Fetch

Writeup by Speer
Category: Forensics

Author: JohnHammond

Description

"Gretchen, stop trying to make fetch happen! It's not going to happen!" - Regina George

file: `fetch.7z`

After decompressing the `7z` file we get a `wmi` file.

```
$ file fetch
fetch: Windows imaging (WIM) image v1.13, XPRESS compressed, reparse
point fixup
```

extracting this with `7zip` dumps a load of windows prefetch `.pf` files.

I decided to use this tool https://github.com/EricZimmerman/PECmd to list out all the registries in the files


```
PECmd.exe -d "<path to directory with .pf files" | findstr.exe /I
"flag"
```

`FLAG{97F33C9783C21DF85D79D613B0B258BD}`