Forensic Challenge:

A Peculiar TV Show

Dr. Sheldon Cooper, renowned theoretical physicist and part-time vexillologist, has generously shared his latest educational masterpiece: "Fun with Flags: A guide". Within its pages, you'll find a deep dive into the world of flags, complete with trivia, design principles, and classic Cooper wit.

The document appears to be exactly what it claims: a guide to vexillology. But is that all it is? The good doctor is known for his love of precision... and puzzles.

⬛ Fun_with_Flags_Gu…

Provided file: Fun_with_Flags_Guide.docx

Approach:

Download and open the provided docx file, and we are greeted by Dr Sheldon Cooper on his guide "Fun with Flags". Lets try to find any "hidden texts" on the word doc itself.

Copy and paste all contents into Notepad and this should reveal hidden messages:

Fun with Flags: A Guide by Dr. Sheldon Cooper ▷ CBCTF{THISISNOTTHEFLAG}

n0T H3re

We are now able to see hidden messages that were previously in white text + small fonts.

But this seems to be a red herring and we need to dive deeper.

Next we try to use the strings command in linux and try to grep something.

> `strings Fun_with_Flags_Guide.docx | grep "CBCTF"`

> `strings Fun_with_Flags_Guide.docx | grep "flag"`

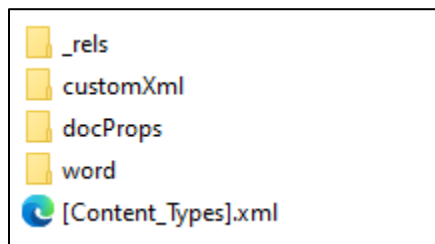> `strings Fun_with_Flags_Guide.docx | grep "{"`

.

.

.

Nothing noteable found… ☹

Next, lets try to extract the docx file itself:

> unzip Fun_with_Flags_Guide.docx -d out/

I could investigate each files… but how about we try "**strings | grep**" on ALL files in this directory.

> `find . -type f -exec strings {} \; | grep "CBCTF"`

`CBCTF{THISISNOTTHEFLAG}` This was the red herring

`CBCTF{y0ur3_1n_mY_sp0t}` Perfect! We got the flag

Flag:

CBCTF{y0ur3_1n_mY_sp0t}