**Stegano50 - Confidence CTF 2014**

**Introduction**: Stegano50 is an easy 50 point steganalysis / forensics challenge that was part of the 2014 Confidence CTF Teaser organized by the Dragon Sector team. Stegano50 was solved by ~90 people during the time of the CTF. This writeup was made possible using resources from the [CTF Wiki](https://github.com/ctfs/write-ups-2014/tree/master/confidence-ds-ctf-teaser/stegano50) as well as, writeups from [PWNTester](http://www.pwntester.com/blog/2014/04/27/dragonsector-pdf-stegano-50/), and [dul.ac](http://blog.dul.ac/2014/04/DSCTF14/).

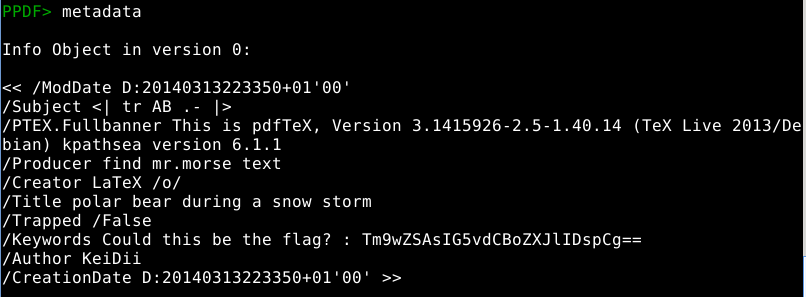
**Task**: Find the flag hidden in the provided PDF File (Stegano50.pdf).

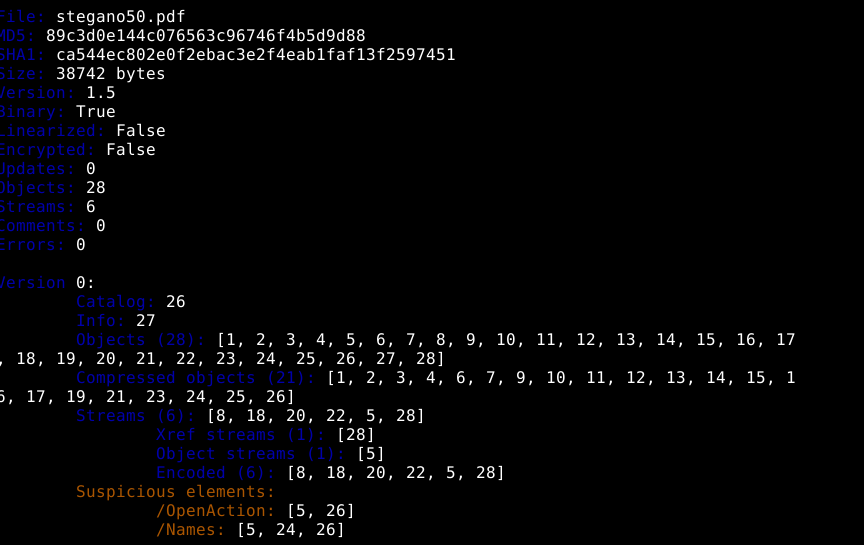
**Solving:** Once we’ve downloaded the PDF file we need to begin analysing the PDF file to search for the hidden flag. If we simply open the pdf file with Adobe Reader we’re presented with a document filled with Lorem Ipsum filler text and a large watermark across the document stating “No Flag Here!”. Lorem Ipsum text is dummy text used in the printing and typesetting industry to model the layout of text documents, so this isn’t of any use to us. Our biggest clue at the moment is the “No Flag Here!” watermark, indicating that our flag is hidden elsewhere in the document. Let’s start by examining the metadata of the PDF.

Metadata is a simply a way of saying “data that describes other data” in this case the metadata of our PDF will show us things like the author, name, size, and date the document was created.

Examining documents such as PDF’s requires the use of tools designed to read PDF’s data format (You can read more about the format of PDF’s [here](http://forensicswiki.org/wiki/PDF)). There are a myriad of tools out there to examine the metadata of PDF files. I’ll be using [Peepdf](http://eternal-todo.com/tools/peepdf-pdf-analysis-tool) written by Jose Esparza simply because it allows us to accomplish the task without the use of any other tools. You can find a copy of Peepdf by googling or simply using the copy contained in the folder.

Examining the info, and metadata of the pdf file using peepdf gives us the following to work with.

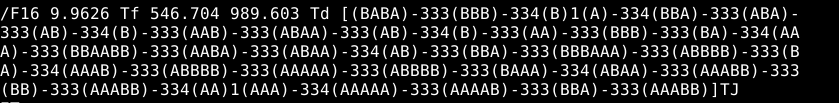




There are a few items of interest in the metadata of this document. The subject, producer, and keywords fields could all be of use to us. The obvious place to our investigation is the keyword field where they give us the potential flag: ‘Tm9wZSAsIG5vdCBoZXJlIDspCg==’ unfortiunately it turns out this flag is a dummy used to throw us off.

We then turn our search to the subject, and producer fields. The producer field tells us to “find mr. morse text” a pretty big hint our flag could be hidden somewhere in this document using Morse Code. Our suspicions are confirmed by the subject field which says “<| tr AB .- |>”. ‘Tr’ is the unix command ‘Text Replace’ which will replace instances of letters or strings with another set of letters or strings. In this case the provided tr command would replace all instances of ‘A’ with ‘.’ and all instances of ‘B’ with ‘-’.

The only question left now is, where do we find the text to replace? Taking a look back at the main document it’s pretty clear the organizers don’t intend for us to replace the Lorem Ipsum text. Let’s start by taking a look at the objects contained in this document. After looking at several objects using peepdf we find something interesting contained in object 8.



Could this be the text we need to convert to Morse Code using the supplied text replace command? Let's find out.

Translating the content contained in object 8 by treating the A’s as periods and the B’s as dashes gives us the following output:

-.-. --- - . --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- .. ... ..... ....- --. ...--

Copying and pasting the output into an online Morse Code translator gives us: COTEGRATULATIONS,FLAG:1NV151BL3M3IS54G3. Which seems to be a little off, probably due to the fact I translated by hand. The final flag is:

CONGRATULATIONS,FLAG: 1NV151BL3M3554G3