Fuzzing exercise

A guide

3 goals

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

How to use it

- 2 files & python 2.7.5 (for `*.pyc`)
- `console.py` (run as $python `console.py`)
- `output.txt` (valid format for parser)

Instructions 1/2

- Unzip exercise-students.zip
- Open output.txt in a text editor
- Open a terminal, cd to this folder and type `$python console.py`
- Write the name of the file you want to parse (*e.g.* output.txt). Leave empty to read the same file.

Instructions 2/2

- Modify output.txt and try the parser again (keep a copy of the original for reference)
- If you break it, the program will terminate!
- Have fun.

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.