

# MSDC

## jsobfs a JavaScript obfuscator

### Notes

- The tool is built using `.net core 2` and could be compiled to run on any platform. The current code attached at the usb is compiled to run at `win10x64`
- The tool is build upon another opensourced obfuscator that could be found at [javascript-obfuscator](#)

### Usage instructions

```
jsobfs 1.0.0
Copyright (C) 2019 jsobfs
USAGE:
Obfuscates javascript files at a given directory:
jsobfs --backup --js_dir path/to/js --jx_ext .js

-d, --js_dir    Required. The directory containing the javascript files.

-b, --backup    (Default: true) backup flag

-e, --jx_ext    (Default: .js) The javascript extension.

--help          Display this help screen.

--version       Display version information.
```

1. Add the executable to the environmental variables; in order to reach it at any directory
2. From the command line type `jsobfs.exe -d <your_directory_containing_js_code>`
  1. The execution will start storing the current files found at the given directory into a `.zip` file with the date of the operation
  2. Then each of the `.js` files will be obfuscated and overwritten

### Notes

In case you are using a type-script files `.ts` make sure to add the flag `-e ".ts"` to change the search criteria