Where to start with reverse engineering

Haifisch

HASHBANG Engineer
RePower, PebbleStatus, PBNest, other tomfoolery and hackery.
DHowett, Sudo.

What is reverse engineering?

- Breaking down software into something we can improve, hack, build software like it.
- Product security analysis
- Bug fixes
- It can be used as a learning tool
- Espionage *rubs hands together*

An example for you,
List all strings in a binary

The “strings” command is installed through Xcode or binutils.

Example usage; strings ./hello

Output:

```
Ohai! Im a string, please don't modify me!
:(
```

Terms to search (Google, not Bing, or Duckduckgo)

Disassemblers

- IDA Pro (Free trial)
- Hopper (Free trial)
- strings

Runtime Analysis

- GDB/LLDB
- Cycript (cycript.org)
- weak_classdump

In the end

Reverse engineering is a lot of poking around software, searching for valuable information that can you can use with or against the software. You will break things in the process, but that’s just part of the fun.