PUTTING THE OPEN BACK INTO CLOSED SOFTWARE

Motivation

- World is full of software without (access to) source
  - Closed source software
  - Software with lost sources
  - (Embedded systems in the field)
- Some form of coexistence is required
  - Interoperation
  - Subsumption
  - Assimilation
  - Annihilation
- Coexistence requires information (intelligence gathering)

What is Frida?

- dynamic instrumentation toolkit
  - debug live processes
- scriptable
  - execute your own debug scripts inside another process
- multi-platform
  - Windows, Mac, Linux, iOS, Android, QNX
- open-source
  - wxWindows (LGPL + static linking exception)

Why would you need Frida?

- For reverse engineering
- For programmable debugging
- For dynamic instrumentation
- For great good!

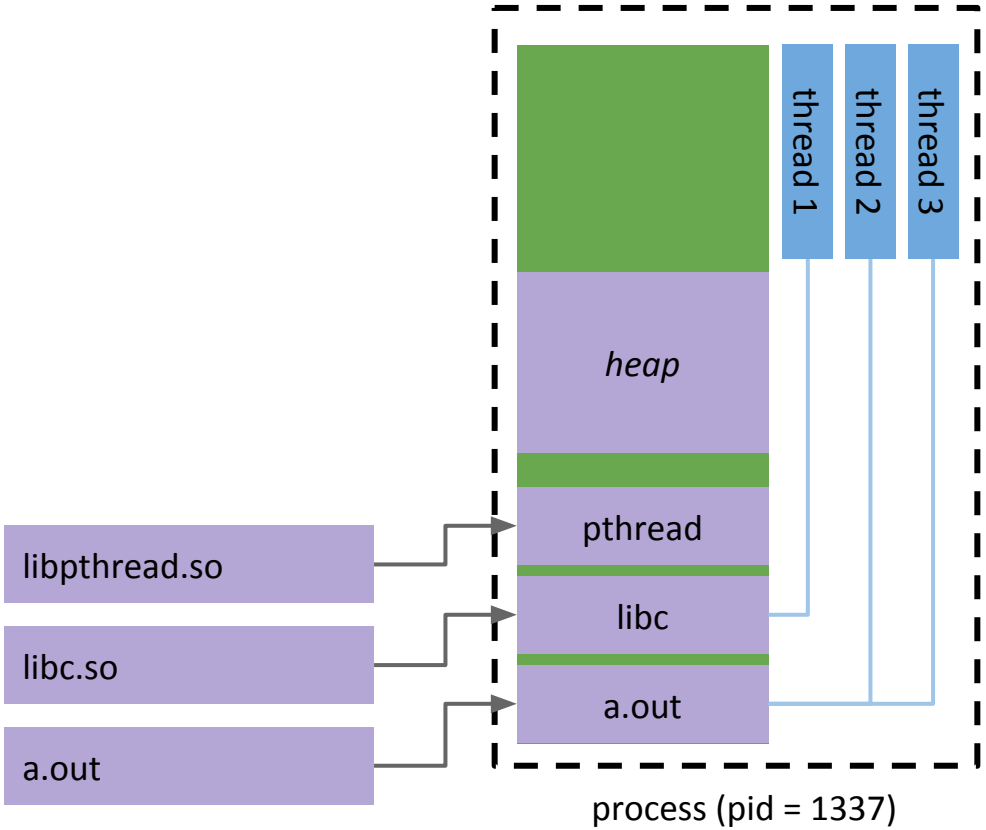
What is reverse engineering?

“discovering the technological principles of a device, object or system through analysis of its structure, function and operation”

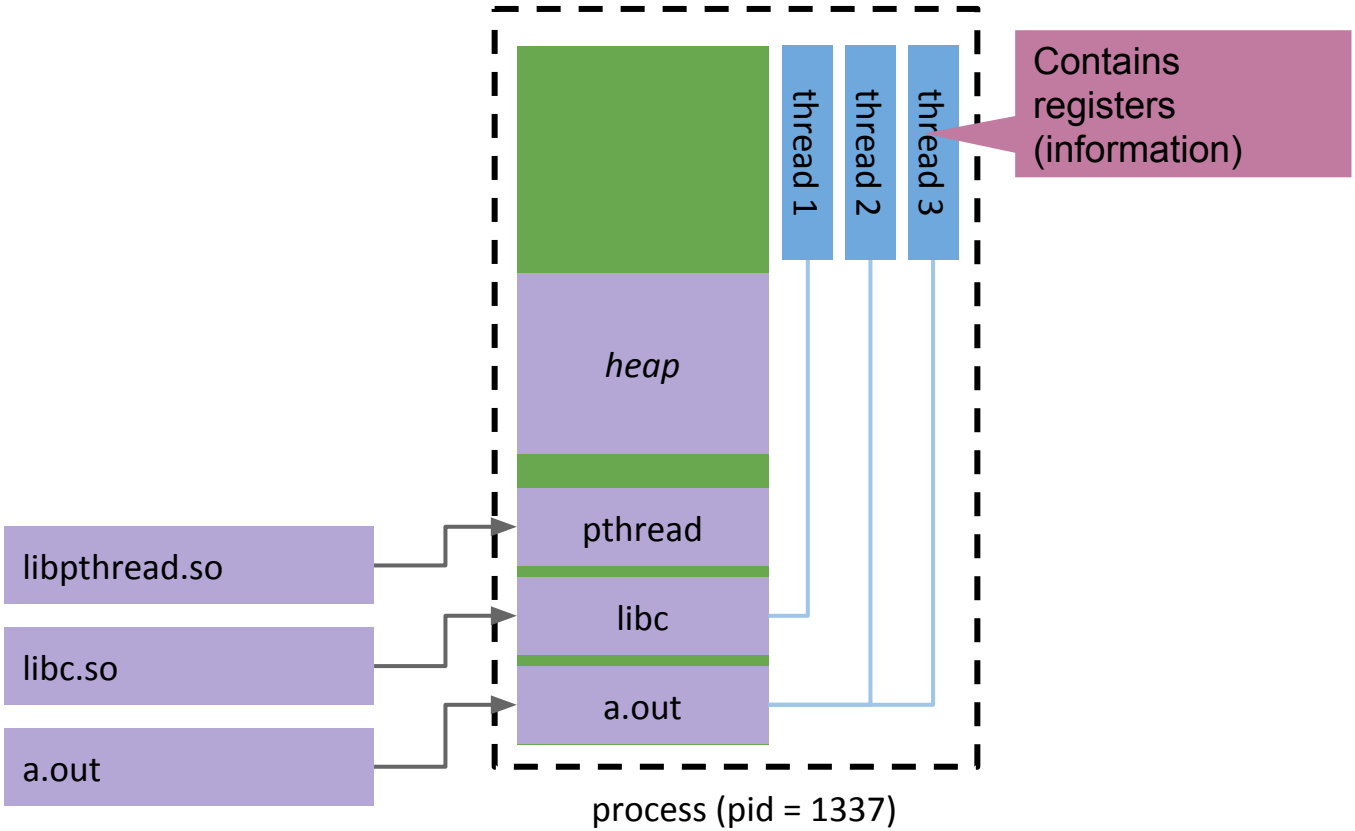
Why do we need reverse engineering?

- Protocol interoperability
  - E.g., MSN-support in GAIM/Pidgin/Empathy, Windows file share support for Linux (Samba)
- Video format playback
  - E.g., DeCSS-support in VLC/MPlayer
- API compatibility
  - E.g., Windows-emulation on Linux / OSX (Wine)
- Unlocking hardware
  - E.g., jailbreaking iPhone, iPod, PS3
- Recovering lost memories
  - E.g., playing Paper Boy on a C64 emulator

Native software - the basics



Native software - the basics



Basic Frida skills

- attaching to processes
- hooking functions
- modifying function arguments
- calling functions
- inspecting memory
- modifying memory


Demo