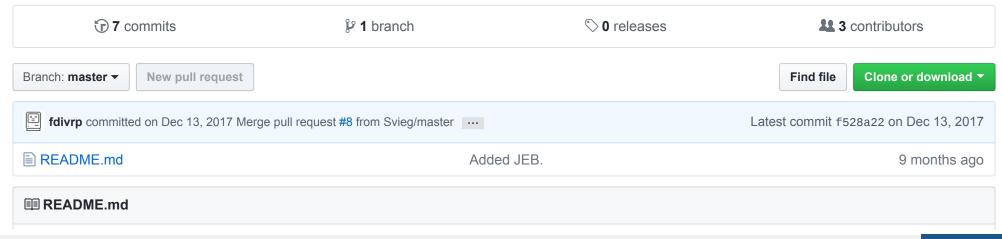


### A curated list of awesome reversing resources



# awesome-reversing

A curated list of awesome reversing resources

- Awesome Reversing
  - Books
  - Courses
  - Practice
  - Hex Editors
  - Binary Format
  - Disassemblers
  - Binary Analysis
  - Bytecode Analysis
  - Import Reconstruction
  - Dynamic Analysis
  - Debugging
  - Mac Decrypt
  - Document Analysis
  - Scripting
  - Android
  - Yara

### **Books**

#### Reverse Engineering Books

- The IDA Pro Book
- Reverse Engineering for Beginners
- Assembly Language for Intel-Based Computers (5th Edition)
- Practical Reverse Engineering
- Reversing: Secrets of Reverse Engineering
- Practical Malware Analysis
- Malware Analyst's Cookbook
- Gray Hat Hacking
- The Art of Memory Forensics
- Hacking: The Art of Exploitation
- Fuzzing for Software Security
- Art of Software Security Assessment
- The Antivirus Hacker's Handbook
- The Rootkit Arsenal
- Windows Internals Part 1 Part 2
- Inside Windows Debugging
- iOS Reverse Engineering
- The Shellcoders Handbook
- A Guide to Kernel Exploitation
- Agner's software optimization resources

### Courses

### Reverse Engineering Courses

- Lenas Reversing for Newbies
- Open Security Training
- Dr. Fu's Malware Analysis
- Binary Auditing Course
- TiGa's Video Tutorials
- Legend of Random
- Modern Binary Exploitation
- RPISEC Malware Course
- SANS FOR 610 GREM
- REcon Training
- Blackhat Training
- Offensive Security
- Corelan Training
- Offensive and Defensive Android Reversing
- Reverse Engineering Malware 101
- ARM Assembly Basics

## **Practice**

Practice Reverse Engineering. Be careful with malware.

- Crackmes.de
- OSX Crackmes
- ESET Challenges
- Flare-on Challenges
- Github CTF Archives
- Reverse Engineering Challenges
- xorpd Advanced Assembly Exercises
- Virusshare.com
- Contagio
- Malware-Traffic-Analysis
- Malshare
- Malware Blacklist
- malwr.com
- vxvault

## **Hex Editors**

#### Hex Editors

- HxD
- 010 Editor
- Hex Workshop
- HexFiend
- Hiew

## **Binary Format**

### Binary Format Tools

- CFF Explorer
- Cerbero Profiler // Lite PE Insider
- Detect It Easy
- PeStudio
- PEiD
- MachoView
- nm View Symbols
- file File information
- codesign Code signing information usage: codesign -dvvv filename

## **Disassemblers**

### Disassemblers

- JEB
- IDA Pro
- Binary Ninja
- Radare
- Hopper
- Capstone
- objdump

fREedom

# **Binary Analysis**

### Binary Analysis Resources

- Mobius Resources
- z3
- bap
- angr

## **Bytecode Analysis**

### Bytecode Analysis Tools

- dnSpy
- Bytecode Viewer
- Bytecode Visualizer
- JPEXS Flash Decompiler

# **Import Reconstruction**

### Import Reconstruction Tools

- ImpRec
- Scylla
- LordPE

# **Dynamic Analysis**

### Dynamic Analysis Tools

- ProcessHacker
- Process Explorer
- Process Monitor
- Autoruns
- Noriben
- API Monitor
- iNetSim
- Wireshark
- Fakenet
- netzob
- Volatility
- Dumpit
- LiME
- Cuckoo
- Objective-See Utilities
- XCode Instruments XCode Instruments for Monitoring Files and Processes User Guide
- dtrace sudo dtruss = strace dtrace recipes
- fs\_usage report system calls and page faults related to filesystem activity in real-time. File I/O: fs\_usage -w -f filesystem
- dmesg display the system message buffer

## **Debugging**

### **Debugging Tools**

- WinDbg
- OllyDbg v1.10
- OllyDbg v2.01
- OllySnD
- Olly Shadow
- Olly CiMs
- Olly UST\_2bg
- x64dbg
- gdb
- vdb
- IIdb
- qira
- unicorn

## **Mac Decrypt**

## Mac Decrypting Tools

- Cerbero Profiler Select all -> Copy to new file
- AppEncryptor Tool for decrypting
- Class-Dump use deprotect option
- readmem OS X Reverser's process dumping tool

## **Document Analysis**

### Document Analysis Tools

- Ole Tools
- Didier's PDF Tools
- Origami

# **Scripting**

### Scripting

- IDA Python Src
- IDC Functions Doc
- Using IDAPython to Make your Life Easier
- Introduction to IDA Python
- The Beginner's Guide to IDA Python
- IDA Plugin Contest
- onehawt IDA Plugin List
- pefile Python Libray

## **Android**

#### Android tools

• Android Developer Studio

- APKtool
- dex2jar
- Bytecode Viewer
- IDA Pro

## Yara

#### Yara Resources

- Yara docs
- Cheatsheet
- yarGen
- Yara First Presentation

© 2018 GitHub, Inc. Terms Privacy Security Status Help



Contact GitHub API Training Shop Blog About