.

# Let's Play a CTF, Part 2

David Zero
**zero-one@zer0-one.net**

February 5, 2018

# Table of Contents

# Review: Challenge #1

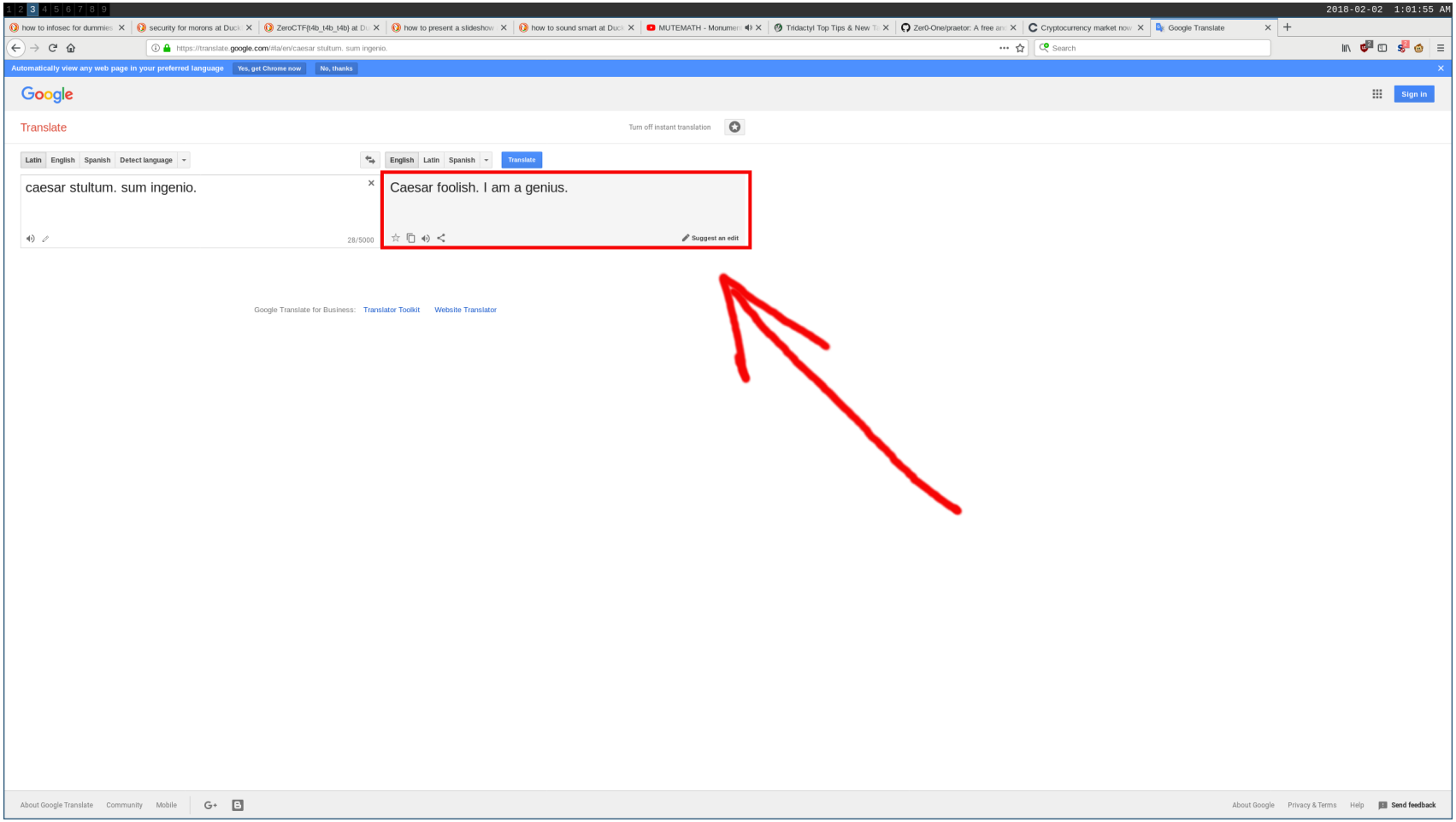
Let's review Challenge #1 and its solutions, as well as what we learned (or what we didn't).

# Challenge #1: Problem

I gave you a 15MB file filled with what looks like complete junk, and asked you to find a flag with the following prompt:

```
Challenge 1
===========

Caesar stultum. Sum ingenio.
```

A reasonable person who does not speak latin would want to know what this means. Can anyone name a product developed here at Google that might help us translate this text?


caesar stultum. sum ingenio.
Caesar foolish. I am a genius.
Translate
Google Translate for Business: Translator Toolkit Website Translator

You may or may not have looked at the included hint, but let's take a look at it:

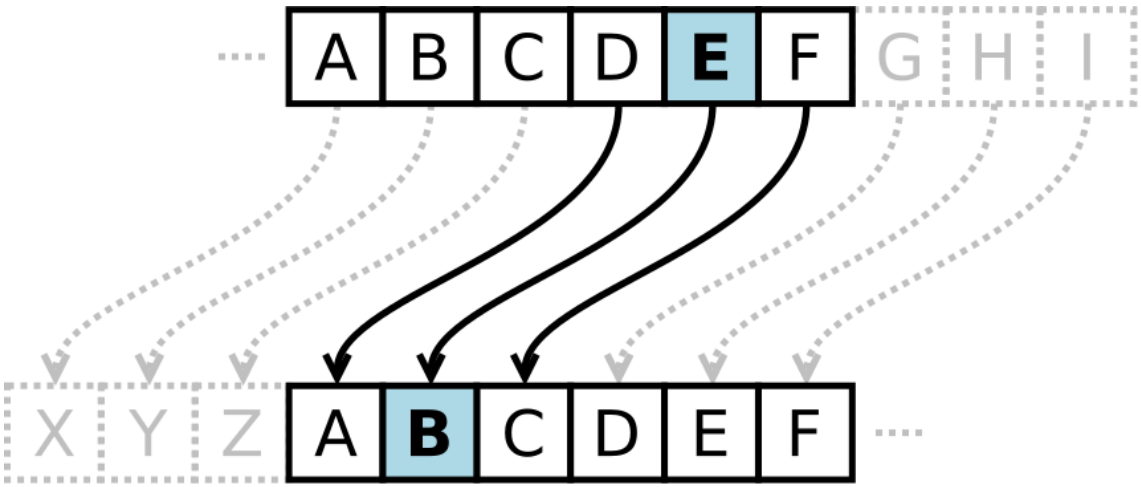
```
HINT
====

When you're surrounded by noise, it can be
   hard to focus. Don't forget about
what you're looking for. Forma et Figura.
```

I would interpret this to mean that the flag is surrounded by irrelevant "noise", and that we should focus on the "form and figure" of the flag.

# Concepts

Let's talk about Julius Caesar. I think Julius Caesar is a pretty cool guy. Eh conquers Gaul and doesnt afraid of anything.

He also used this nifty (during a time when most people couldn't read, anyway) cipher in all of his confidential communications:



We know this today as a "Caesar cipher" or "Caesar shift cipher". It's a dead-simple substitution cipher that we use in modern times to help you to remember to drink your Ovaltine.

Has anyone here **not** used any of the following utilities?

- grep
- sed
- tr
- vim

# Challenge #1: Solution

Alright then, let's try to filter out the noise:

```
grep "ZeroCTF" secretum.
```

No luck. Let's try looking for left-brackets:

```
grep "{" secretum.
```

Still nothing.
At this point, you did one of three things:

- Gave up immediately (shame on you).
- Gave up on filtering the noise and went completely off-track.
- Tried more filters.

At this point, I'd like to hear how you solved this.

Did you notice that there was only a single right-bracket in the whole file?

```
grep -a "}" secretum
```

Running the above command would have returned (among a bit of other garbage):

```
FkxuIZL{i4xvk_b3do11as}
```

This looks to be in the form of a flag, but it also doesn't appear to be plaintext. Given the clue about Caesar, we might try a rot-13:

```
echo "FkxuIZL{i4xvk_b3do11as}" | tr a-zA-Z n-za-mN-ZA-M
```

Which yields:

```
SxkhVMY{v4kix_o3qb11nf}
```

No good. However, this really does look like a Caesar shift, so let's think for a second; we know that the first letter of the flag is "Z", so let's map Z to F, and try to decipher it again:

```
echo "FkxuIZL{i4xvk_b3do11as}" | tr g-za-fG-ZA-F a-zA-Z
```

Which finally yields the flag:

```
ZeroCTF{c4rpe_v3xi11um}
```

# Big Lesson #1

To those who had started out filtering the file (grep, sed, etc), but gave up:

If you had just continued following your intuition the tiniest bit further, you would have found the flag immediately.

The first Big Lesson™ is: Follow your gut instinct all the way through. A problem that seems like it has a simple solution probably does.

# Big Lesson #2

To those who were completely off-track:

Your gut instinct was wrong, but that's OK, it'll get better with experience. You don't always have to make assumptions about what to do next. Read and interpret any hints you get (explicit or otherwise) carefully. When you do have to make assumptions about what to do next, be greedy; assume the simplest path first.

The second Big Lesson™ is: Keep It Simple, Caesar.

Would anyone like to share something unique they learned while completing the challenge?

# Challenge #2

This brings us to Challenge #2, which you will find **here**.

This challenge has two parts, each with one flag at the end. Either part can be solved without first solving the other. Each flag is worth 100 points.
Just as before, there are bonus flags (2 this time) hidden within the presentation. This will probably be the last time I do that, since it's becoming difficult to find ways to hide flags here that are still easy-tier.

# SECRET//NOFORN

[redacted]