Fuzzing exercise

A guide

3 goals

- Reverse engineer the file format and generate a valid file with the text UTW2014
- Discover the easter eggs
- Crash the program

How to use it

- 3 files & python 2.7.5 (for `*.pyc`)
  - input file (generated by `writefile.py`)
  - `console.py` (run as $python `console.py`)
  - `readfile.pyc` (parser)
- The students don't have access to `writefile.py` or `readfile.py`

Where is the fuzz?

- Due to the short time available the parser can't be too hard to break.
- Manual modifications should be sufficient.
- Although we won't need a "real" fuzzer it gives an idea of what one should do.

TODO

- Try to solve the exercise (preferably without looking at the source code of `write/readfile.py`)
- The input file provided with the zip is called output.txt
- Have fun!

Help

- use -h flag after the commands to get help
- email me: hndantas@gmail.com