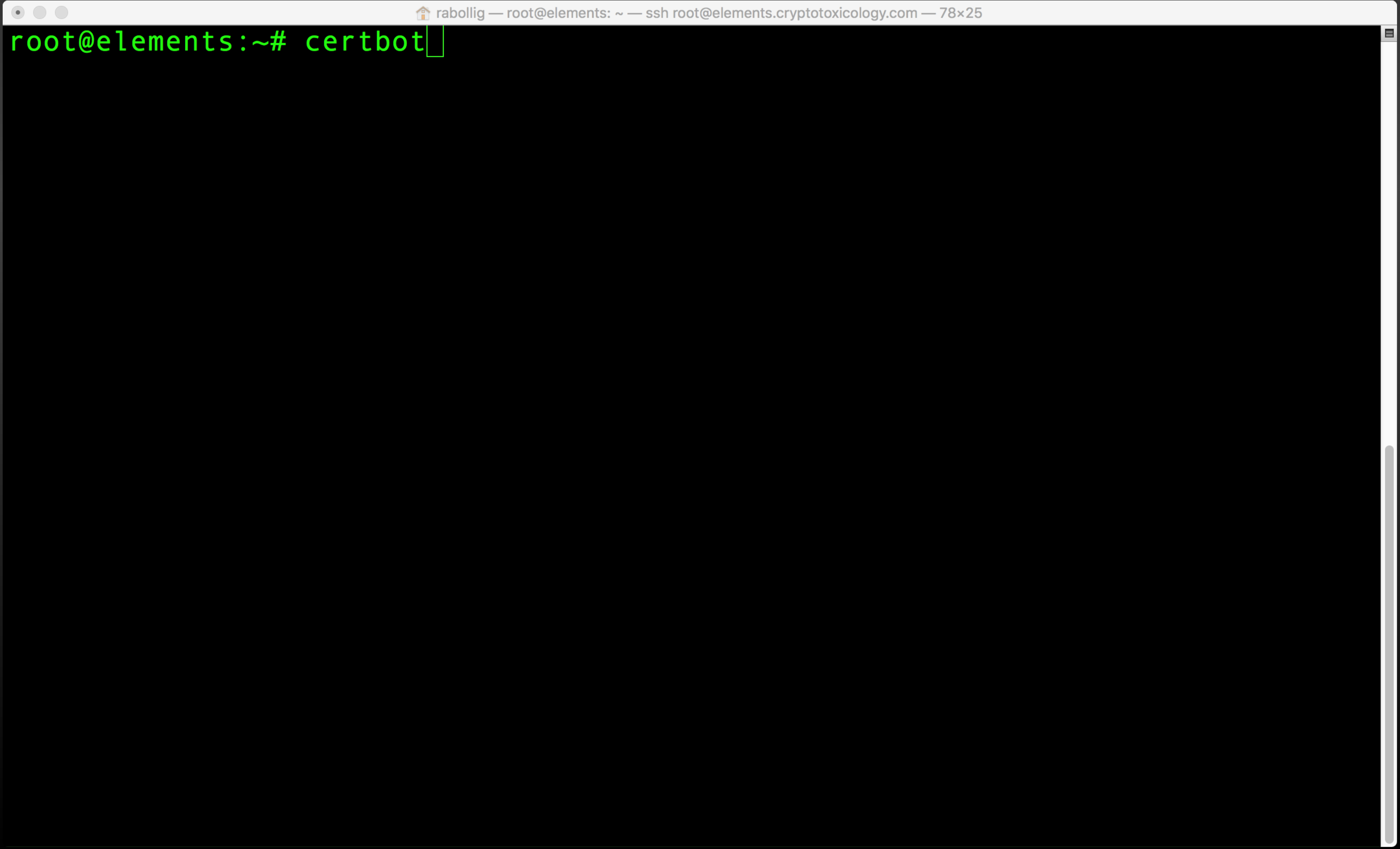
Certbot's DNS plugins which can be used to automate obtaining a wildcard certificate from Let's Encrypt's ACMEv2 server are not available for your OS yet. This should change soon but if you don't want to wait, you can use these plugins now by running Certbot in Docker instead of using the instructions on this page.

Get Started

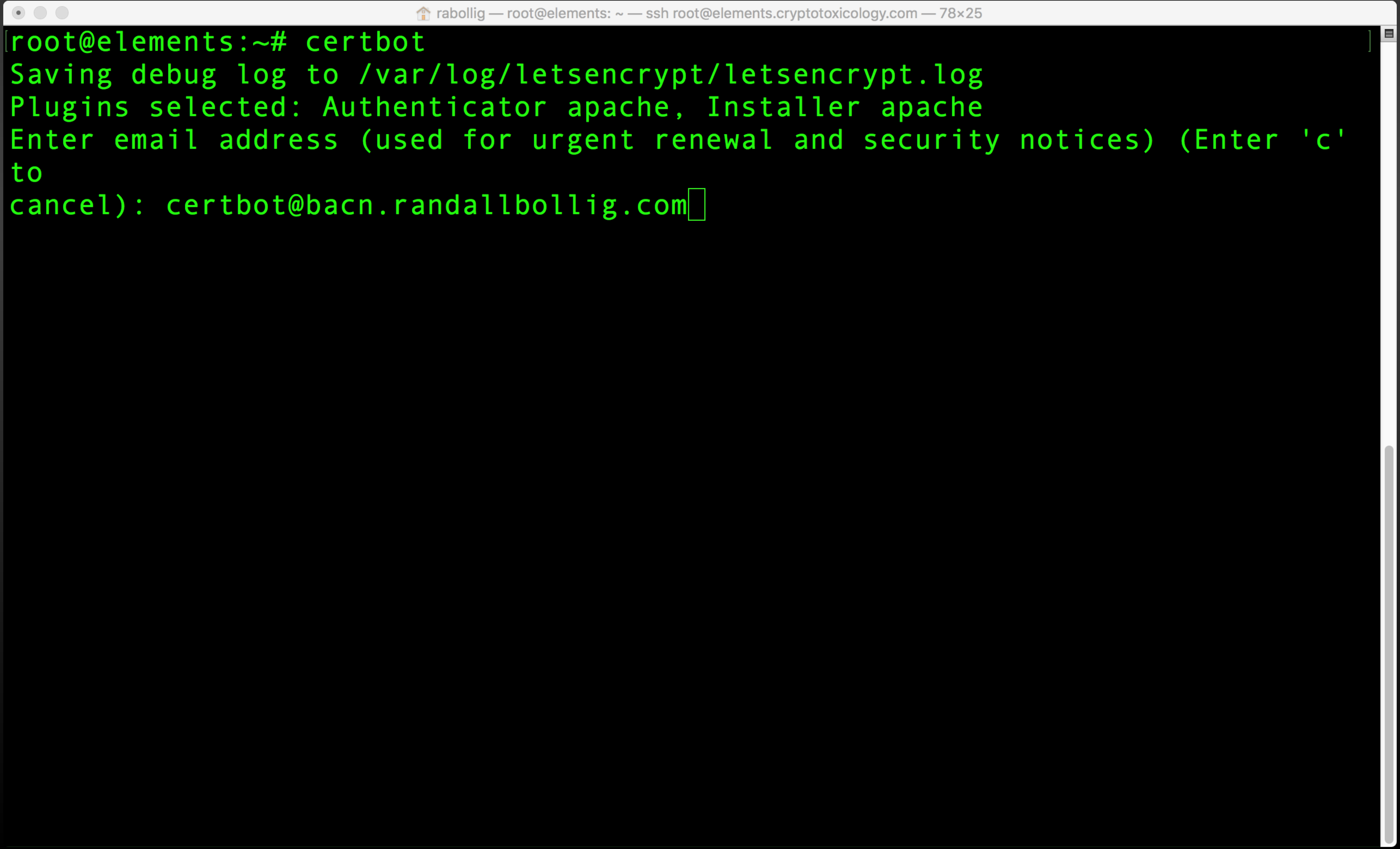
Certbot has a fairly solid beta-quality Apache plugin, which is supported on many platforms, and automates certificate installation.

```
$ sudo certbot --apache
```

Running this command will get a certificate for you and have Certbot edit your Apache configuration automatically to serve it. If you're feeling more conservative and would like to make the changes to your Apache configuration by hand, you can use the `certonly` subcommand:

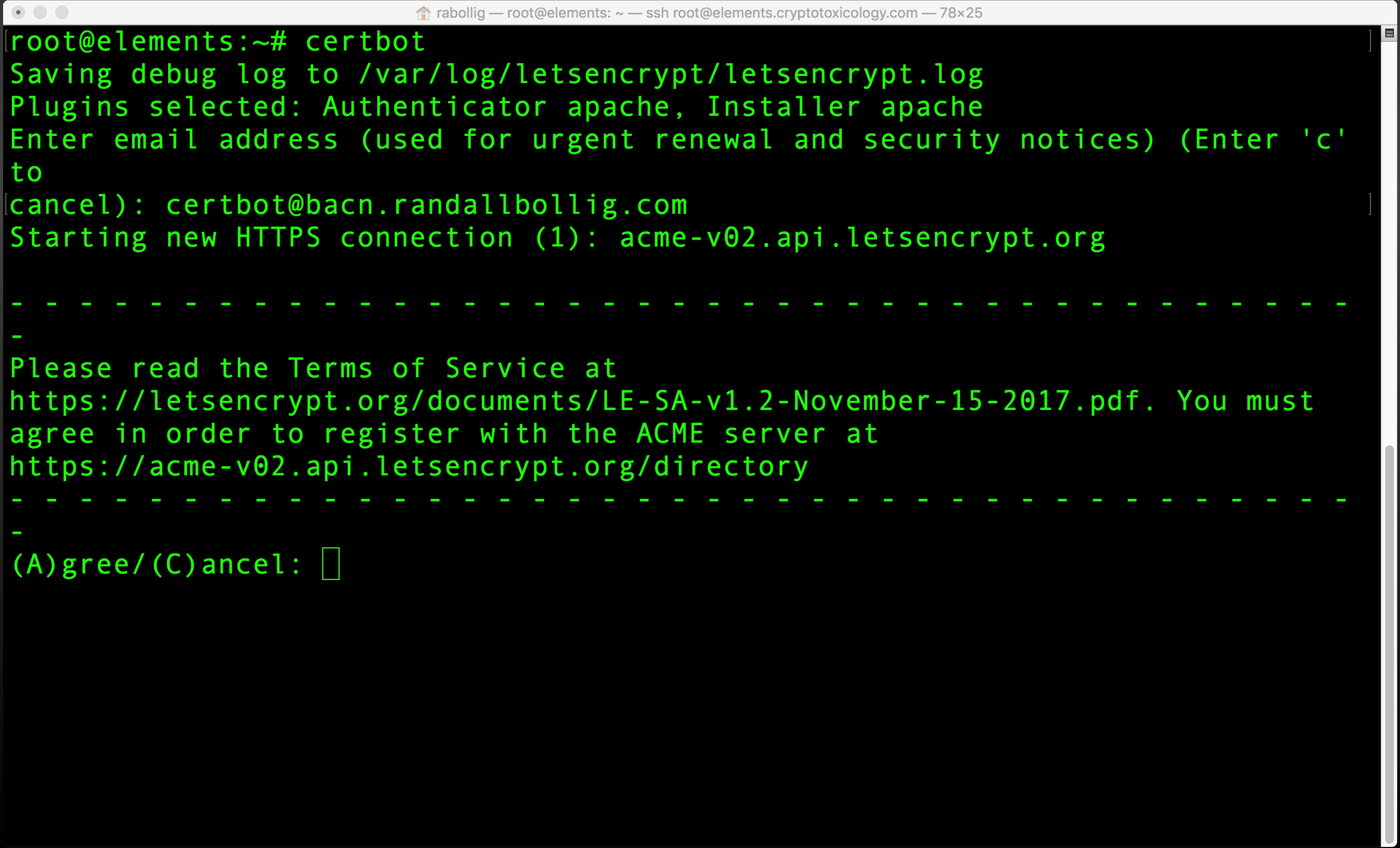

rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 78×25

```
root@elements:~# certbot
```



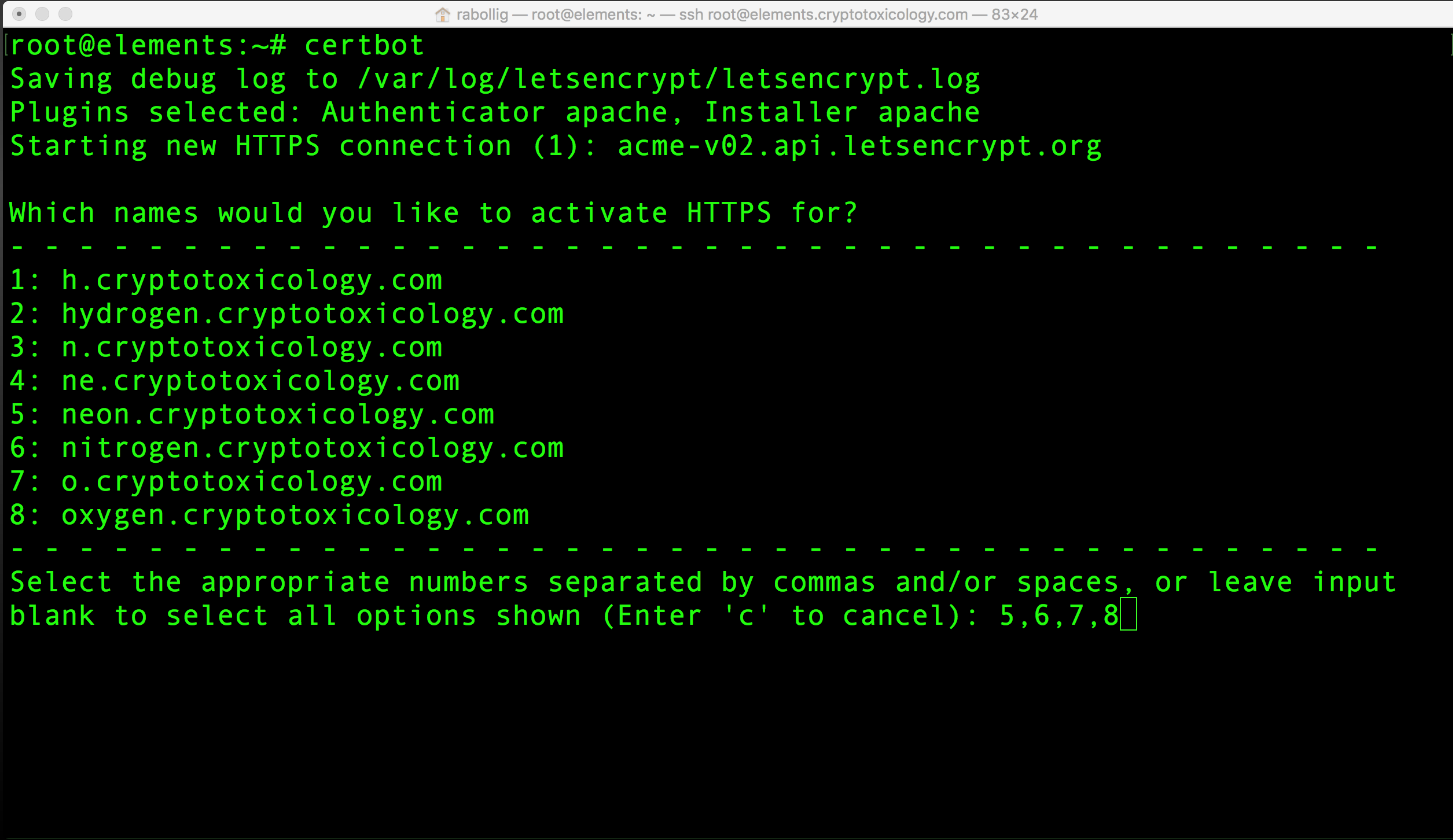
rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 78×25

```
root@elements:~# certbot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c'
to
cancel): certbot@bacn.randallbollig.com
```



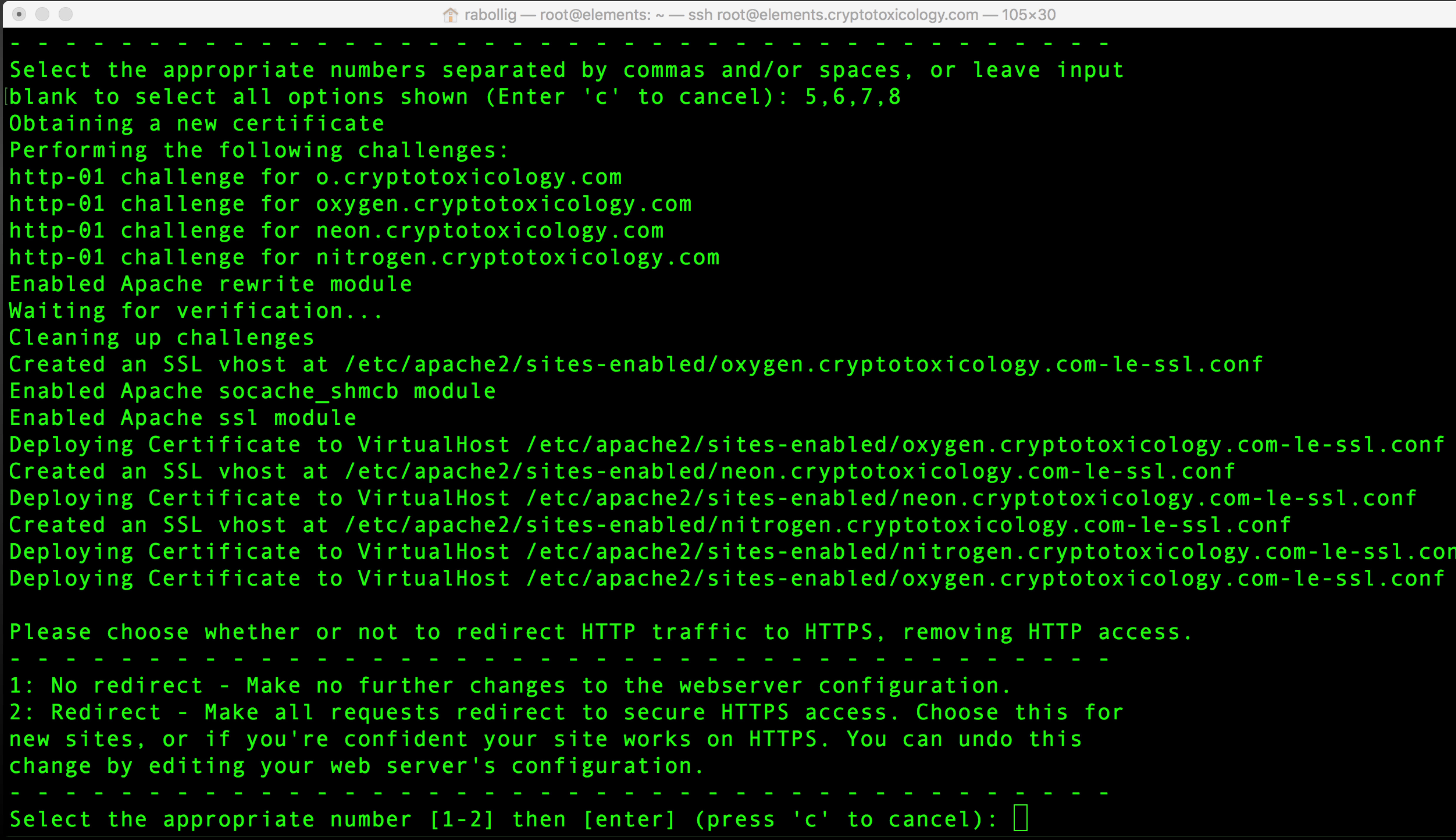
rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 78×25

```
root@elements:~# certbot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c'
to
cancel): certbot@bacn.randallbollig.com
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
(A)gree/(C)ancel: 
```

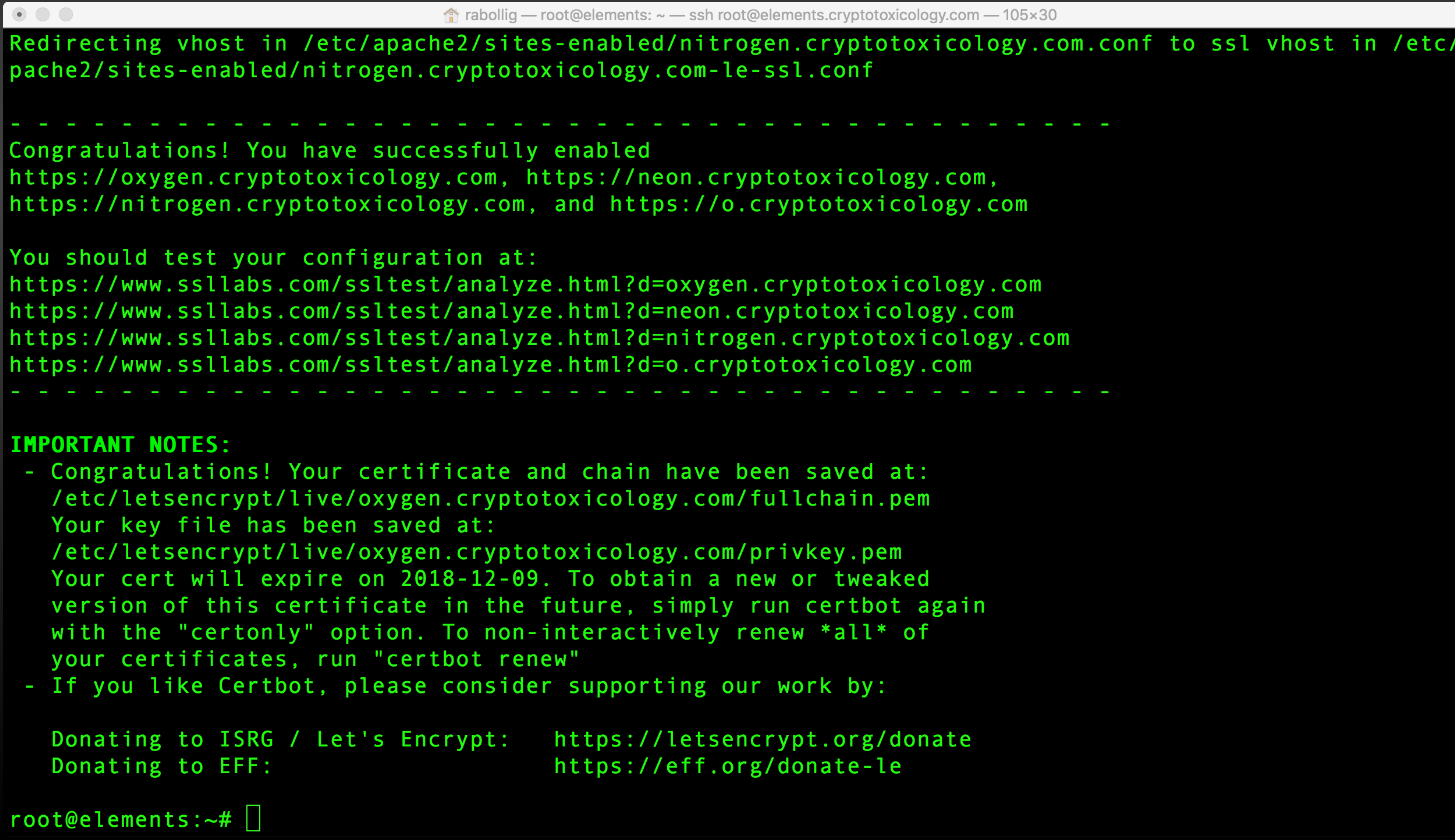


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 83×24

```
root@elements:~# certbot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: h.cryptotoxicology.com
2: hydrogen.cryptotoxicology.com
3: n.cryptotoxicology.com
4: ne.cryptotoxicology.com
5: neon.cryptotoxicology.com
6: nitrogen.cryptotoxicology.com
7: o.cryptotoxicology.com
8: oxygen.cryptotoxicology.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 5,6,7,8
```


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 5,6,7,8
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for o.cryptotoxicology.com
http-01 challenge for oxygen.cryptotoxicology.com
http-01 challenge for neon.cryptotoxicology.com
http-01 challenge for nitrogen.cryptotoxicology.com
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-enabled/oxygen.cryptotoxicology.com-le-ssl.conf
Enabled Apache socache_shmcb module
Enabled Apache ssl module
Deploying Certificate to VirtualHost /etc/apache2/sites-enabled/oxygen.cryptotoxicology.com-le-ssl.conf
Created an SSL vhost at /etc/apache2/sites-enabled/neon.cryptotoxicology.com-le-ssl.conf
Deploying Certificate to VirtualHost /etc/apache2/sites-enabled/neon.cryptotoxicology.com-le-ssl.conf
Created an SSL vhost at /etc/apache2/sites-enabled/nitrogen.cryptotoxicology.com-le-ssl.conf
Deploying Certificate to VirtualHost /etc/apache2/sites-enabled/nitrogen.cryptotoxicology.com-le-ssl.con
Deploying Certificate to VirtualHost /etc/apache2/sites-enabled/oxygen.cryptotoxicology.com-le-ssl.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
Redirecting vhost in /etc/apache2/sites-enabled/nitrogen.cryptotoxicology.com.conf to ssl vhost in /etc/
pache2/sites-enabled/nitrogen.cryptotoxicology.com-le-ssl.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled
https://oxygen.cryptotoxicology.com, https://neon.cryptotoxicology.com,
https://nitrogen.cryptotoxicology.com, and https://o.cryptotoxicology.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=oxygen.cryptotoxicology.com
https://www.ssllabs.com/ssltest/analyze.html?d=neon.cryptotoxicology.com
https://www.ssllabs.com/ssltest/analyze.html?d=nitrogen.cryptotoxicology.com
https://www.ssllabs.com/ssltest/analyze.html?d=o.cryptotoxicology.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/oxygen.cryptotoxicology.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/oxygen.cryptotoxicology.com/privkey.pem
   Your cert will expire on 2018-12-09. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

root@elements:~# 
```

nitrogen.crytotoxicology.com
nitrogen.cryptotoxicology.com
OK

DST Root CA X3
↳ Let's Encrypt Authority X3
↳ oxygen.cryptotoxicology.com

Key ID 89 DA 9C BB 9B BD 69 48 E4 B7 86 EF 64 3D 6A EB F8 76 6C 12

Extension Authority Key Identifier (2.5.29.35)
Critical NO
Key ID A8 4A 6A 63 04 7D DD BA E6 D1 39 B7 A6 45 65 EF F3 A8 EC A1

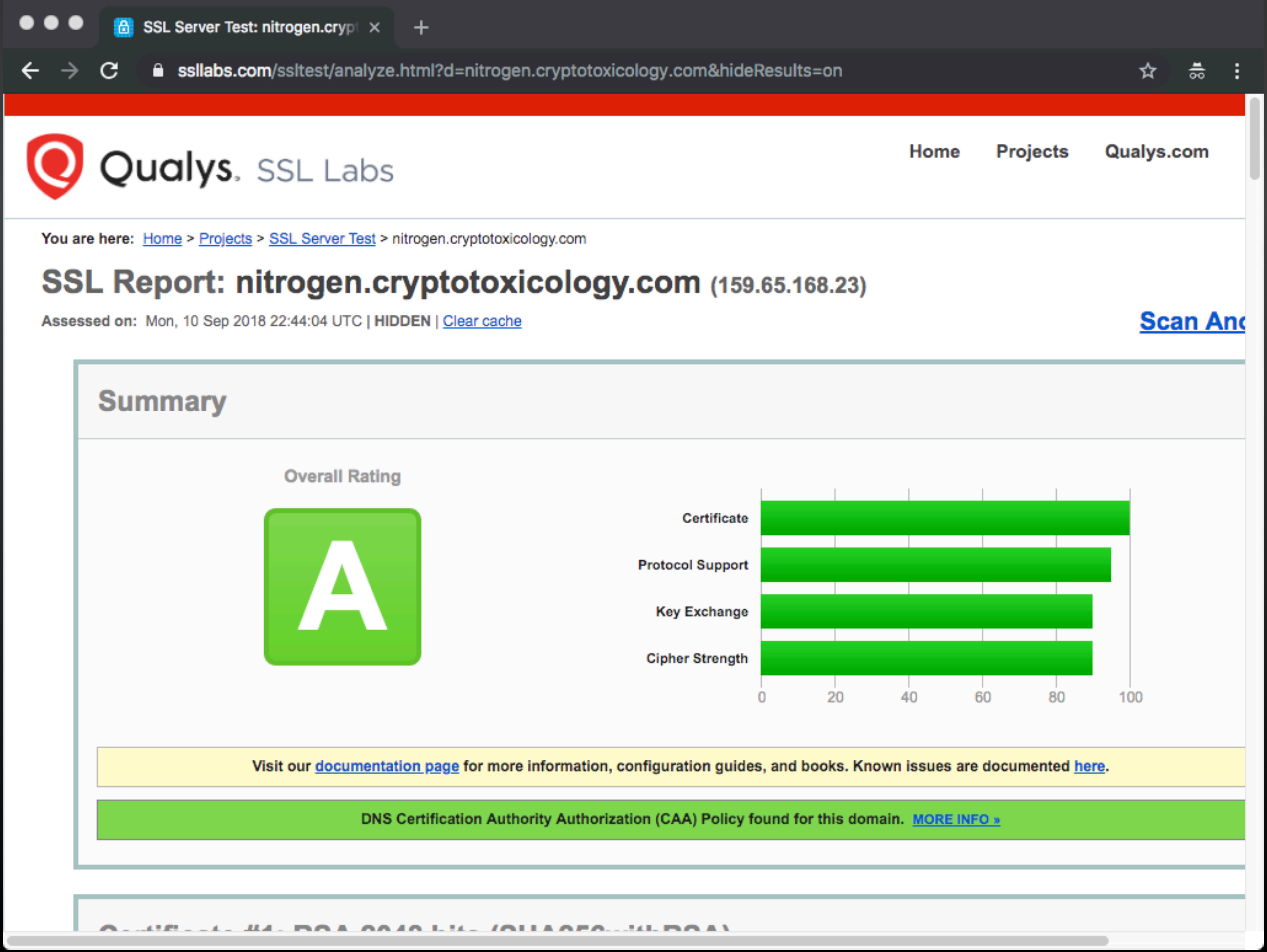
Extension Subject Alternative Name (2.5.29.17)
Critical NO
DNS Name neon.cryptotoxicology.com
DNS Name nitrogen.cryptotoxicology.com
DNS Name o.cryptotoxicology.com
DNS Name oxygen.cryptotoxicology.com

rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName oxygen.cryptotoxicology.com
        ServerAlias o.cryptotoxicology.com
        DocumentRoot /var/www/html
Include /etc/letsencrypt/options-ssl-apache.conf
SSLCertificateFile /etc/letsencrypt/live/oxygen.cryptotoxicology.com/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/oxygen.cryptotoxicology.com/privkey.pem
</VirtualHost>
</IfModule>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/apache2/sites-enabled/oxygen.cryptotoxicology.com-le-ssl.conf" 10L, 409C         1,1           All
```

rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
# This file contains important security parameters. If you modify this file
# manually, Certbot will be unable to automatically provide future security
# updates. Instead, Certbot will print and log an error message with a path to
# the up-to-date file that you will need to refer to when manually updating
# this file.

SSLEngine on

# Intermediate configuration, tweak to your needs
SSLProtocol             all -SSLv2 -SSLv3
SSLCipherSuite          ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES1
28-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES
128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECD
HE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE
-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES12
8-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
SSLHonorCipherOrder     on
SSLCompression          off

SSLOptions +StrictRequire

# Add vhost name to log entries:
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" vhost_combined
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common

#CustomLog /var/log/apache2/access.log vhost_combined
#LogLevel warn
#ErrorLog /var/log/apache2/error.log
                                                                                     23,1          Top
```



SSL Server Test: nitrogen.cryp
ssllabs.com/ssltest/analyze.html?d=nitrogen.cryptotoxicology.com&hideResults=on
Qualys. SSL Labs
Home
Projects
Qualys.com

You are here: Home > Projects > SSL Server Test > nitrogen.cryptotoxicology.com

SSL Report: nitrogen.cryptotoxicology.com (159.65.168.23)

Assessed on: Mon, 10 Sep 2018 22:44:04 UTC | HIDDEN | Clear cache

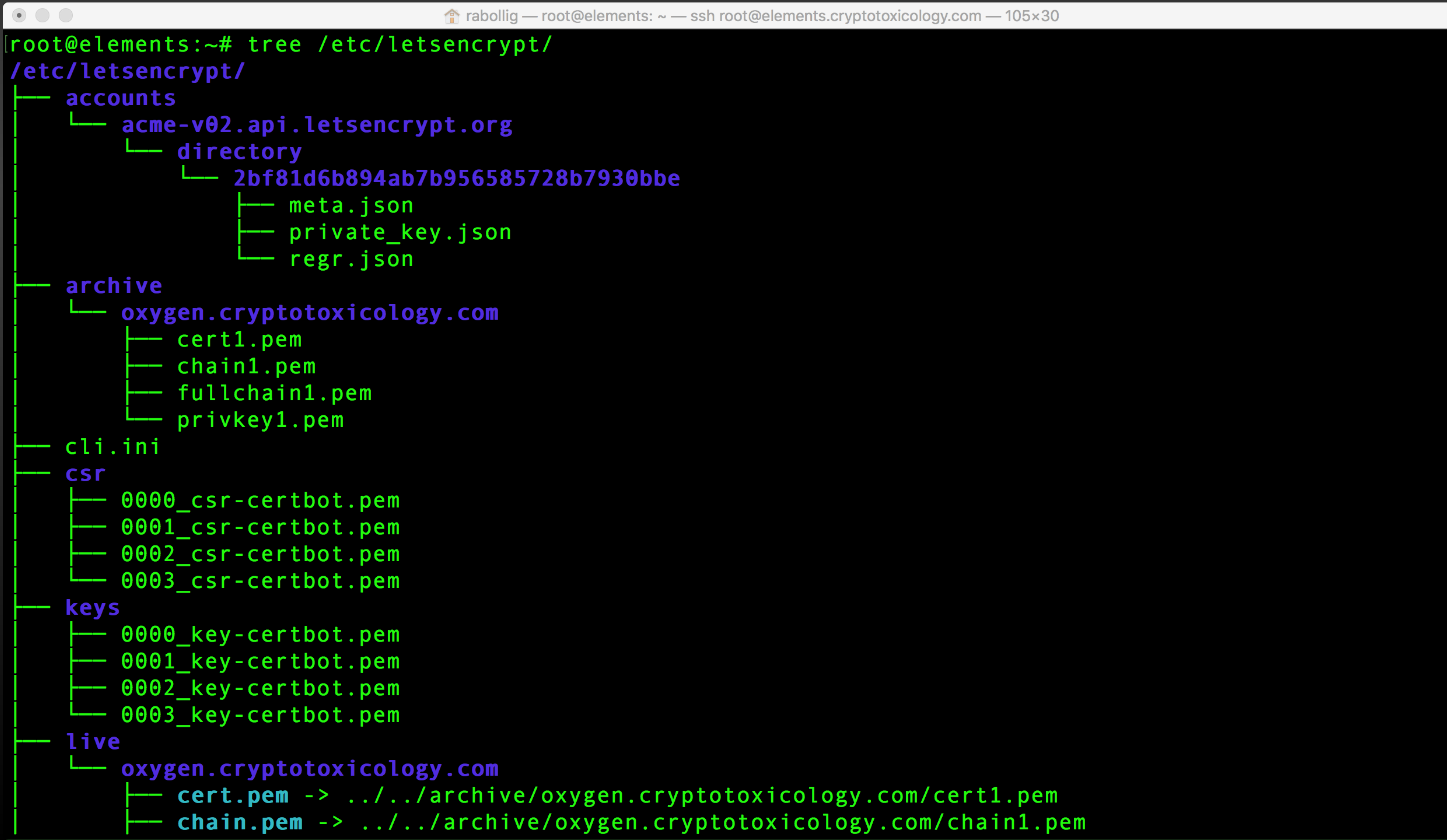
Scan Anc

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

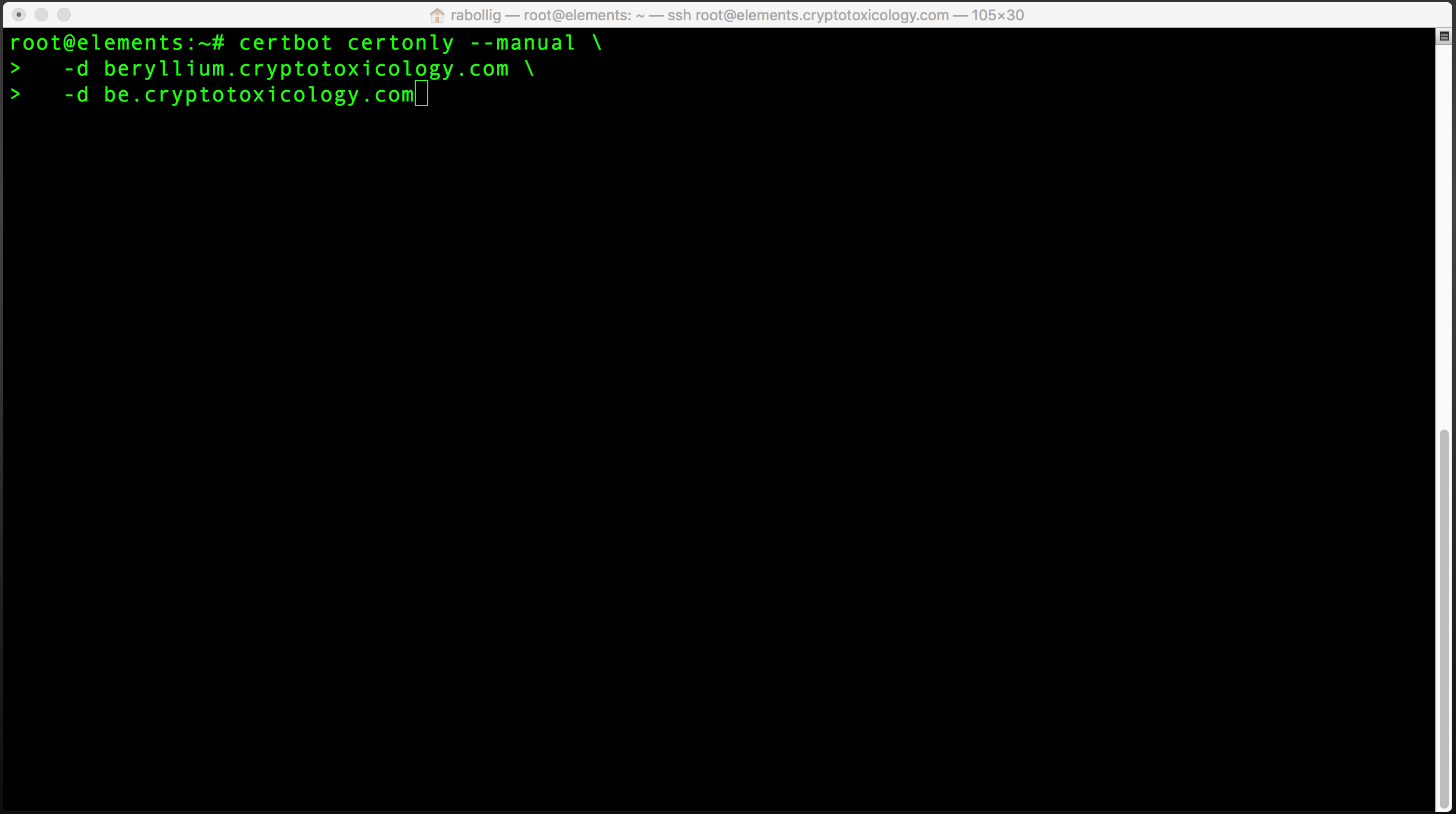


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
root@elements:~# tree /etc/letsencrypt/
/etc/letsencrypt/
├── accounts
│   └── acme-v02.api.letsencrypt.org
│       └── directory
│           └── 2bf81d6b894ab7b956585728b7930bbe
│               ├── meta.json
│               ├── private_key.json
│               └── regr.json
├── archive
│   └── oxygen.cryptotoxicology.com
│       ├── cert1.pem
│       ├── chain1.pem
│       ├── fullchain1.pem
│       └── privkey1.pem
├── cli.ini
├── csr
│   ├── 0000_csr-certbot.pem
│   ├── 0001_csr-certbot.pem
│   ├── 0002_csr-certbot.pem
│   └── 0003_csr-certbot.pem
├── keys
│   ├── 0000_key-certbot.pem
│   ├── 0001_key-certbot.pem
│   ├── 0002_key-certbot.pem
│   └── 0003_key-certbot.pem
├── live
│   └── oxygen.cryptotoxicology.com
│       ├── cert.pem -> ../../archive/oxygen.cryptotoxicology.com/cert1.pem
│       ├── chain.pem -> ../../archive/oxygen.cryptotoxicology.com/chain1.pem
```

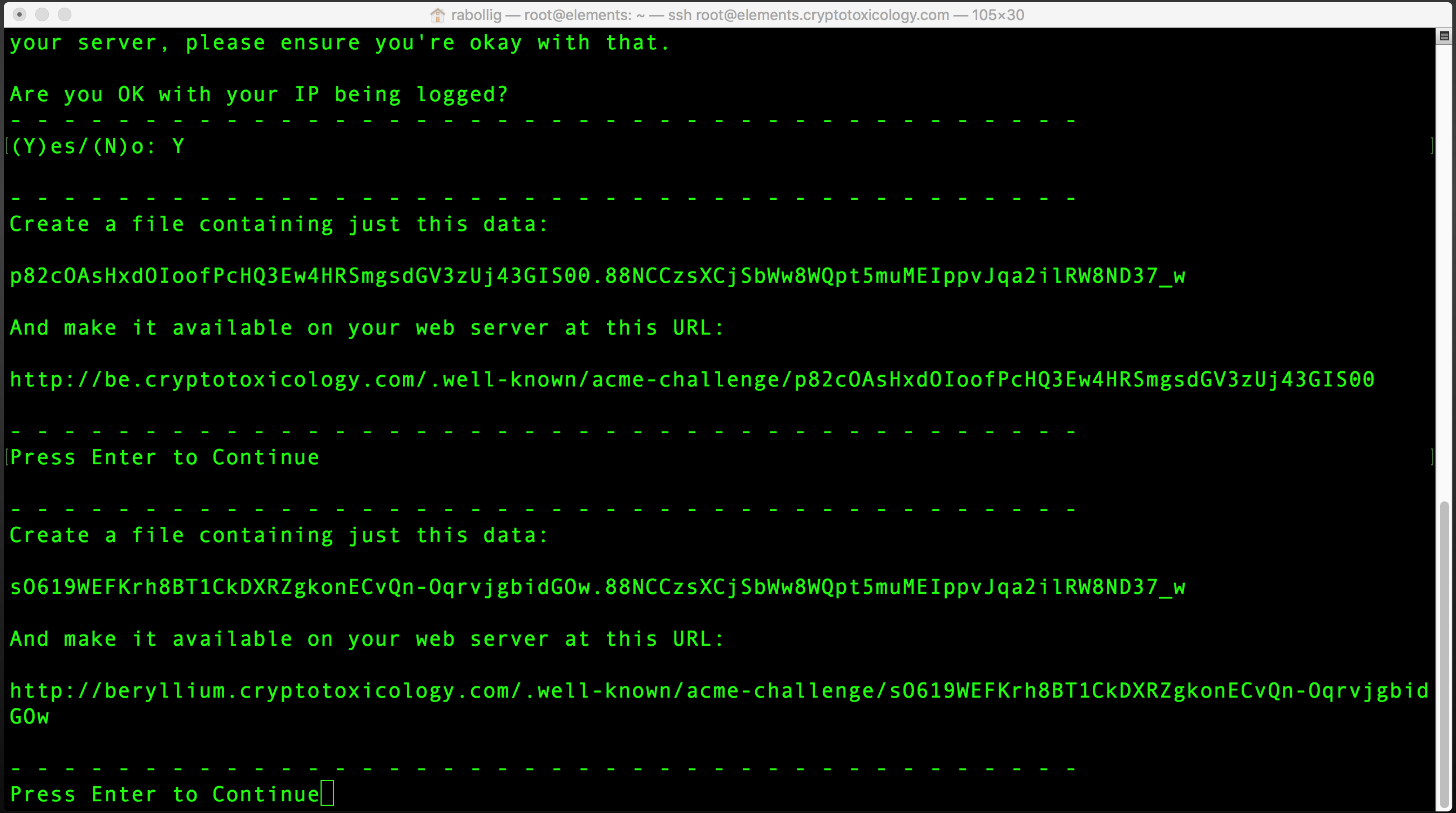
Any questions at this point?

Next we will walk through it manually and see what happens behind the scenes



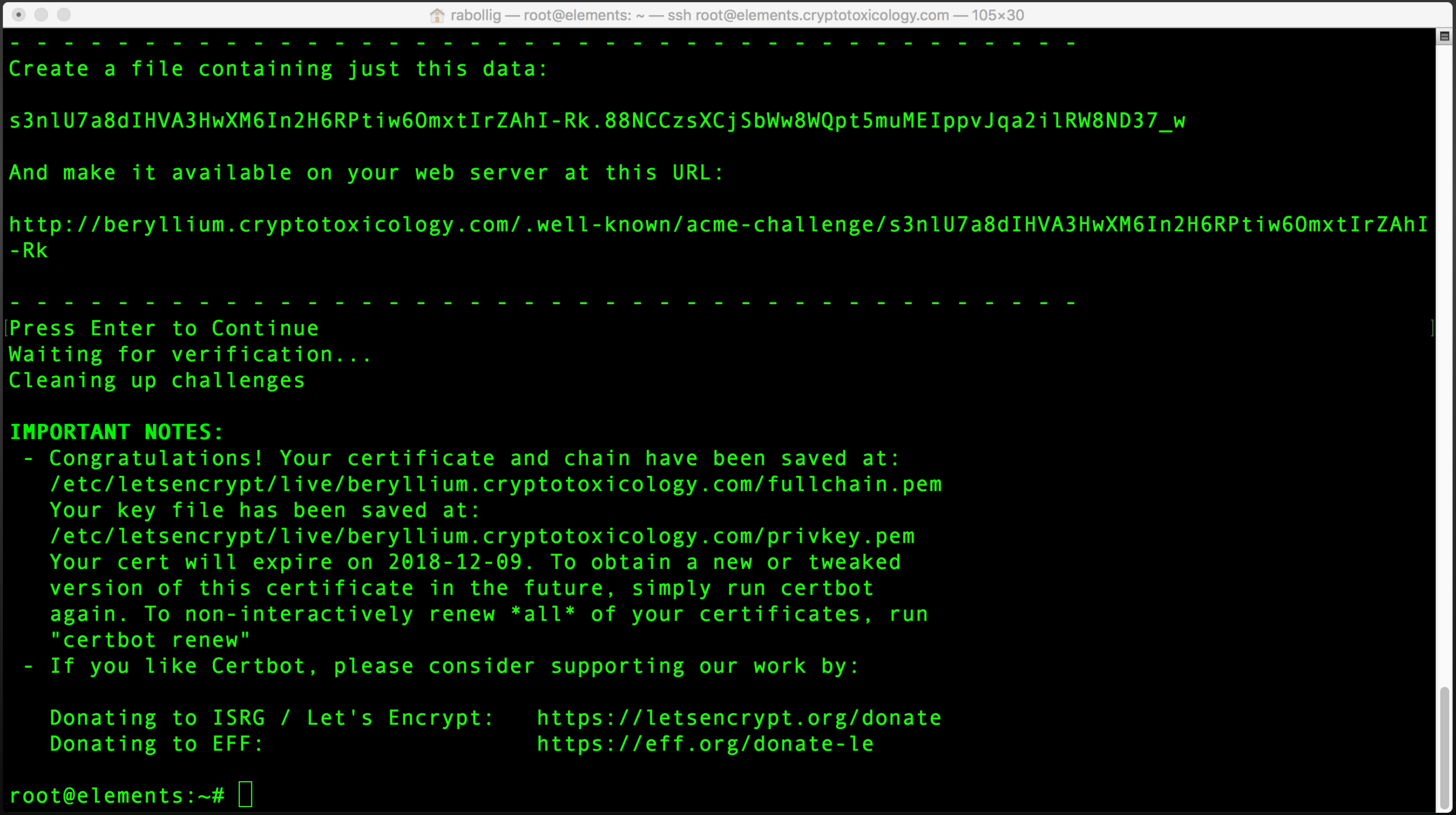
rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
root@elements:~# certbot certonly --manual \
>   -d beryllium.cryptotoxicology.com \
>   -d be.cryptotoxicology.com
```

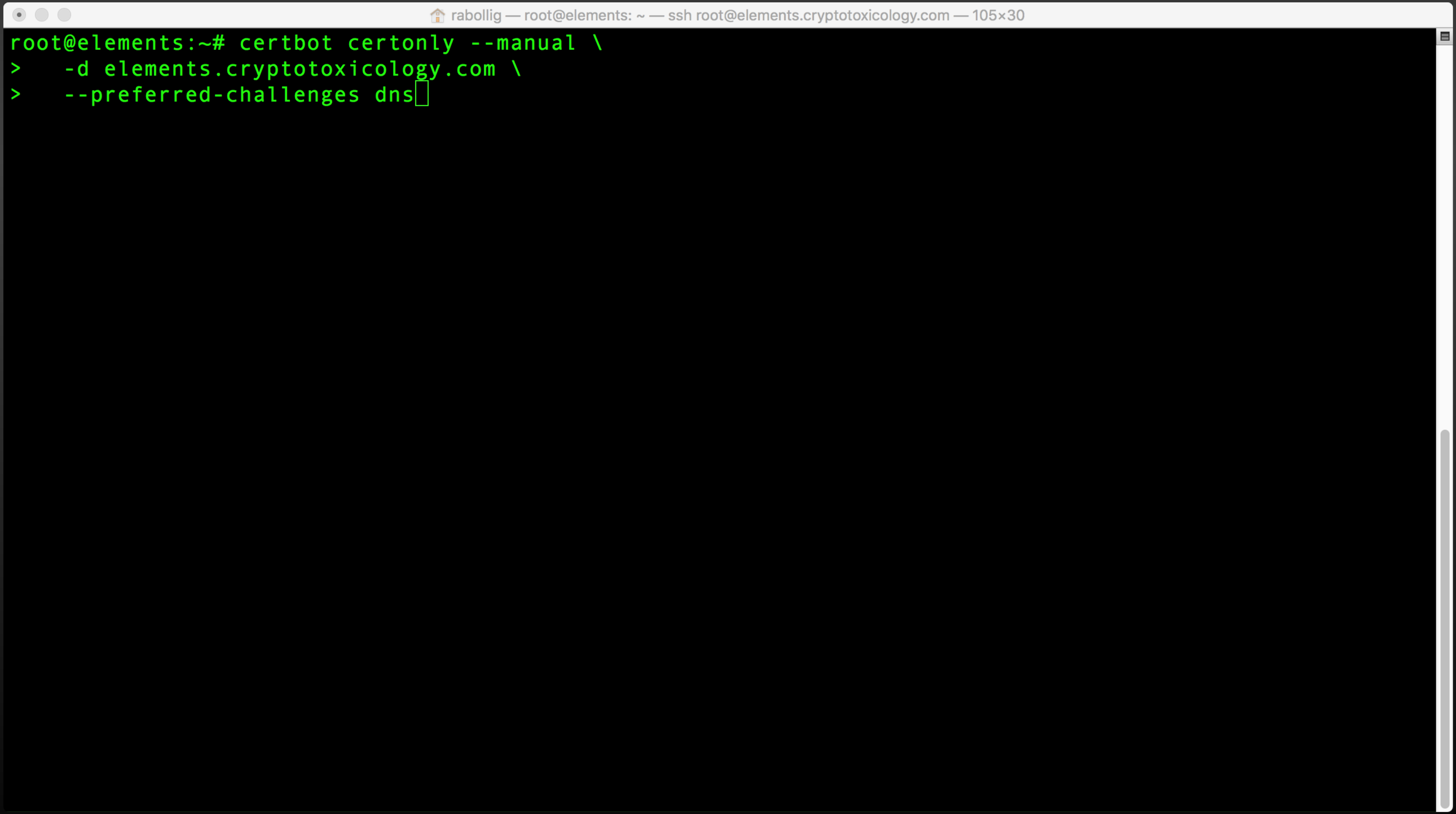


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Create a file containing just this data:

p82cOAsHxdOIoofPcHQ3Ew4HRSmgsdGV3zUj43GIS00.88NCCzsXCjSbWw8WQpt5muMEIppvJqa2ilRW8ND37_w

And make it available on your web server at this URL:

http://be.cryptotoxicology.com/.well-known/acme-challenge/p82cOAsHxdOIoofPcHQ3Ew4HRSmgsdGV3zUj43GIS00

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Create a file containing just this data:

sO619WEFKrh8BT1CkDXRZgkonECvQn-OqrvjgbidGOw.88NCCzsXCjSbWw8WQpt5muMEIppvJqa2ilRW8ND37_w

And make it available on your web server at this URL:

http://beryllium.cryptotoxicology.com/.well-known/acme-challenge/sO619WEFKrh8BT1CkDXRZgkonECvQn-Oqrvjgbid
GOw

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

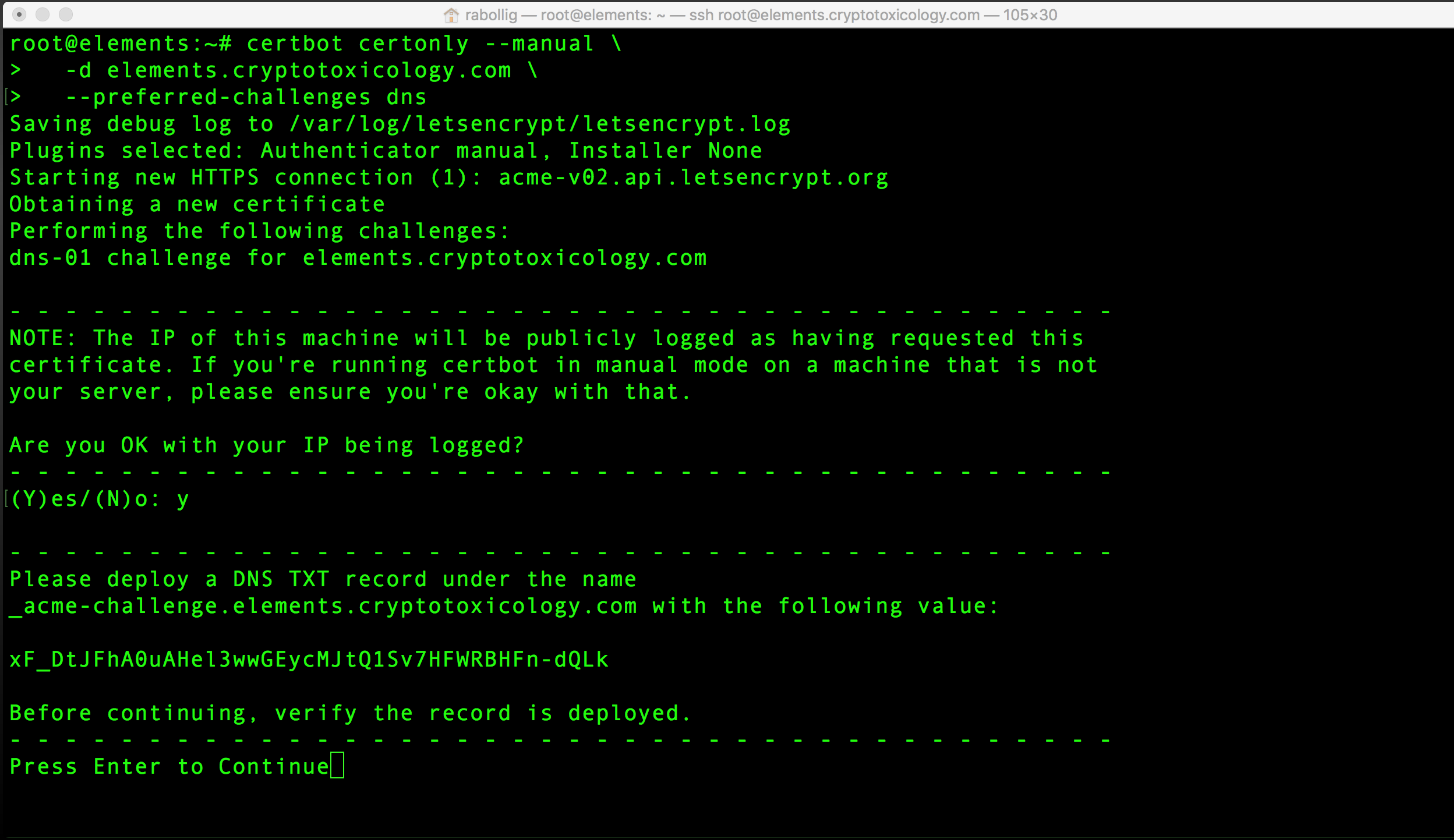

rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Create a file containing just this data:

s3nlU7a8dIHVA3HwXM6In2H6RPtiw6OmxtIrZAhI-Rk.88NCCzsXCjSbWw8WQpt5muMEIppvJqa2ilRW8ND37_w

And make it available on your web server at this URL:

http://beryllium.cryptotoxicology.com/.well-known/acme-challenge/s3nlU7a8dIHVA3HwXM6In2H6RPtiw6OmxtIrZAhI
-Rk

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/beryllium.cryptotoxicology.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/beryllium.cryptotoxicology.com/privkey.pem
   Your cert will expire on 2018-12-09. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

root@elements:~# 
```



rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
root@elements:~# certbot certonly --manual \
>   -d elements.cryptotoxicology.com \
>   --preferred-challenges dns
```


rabollig — root@elements: ~ — ssh root@elements.cryptotoxicology.com — 105×30

```
root@elements:~# certbot certonly --manual \
>   -d elements.cryptotoxicology.com \
>   --preferred-challenges dns
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for elements.cryptotoxicology.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.

Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.elements.cryptotoxicology.com with the following value:

xF_DtJFhA0uAHel3wwGEycMJtQ1Sv7HFWRBHFn-dQLk

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

Wildcard Certificates

- DNS Verification only
- Just ask for *.domain.tld
- Also ask for .domain.tld
- *.*.domain.tld is different than *.domain.tld

Configuring Load Balancers

- Port /.well-known/ to a single node
- Use DNS01 verification
- Be aware of rate limits if nodes are keyed differently

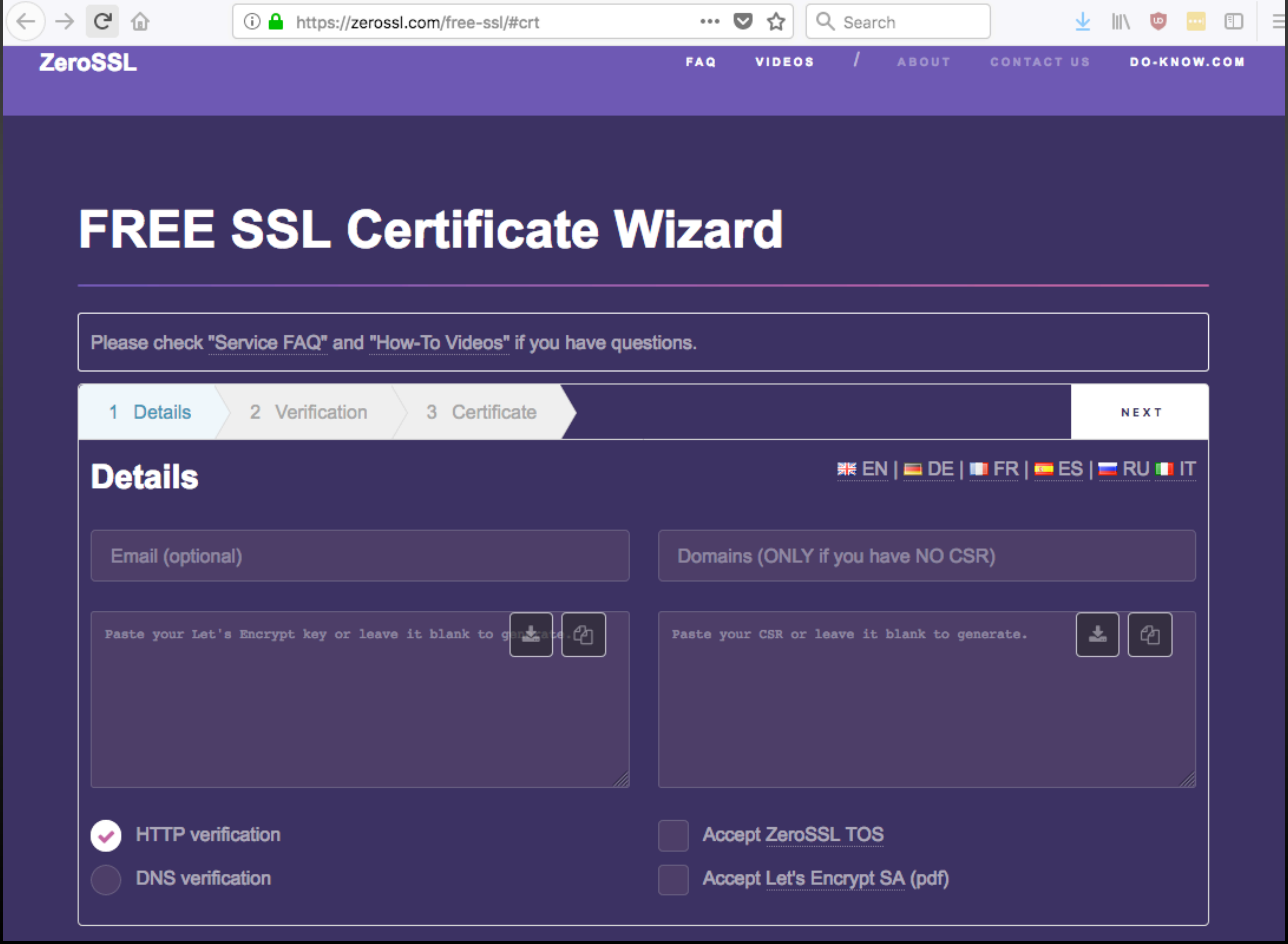
Limitations

- Certs good for 90 days
- Rate limits (50 certs/domain/week, 100 hosts/cert, 20-40 requests/second, 300 pending, 500 accounts/IP/3-hours, no limit on renewals)
- No EV certs

Personal
Open source
Business
Explore
Pricing
This repository
Search
Sign in or Sign up
analogic / lescript
Watch 11
Star 176
Fork 26
Code
Issues 5
Pull requests 2
Projects 0
Pulse
Graphs

Simplified PHP ACME client

```php
<?php

require 'Lescript.php';
try {
    $le = new Analogic\ACME\Lescript('/certificate/storage', '/var/www/test.com');
    $le->contact = array('mailto:test@test.com'); // optional
    $le->initAccount();
    $le->signDomains(array('test.com', 'www.test.com'));
} catch (\Exception $e) {
    $logger->error($e->getMessage());
    $logger->error($e->getTraceAsString());
}
```



FREE SSL Certificate Wizard

Please check "Service FAQ" and "How-To Videos" if you have questions.

Details

Email (optional)

Domains (ONLY if you have NO CSR)

Paste your Let's Encrypt key or leave it blank to generate.

Paste your CSR or leave it blank to generate.

● HTTP verification

○ DNS verification

□ Accept ZeroSSL TOS

□ Accept Let's Encrypt SA (pdf)

The HTTP/2 web server with automatic HTTPS

Serve The Web Like It's 2017

Commercial CA Reactions

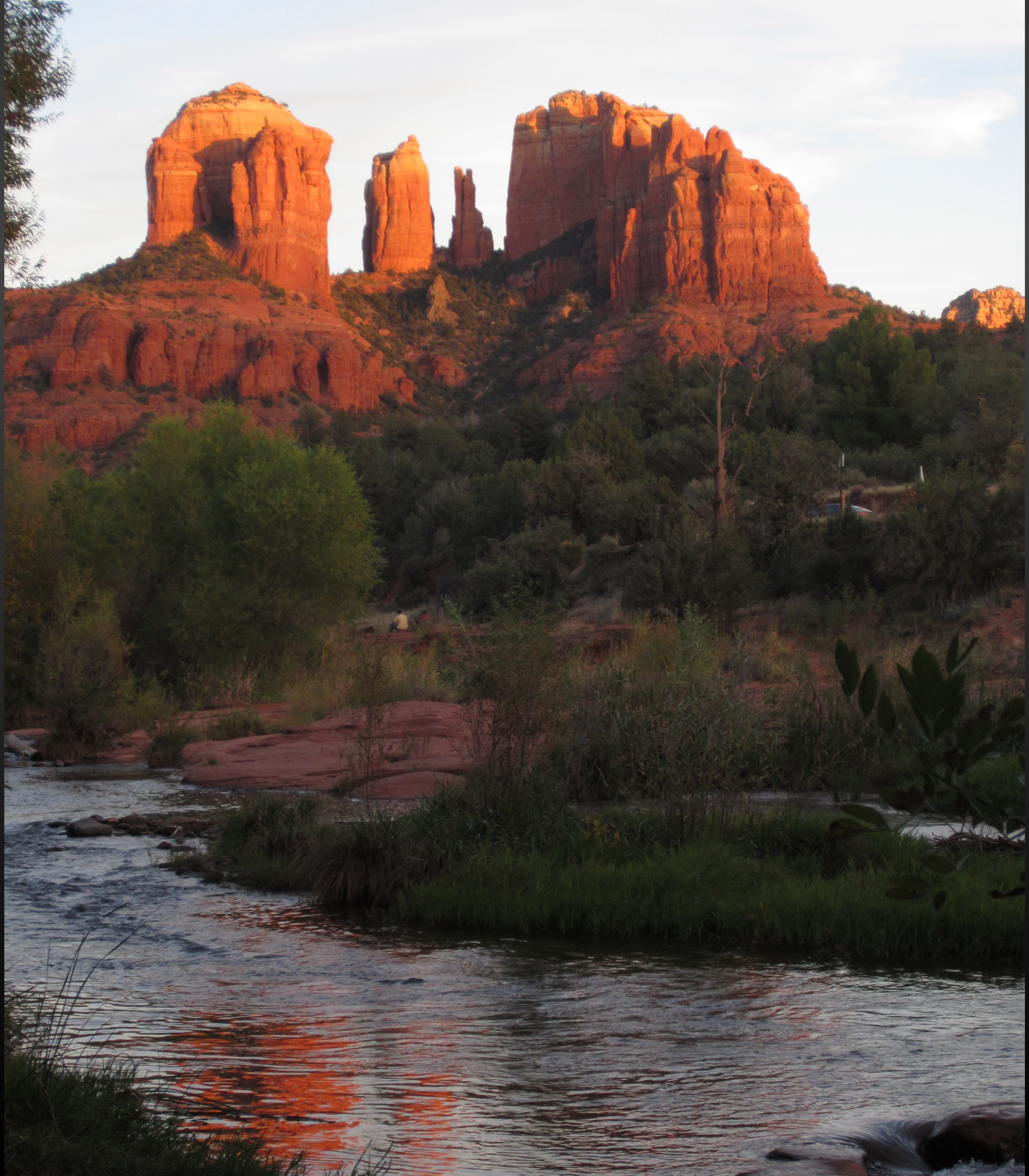
- Most of the certificates being issued are for sites that did not have certificates to begin with (not eroding market share)

- OV, EV, and wildcard certificates are the actual money-makers.   With DV certs racing to the bottom

- Customized certs

Alternative Free CAs

- Amazon - Available on Elastic Load Balancer (ELB) and CloudFront *
- CDNs - SAN certificates *
- Test products from commercial CAs



That’s All, Folks!

randall@codeknights.com
https://www.codkenights.com/presentations/

RANDALL BOLLIG

This presentation is in no way associated with Let’s Encrypt nor the Internet Security Research Group. It does not represent the opinion of Randall’s clients or employer.

Keep circulating the tapes.

Deep Dive into Let’s Encrypt

Contact Randall at randall@codeknights.com

Slides, captions, and transcript available at:
https://codeknights.com/presentations/