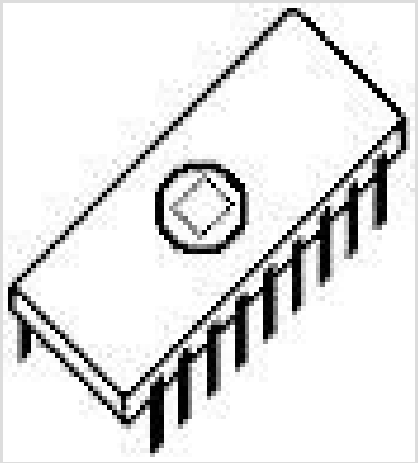
Universal Decompiler: Open Source By Force



John McMaster
RCOS
10/17/10

Project Goals

- Flexible target architecture
- Geared towards embedded platforms (8051, BlackFin, ARM, etc)
- Architectures can be defined through a config file or through a loadable module
- Repurpose the Candela laser!
  - Haven't for some time, but still on my mind

Last semester

- Focus on Fast Library Identification and Recognition Technology (FLIRT) implementation
- obj2pat: object file to .pat function signature
- pat2sig: .pat file
- Misc engine fixes

Summer progress

- Rewrote BFD object to signature code
  - Was previously based on hacked C code
- Spent summer RE malicious software
  - learned many new techniques
- Learned basic Qt
- Various bug fixes
- Public signature archive
  - http://github.com/JohnDMcMaster/uvsig

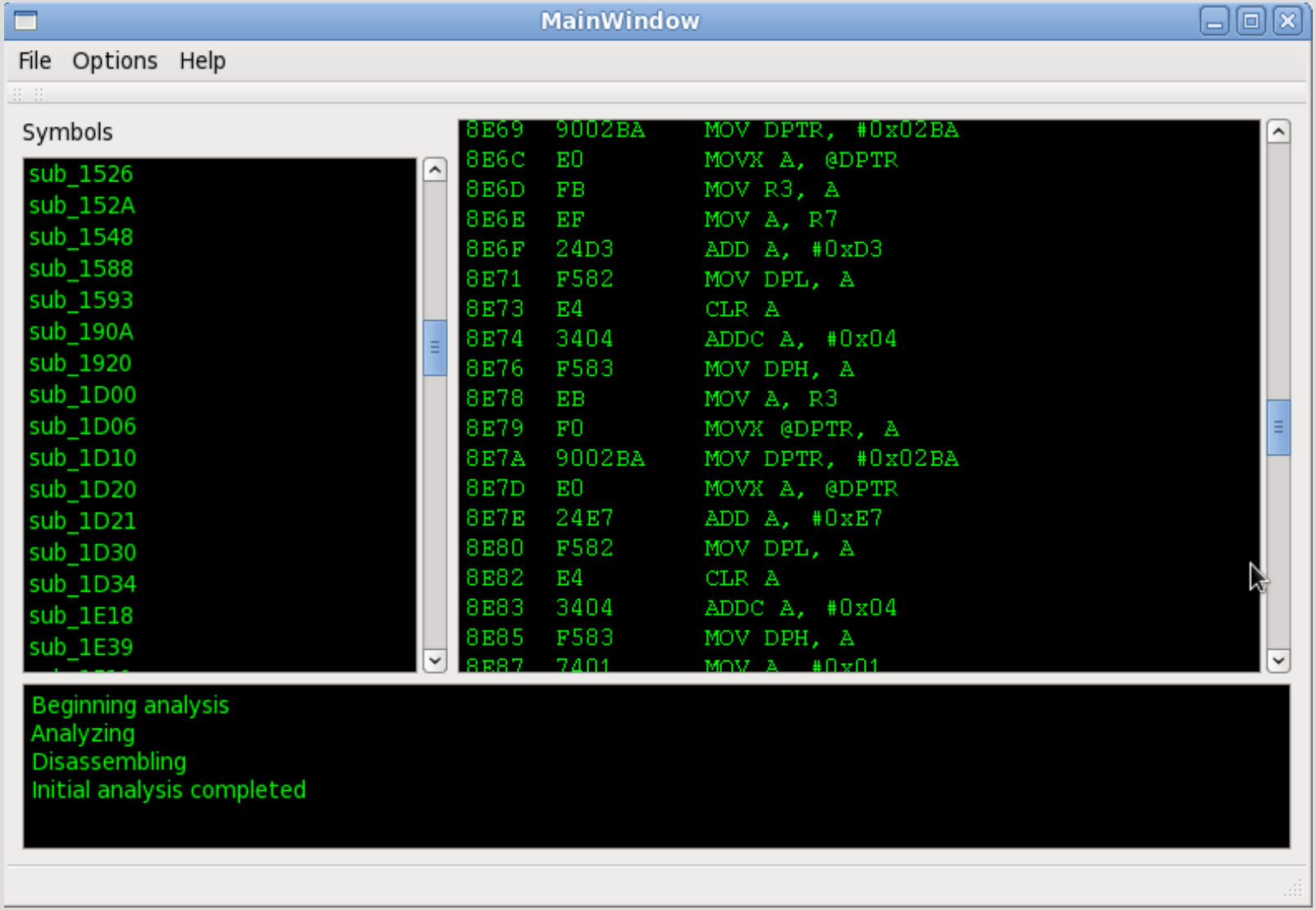
Semester Milestones

- GOAL: user interface tools
- 1: disassembler/decompiler GUI
- 2: license scanner GUI
- 3: plugin and event systems

Graphical user interface

- Easier to give hints through GUI then bash
- Disassembly annotation environment
  - Even if decompiling isn't possible
- IDA had a disassembler GUI over a decade before a decompiler
- GUIs will be developed in Qt
  - Open source (LGPL)
  - Well documented
  - Feature rich: Qt Designer, many widgets

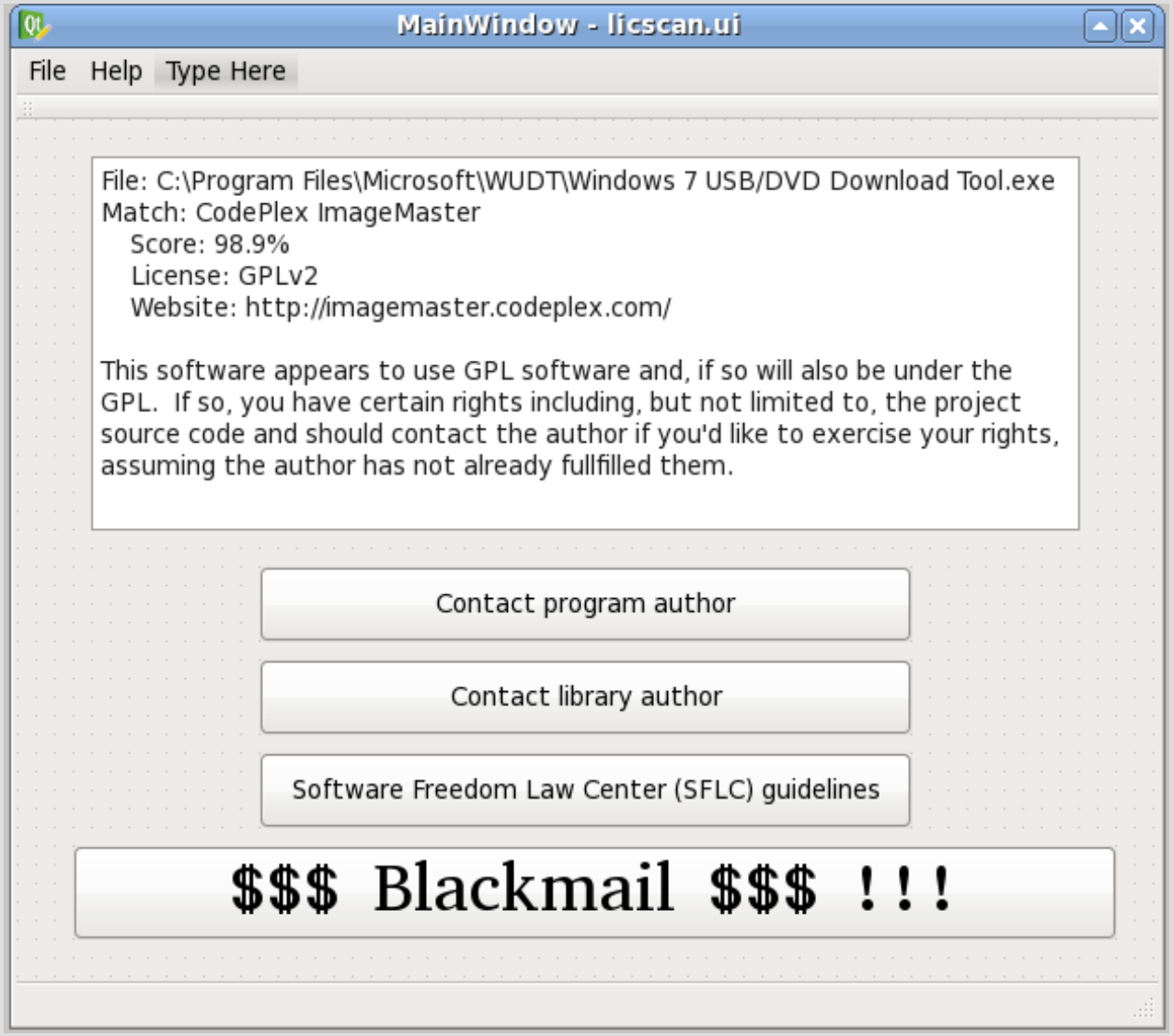
Initial sandbox



License scanner

- Commercial software sometimes violates GPL and other licenses
- Finds this code within closed source binaries
- Proprietary companies/systems do this
  - Black Duck Software
  - OpenLogic
- Build library signature database
  - Even from people typically not interested in RE
- I will not handle license violations
  - Up to user what to do

Mock UI


MainWindow - licscan.ui
File
Help
Type Here
File: C:\Program Files\Microsoft\WUDT\Windows 7 USB/DVD Download Tool.exe
Match: CodePlex ImageMaster
Score: 98.9%
License: GPLv2
Website: http://imagemaster.codeplex.com/
This software appears to use GPL software and, if so will also be under the GPL. If so, you have certain rights including, but not limited to, the project source code and should contact the author if you'd like to exercise your rights, assuming the author has not already fullfilled them.
Contact program author
Contact library author
Software Freedom Law Center (SFLC) guidelines
$$$ Blackmail $$$!!!

Preparing for the GUI

- Initial algorithm will be simple and potentially misleading/inaccurate
  - % of functions matched in a library
  - % of code covered
  - We may only use a small function subset
- Make obj2pat, pat2sig match FLAIR output
- Desirable if program could run on Windows
  - Never tried before

Plugin support

- Allows cleaner isolation of disassembly engines
- Easier to integrate third party code
- Requires callback/event system
- Ability to use GPL'd software by isolating them to like licensed plugins

Questions????