

1. What is the purpose of Certificate Authority?

Certificate Authority issues SSL certificates. They are an organization that acts to validate identities and bind them to cryptographic key pairs with digital certificates.

2. What color is this?

```
01010011 01100101 01100001 00100000 01000110 01101111 01100001
01101101 00100000 01000111 01110010 01100101 01100101 01101110
```

Sea Foam Green

ASCII text

Sea Foam Green

Hex (bytes)

53 65 61 20 46 6F 61 6D 20 47 72 65 65 6E

Binary (bytes)

```
01010011 01100101 01100001 00100000 01000110 01101111
01100001
01101101 00100000 01000111 01110010 01100101 01100101
01101110
```

Was this message encrypted or encoded?

Encoded

3. Put these encryption schemes in order from least to most secure:
- Vigenere
 - DES
 - RSA
 - Caesar

The easiest way to figure this out is to put them in historical order:

- Caesar
- Vigenere
- DES
- RSA

4. What is the name of the Root CA Certificate used by the Smithsonian Museum's website? What top-level domain does their website use?

Search for the Smithsonian Museum and find their domain which is si.edu. Visit the site and view the certificate info:

Certificate

si.e...	Entrust Certification Authority - L1K	Entrust Root Certification Authority - G2
Subject Name		
Country	US	
Organization	Entrust, Inc.	
Organizational Unit	See www.entrust.net/legal-terms	
Organizational Unit	(c) 2009 Entrust, Inc. - for authorized use only	
Common Name	Entrust Root Certification Authority - G2	
Issuer Name		
Country	US	
Organization	Entrust, Inc.	
Organizational Unit	See www.entrust.net/legal-terms	
Organizational Unit	(c) 2009 Entrust, Inc. - for authorized use only	
Common Name	Entrust Root Certification Authority - G2	

Its Common Name is Entrust Root Certification Authority - G2. It uses a .edu TLD.

5. Answer this question:

V2hhdCBjb2xvciBpcyB0aGU3RhdHV1IG9mIExpYmVydHk/IA==

We can tell it is base64 because of the "==" at the end. Drop it in a decoder:

ASCII text

What color is the Statue of Liberty?

Hex (bytes)

Binary (bytes)

Decimal (bytes)










Base64

V2hhdCBjb2xvciBpcyB0aGUgU3Rh dHVlIG9mIExpYmVydHk/IA==


It is green

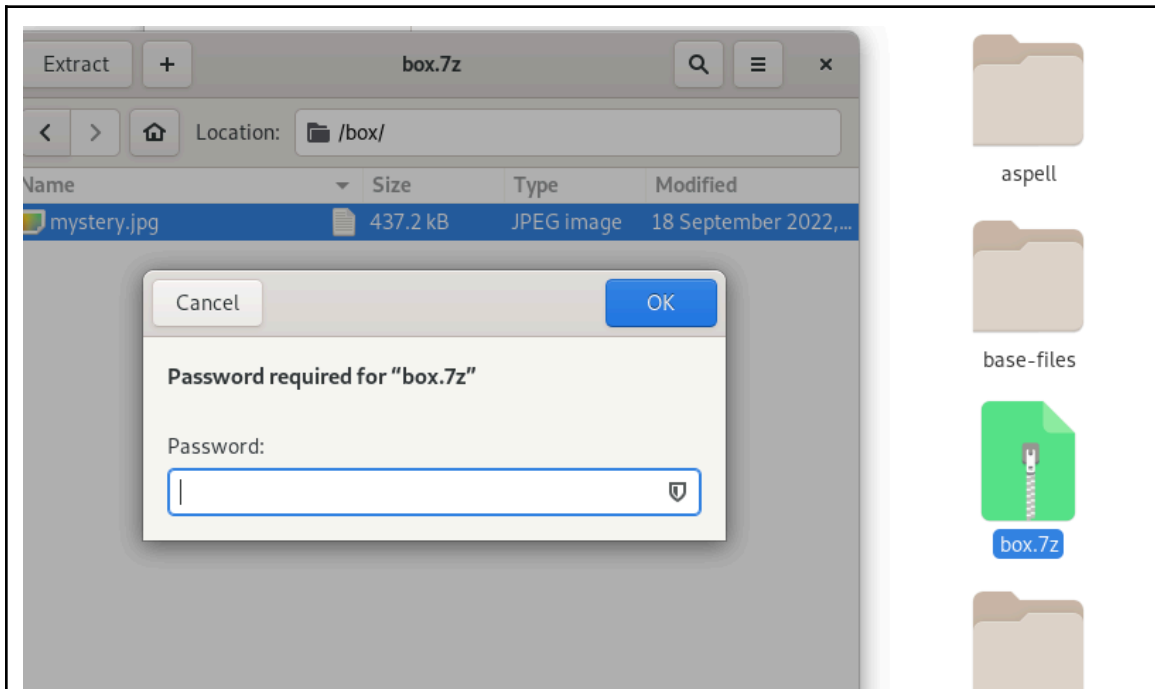
6. There is a zip file located at **/usr/share/box.7z**. Its password is encoded in the maritime signal flags in your Pictures directory. Hint: Read from bottom to top. What is in the box?

Search maritime signal flags and open the image.

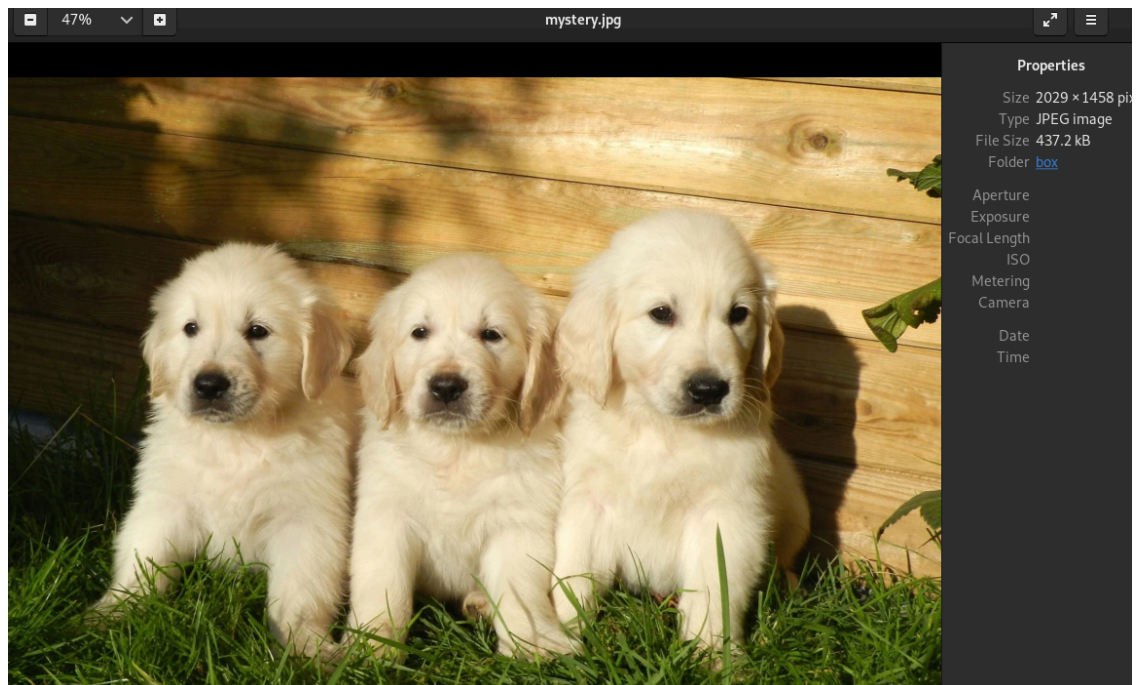
phonetic name	Flag	Blazon	ICS meaning as single flag	with numeric complements
A Alfa		Swallowtailed, per pale argent and azure	"I have a diver down; keep well clear at slow speed."	Azimuth or bearing
B Bravo		Swallowtailed, gules	"I am taking in or discharging or carrying dangerous goods." (Originally used by the Royal Navy specifically for military explosives.)	
C Charlie		Azure, a fess gules fimbriated argent	"Affirmative." ^{[A][B]}	Course in degrees magnetic
D Delta		Or, a Spanish fess azure	"Keep clear of me; I am maneuvering with difficulty." ^[A]	Date
E Echo		Per fess azure and gules	"I am altering my course to starboard." ^[B]	
F Foxtrot		Argent, a lozenge throughout gules	"I am disabled; communicate with me." ^[C]	
G Golf		Paly of six or and azure	"I require a pilot." ^[D] By fishing vessels near fishing grounds: "I am hauling nets."	Longitude (The first 2 or 3 digits denote degrees; the last 2 denote minutes.)
H Hotel		Per pale argent and gules	"I have a pilot on board." ^[B]	
I India		Or, a pellet	"I am altering my course to port." ^[B]	
J Juliet		Per pale argent and gules	"I am on fire and have dangerous cargo on board; keep well clear of me."	

Read them from bottom to top and then read **abc1def2ghi3jk** This is our password. Now go find the .7z file and try to open it:





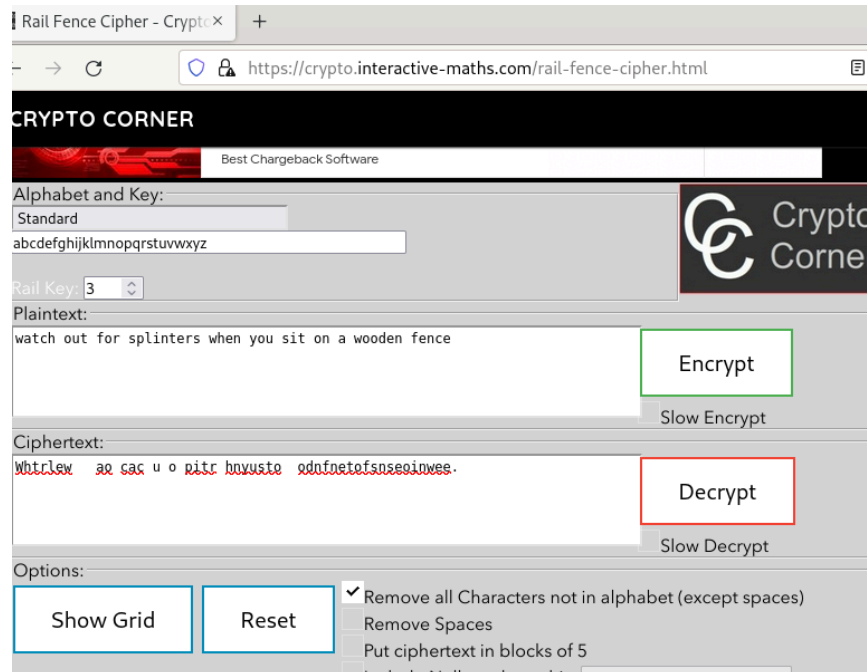
Enter the password.



The answer is puppies.

- What do I need to watch out for? I am really on the **fence** about showing you this encoded message. I think you can handle it: **Whtrlew ao cac u o pitr hnyusto odnfnetofsnseooinwee.**

This is a rail fence cipher. Find a rail fence cipher solver online. This is the default three rails and no offset.



You should watch out for splinters.

8. What time is it?

REFTSCBET1RET1QgREFTSERBU0ggRE9UCkRBU0ggREFTSERBU0hEQVNICKRBU0hEQ
 VNIIERPVERBU0ggREFTSERPVERBU0ggRE9UCkRBU0ggRE9URE9URE9URE9UIERPVA
 pEQVNIRE9URE9UIERBU0hEQVNIREFTSCBEQVNIRE9UIERPVERPVERBU0ggREFTSCB
 ET1RET1RET1Q=

This is more base64. Drop it in a decoder, and we see this:

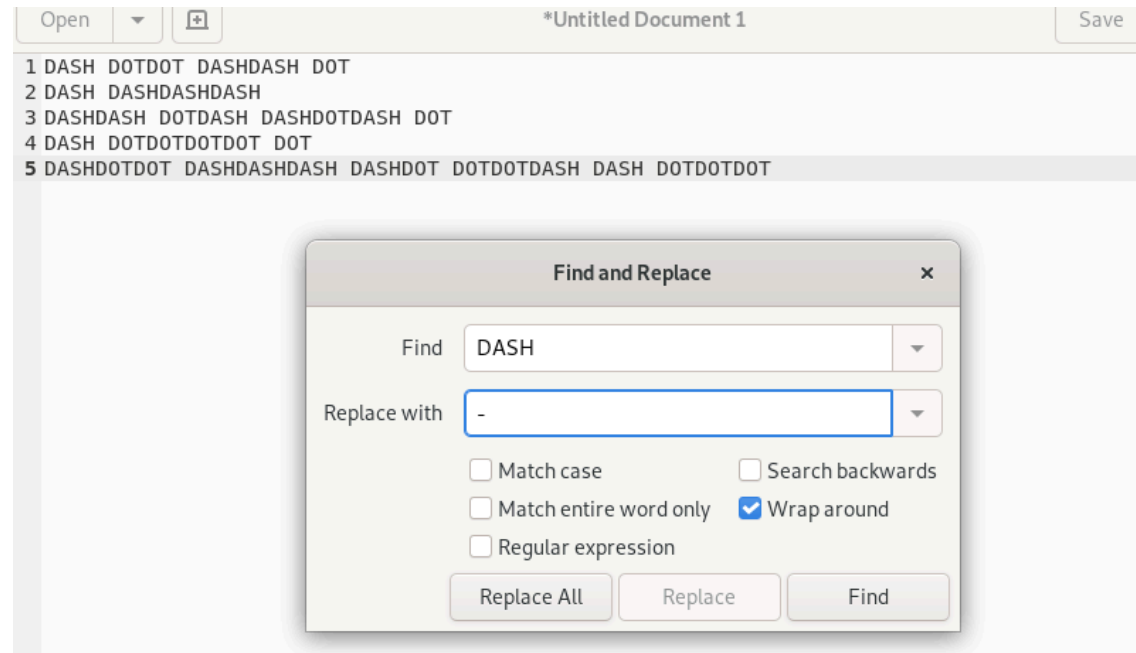
ASCII text

```

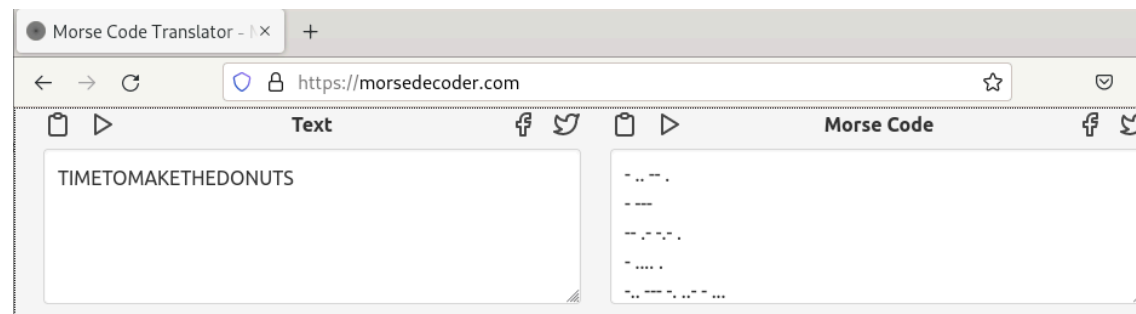
DASH DOTDOT DASHDASH DOT
DASH DASHDASHDASH
DASHDASH DOTDASH DASHDOTDASH DOT
DASH DOTDOTDOTDOT DOT
DASHDOTDOT DASHDASHDASH DASHDOT DOTDOTDASH DASH DOTDOTDOT
  
```

Hex (bytes)

This will need some conversion before it can be decoded, but we can tell it is morse code. You can do it by hand or with a find/replace in a text editor.



Find an online morse code translator:



Time to make the donuts.

- There is a One Time Pad located here: **/usr/share/code.png**. Use it to decipher this message: **CZ3FULJE70GSFH**

The file is a QR code. This should be easy since we have seen one before. Use a smartphone to read the code. It says <http://review3.candy.net>. Visit the page:
We see a simple web page:

Review 3
+

← → ↻
review3.candy.net

Review 3 Assets

- [One Time Pad](#)
- [Secret CSR](#)
- [chainbundle.pem](#)

Open the One Time Pad:

review3.candy.net/one-time-×
+

← → ↻
review3.candy.net/one-time-pad.txt

```

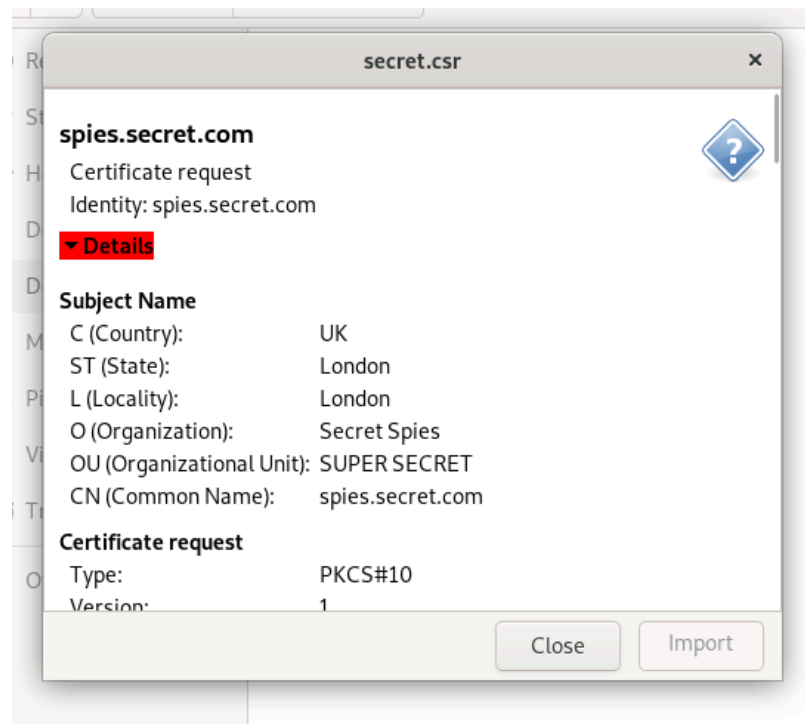
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 _ . ! ?
-----
4 1 R 3 5 T A D 6 J 2 M Y 0 C I G 0 ? Q K W Z B 7 N ! _ E F 9 U S 8 . V P X L H
5 K 3 M . N H 0 V _ C L ! Z B 4 R X Q I A 6 7 S D P W 0 9 ? G T J 2 8 Y 1 E U F
? T 3 . H V 4 A 0 G Q 6 2 J U ! S Z W L R M 0 _ N 8 B P X 5 C I 7 K D 9 E Y F 1
B N _ C F K 6 5 X 1 H E 0 U 0 ! D Q V 9 Y . G 3 W ? M Z A 2 S I J L R P 4 T 7 8
Y K C 3 . I 7 ! 1 L P 4 Q D 0 5 E B G S 6 8 ? Z 0 T W X A J M R _ N 2 H U F 9 V
K J R Y 1 9 5 G L . 7 U Z H I C 2 M 0 S ? 6 X 8 D F P 0 E _ ! A T B Q 4 W 3 N V
L N U ? 1 I . 8 6 S T K 0 P 2 4 3 A J 9 7 E B X M 0 Q W Z F ! _ G Y R 5 C D V H
N ! S ? D X 7 P . W C V R 0 F M L Y 1 U 8 B 4 H 5 I 3 A 0 J 9 2 Z 6 G _ E K T Q
0 I L T 7 Q ! G N 5 C U 3 J 4 8 R 0 6 1 9 X B H S 2 . F V P M A ? E K Y Z _ D W
P 7 L ! Y S A 8 0 E J D . 0 ? R 9 B Q G M K I C _ V U 1 F 6 X W 3 5 4 2 N Z H T
Q 6 W Y 0 4 1 D R E N C S 5 G Z _ T F 3 I 8 L 0 7 A J ! B H 2 9 ? V . U M K P X
Q 0 9 J H ? 7 ! K X T Z 8 W R C U 4 I Y S A _ L B 5 G M 2 1 N 0 E P 3 V 6 D F .
Q U 2 0 V 0 F Y S M _ T 3 X B 8 9 E . R ? 4 H N 6 D K Z A ! 5 I 1 C P W J L G 7
S G E R 8 A 3 H 1 ? V Y N B T X I 4 ! W 9 _ M Q C 0 0 F U K 2 J D Z 5 P . 6 L 7
N ! S ? D X 7 P . W C V R 0 F M L Y 1 U 8 B 4 H 5 I 3 A 0 J 9 2 Z 6 G _ E K T Q
V 4 Z Q C 8 M K E ! 5 Y P 6 S H B 9 D 2 7 U I W T F ? J 0 . _ 0 G 3 X 1 N R L A
X F W 8 T . 0 ! U I 3 1 D R V M G 6 ? S A K L N 7 J Q Z C P 5 0 2 Y E H B 9 4 _
Y 8 ! Q 6 M K N V _ U H I E L 4 . P F A Z 3 7 1 R T S B W X 0 0 5 2 9 G ? D J C
Y 9 K I N L 0 A P W G 1 2 U R D T J F Z B _ 3 S X . ! C 6 H 5 4 M E ? 7 Q 8 0 V
Z Y 9 Q P ! F R J A 8 K 5 U 6 D 0 1 4 . L G B C S N W X _ ? V M 3 2 0 H T I 7 E

```

This will have to be decoded by hand. The answer is: Once is enough.

10. Time for a snack. What are we having? **Doyw oao Jvqst1f Pkwcd** The key for this Vigenere cipher is the city referenced in the Secret CSR.

The Secret CSR is on the Review 3 Assets page. Download it and double-click on it in the Downloads folder to view OR you can use an online CSR decoder to read the data.



We can see that London is going to be our key. Find an online Vigenere cipher solver and drop in the ciphertext along with the key:



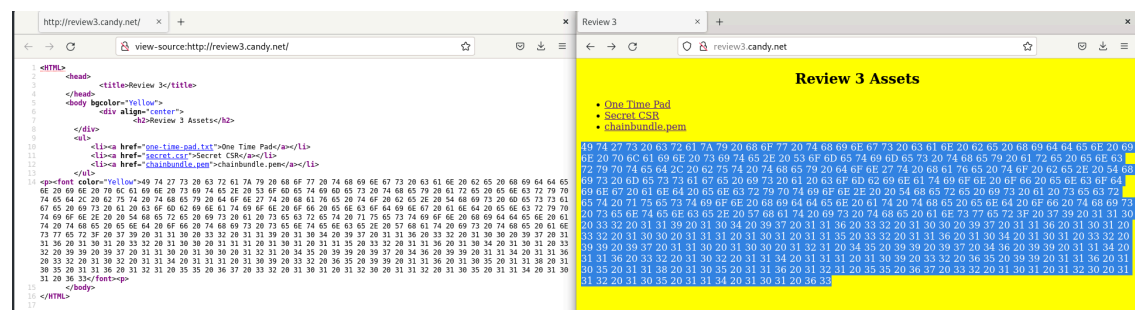
So we are having Salt and Vinegar chips.

11. Answer the following questions about the chainbundle.pem file:
 - a. When does each certificate expire?
 - b. What province is the root CA in?
 - c. What is the name of the intermediate certificate?

- Taffy Intermediate CA-57 expires on 9/18/2023, the Taffy Root CA-03 expires on 9/15/2032.
- Alberta
- Taffy Intermediate CA-57 (yes it's misspelled).

12. There is a secret message hidden on the Review 3 Assets page. What is it?

The message is yellow text on a yellow background. You can view the message two ways, either click and drag on the page to highlight the text, or view the page source.



The text is hexadecimal. Find a decoder:

ASCII text

It's crazy how things can be hidden in plain site.
Sometimes they are encrypted, but they don't have to be.
This message is a combination of encoding and encryption.
There is a secret question hidden at the end of this
sentence. What is the answer? 79 110 32 119 104 97 116 32
100 97 116 101 32 100 111 101 115 32 116 104 101 32 99 97
110 100 121 45 99 97 46 99 114 116 32 102 114 111 109 32
65 99 116 105 118 105 116 121 55 67 32 101 120 112 105 114
101 63

Hex (bytes)

20 31 32 31 20 33 33 20 30 37 20 33 32 20 31 30 31 20 31
32 30 20 31 31 32 20 31 30 35 20 31 31 34 20 31 30 31 20
36 33

We can see that there is a bit of the message at the end that is just numbers. This is decimal encoded data:

ASCII text

On what date does the candy-ca.crt from Activity7C expire?

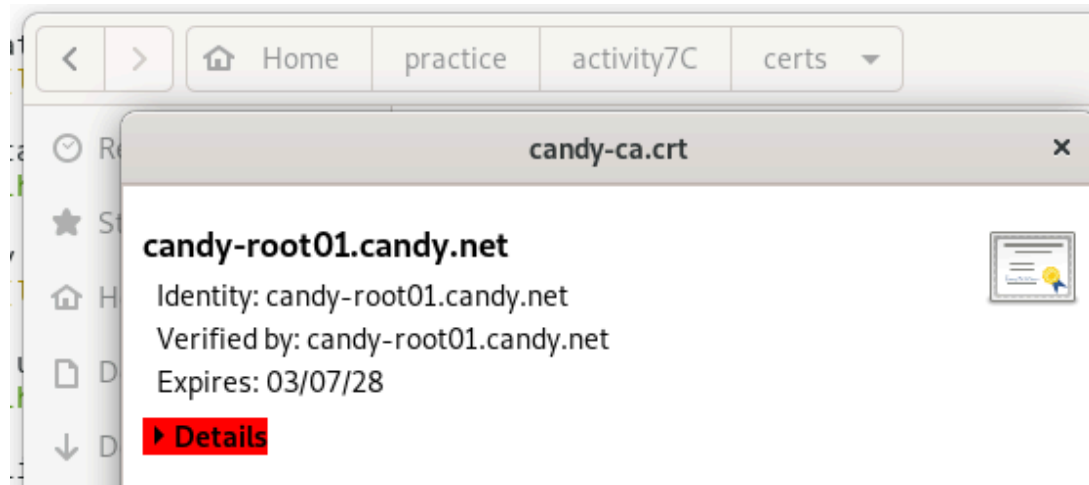
Hex (bytes)

Binary (bytes)

Decimal (bytes)

```
79 110 32 119 104 97 116 32 100 97 116 101 32 100 111 101
115 32 116 104 101 32 99 97 110 100 121 45 99 97 46 99 114
116 32 102 114 111 109 32 65 99 116 105 118 105 116 121 55
67 32 101 120 112 105 114 101 63
```

If you have already cleaned up activity7C, you can just set it up again and go check the candy-ca.crt file.



It expires on 03/07/2028.