

-
- Original source of list: https://github.com/REMath/literature_review

Mechanization of Exploits

- https://github.com/REMath/literature_review/blob/master/mechanization_of_exploits.org

Binary Analysis

- Moflow BAP-based tools to do post-crash graph backtaint slicing, post-crash forward symbolic emulation to look for more exploitable conditions, whitebox fuzzing based in SAGE
- <https://github.com/vrtadmin/moflow>
- <https://github.com/zardus/pyvex>
- Mcsema is a rewriting and static analysis framework based on LLVM
- <https://github.com/trailofbits/mcsema>
- <https://github.com/bdcht/amoco>
- A tool that exports LLVM bitcode into a Datalog workspace
- <https://github.com/plast-lab/llvm-datalog>
- Dagger is a decompilation framework based on LLVM
- <http://dagger.repzret.org/>
- <http://bap.ece.cmu.edu/>, <https://github.com/BinaryAnalysisPlatform/bap>
- <http://dynamorio.org/>
- <https://bitbucket.org/simona/mltk>
- <http://insight.labri.fr/trac>, <https://github.com/perror/insight>
- <https://github.com/rose-compiler/rose/tree/master/projects/BinQ>
- <https://github.com/neuromancer/SEA>
- <http://bitblaze.cs.berkeley.edu/>
- <http://code.google.com/p/avalanche/>
- <https://bincoa.labri.fr/trac>
- <https://github.com/jkinder/jakstab>
- <https://code.google.com/p/tree-cbass/>
- <https://github.com/bitblaze-fuzzball/fuzzball> (https://nebelwelt.net/blog/20140114-having_phun_with_SE.ht)
- <https://code.google.com/p/decaf-platform/>
- <http://esec-lab.sogeti.com/pages/Fuzzgrind>
- <http://code.google.com/p/idaocaml/>
- <http://doar-e.github.io/blog/2013/09/16/breaking-kryptonites-obfuscation-with-symbolic-execution/>
- <https://github.com/tosanjay/BOPFunctionRecognition>

-
- <https://github.com/codelion/pathgrind>
 - <http://doar-e.github.io/blog/2013/09/16/breaking-kryptonites-obfuscation-with-symbolic-execution/>
 - http://yurichev.com/writings/z3_rockey.pdf
 - <http://eindbazen.net/2013/04/pctf-2013-cone-binary-250-2/>
 - <http://shell-storm.org/blog/Binary-analysis-Concolic-execution-with-Pin-and-z3/>
 - An architecture-independent decompiler to LLVM IR
 - <https://github.com/draperlaboratory/fracture>
 - DECAF - <https://code.google.com/p/decaf-platform/>
 - Binwalk: Firmware analysis tool
 - <http://binwalk.org/>
 - <https://code.google.com/p/miasm/>
 - Angr: <http://angr.io/>
 - Triton is a DBA that provides Dynamic Symbolic Execution (DSE), Taint Engine, AST for x86/x86-64 and an SMT solver
 - <http://triton.quarkslab.com/>

Analysis of Communication Protocols

- Netzob is an open source tool for reverse engineering, traffic generation and fuzzing of communication protocols. It allows to infer the message format and the state machine of a protocol through passive and active processes. The model can afterward be used to simulate realistic and controllable traffic. - <http://www.netzob.org/>
- Communication protocols determine how network components interact with each other. Therefore, the ability to derive a specification of a protocol can be useful in various contexts, such as to support deeper black-box testing or effective defense mechanisms. Unfortunately, it is often hard to obtain the specification because systems implement closed (i.e., undocumented) protocols, or because a time consuming translation has to be performed, from the textual description of the protocol to a format readable by the tools. To address these issues, we developed ReverX, a Java application that generates automata for the language and protocol state machine from network traces. Since our solution only resorts to interaction samples of the protocol, it is well-suited to uncover the message formats and protocol states of closed protocols and also to automate most of the process of specifying open protocols. - <https://code.google.com/p/reverx/>

Intermediate Representations

- An Intermediate Representation for Integrating Reverse Engineering Analyses (1998)
- <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.47.2766>
- REIL: A platform-independent intermediate representation of disassembled code for static code analysis
- [http://moflow.org/ref/REIL%20-%20A%20platform-independent%20intermediate%20representation%20of%](http://moflow.org/ref/REIL%20-%20A%20platform-independent%20intermediate%20representation%20of%20)
- Relational Reverse Engineering Intermediate Language
- <http://www2.in.tum.de/bib/files/sepp11precise.pdf>
- VinE Project Documentation
- <http://bitblaze.cs.berkeley.edu/papers/vine.pdf>
- BIL
- <http://bap.ece.cmu.edu/doc/bap.pdf>
- LLVM
- http://infoscience.epfl.ch/record/149975/files/x86-llvm-translator-chipounov_2.pdf , <http://eurosys2013.tudos.org/content/uploads/2013/paper/Anand.pdf>
- TSL: A System for Generating Abstract Interpreters and its Application to Machine-Code Analysis
- <http://research.cs.wisc.edu/wpis/papers/toplas13-tsl-final.pdf>
- Combining Several Analyses into One OR What is a Good Intermediate Language for the Analysis of Executables?
- <http://www.dagstuhl.de/mat/Files/12/12051/12051.SimonAxel.Slides.pdf>
- Jakstab uses an IR described in chapter two
- <http://www.cs.rhul.ac.uk/home/kinder/papers/phdthesis.pdf>
- Wire – A Formal Intermediate Language for Binary Analysis
- <https://drive.google.com/file/d/0BymO5h8P3PgAakZqY1RQSIldzRmM/edit?usp=sharing>
- Automated Synthesis of Symbolic Instruction Encodings from I/O Samples - http://research.microsoft.com/en-us/um/people/pg/public_psfiles/pldi2012.pdf
- Towards A Binary Intermediate Language for Real-Time Embedded System by Jianqi Shi, Qin Li, Longfei Zhu, Xin Ye, Yanhong Huang, Huixing Fang and Fu Song
- <http://research.sei.ecnu.edu.cn/~song/publications/MPiE14.pdf>
- RockSalt: Better, Faster, Stronger SFI for the x86
- <http://www.cse.lehigh.edu/~gtan/paper/rocksalt.pdf>

Alias / Value Analysis

- Alias Analysis for Assembly
- <http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/2006/CMU-CS-06-180R.pdf>
- Probabilistic Alias Analysis for ARM Executable Code

-
- <https://drive.google.com/file/d/0BymO5h8P3PgAc29nUFBleGFtTnc/edit?usp=sharing>
 - WYSINWYX: What You See Is Not What You Execute
 - <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.637&rep=rep1&type=pdf>
 - Static Analysis of x86 Executables by Johannes Kinder
 - <http://www.cs.rhul.ac.uk/home/kinder/papers/phdthesis.pdf>
 - BDDStab: BDD-based Value Analysis of Binaries
 - http://cs.au.dk/~amoeller/tapas2014/tapas2014_2.pdf
 - Static Analysis of x86 Assembly: Certification and Robustness Analysis
 - <http://dumas.ccsd.cnrs.fr/docs/00/63/64/45/PDF/Laporte.pdf>

Control Flow Recovery

- Alias / Value Analysis
- https://github.com/REMath/literature_review#alias-value-analysis
- Alternating Control Flow Reconstruction
- <http://dslab.epfl.ch/pubs/alternatingCFR.pdf>
- Refinement-based CFG Reconstruction from Unstructured Programs by Sebastien Bardin, Philippe Herrmann, and Franck Vedrine
- http://www.labri.fr/perso/fleury/download/papers/binary_analysis/long-final-vmcai-11.pdf
- Control flow reconstruction from PowerPC binaries
- <http://www2.in.tum.de/bib/files/mihaila09reconstruction.pdf>
- Interprocedural Analysis of Low-Level Code
- <http://mediatum.ub.tum.de/doc/1006212/1006212.pdf>

Binary Rewriting

- Control Flow Integrity
- https://github.com/REMath/literature_review#control-flow-integrity
- Metamorphic Software for Buffer Overflow Mitigation
- <http://www.cs.sjsu.edu/faculty/stamp/students/cs298report.doc>
- Advanced Metamorphic Techniques in Computer Viruses
- <http://vxheavens.com/lib/apb01.html>
- Metamorphism in practice or “How I made MetaPHOR and what I’ve learnt”
- <http://vxheavens.com/lib/vmd01.html>
- Automated reverse engineering: Mistfall engine
- <http://vxheavens.com/lib/vzo21.html>
- Writing disassembler

-
- <http://vxheavens.com/lib/vmd05.html>
 - Benny's Metamorphic Engine for Win32
 - <http://vxheaven.org/29a/29a-6/29a-6.316>
 - "Do polymorphism" tutorial
 - <http://vxheavens.com/lib/vwm01.html>
 - Introductory Primer To Polymorphism in Theory and Practice
 - <http://vxheaven.org/lib/static/vdat/tupripol.htm>
 - Recompiling the metamorphism
 - <http://vxheavens.com/lib/vhe11.html>
 - Theme: Metamorphism
 - <http://vxheaven.org/29a/29a-4/29a-4.216>
 - Some ideas about metamorphism
 - <http://vxheavens.com/lib/vzo20.html>
 - Meta-Level Languages in Viruses
 - <http://vxheavens.com/lib/vsp44.html>
 - Metamorphism (part 1)
 - <http://vxheavens.com/lib/vzo10.html>
 - Metamorphism
 - <http://vxheavens.com/lib/vlj00.html>
 - The Viral Darwinism of W32.Evol
 - http://www.openrce.org/articles/full_view/27 (http://www.openrce.org/articles/files/evol_disasm.html)
 - The Molecular Virology of Lexotan32: Metamorphism Illustrated
 - http://www.openrce.org/articles/full_view/29
 - The Design Space of Metamorphic Malware
 - <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.486&rep=rep1&type=pdf>
 - Diablo
 - <http://diablo.elis.ugent.be/>

Abstract Interpretation

- <http://arxiv.org/abs/0810.2179> (code: <http://hal.inria.fr/docs/00/33/23/39/ANNEX/absint.v>)
- <http://dumas.ccsd.cnrs.fr/docs/00/63/64/45/PDF/Laporte.pdf> (Coq code in the paper)
- <http://pop-art.inrialpes.fr/interproc/interprocweb.cgi> (code: <http://pop-art.inrialpes.fr/people/bjeannet/bjeannet/forge/interproc/index.html>)
- <http://www.cs.indiana.edu/l/www/classes/b621/abiall.pdf>
- <http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/>
- <http://www.hexblog.com/?p=42>

-
- https://www.openrce.org/blog/view/1672/Control_Flow_Deobfuscation_via_Abstract_Interpretation
(code: <https://www.openrce.org/repositories/users/RolfRolles/BitwiseAI.ml>)
 - <http://www.irisa.fr/celtique/teaching/PAS/>

Logical solvers

- <https://github.com/leanprover/lean/>
- <http://z3.codeplex.com/>
- <http://alt-ergo.ocamlpro.com/>
- <http://yices.csl.sri.com/>
- <http://cvc4.cs.nyu.edu/web/>
- <http://minisat.se/>
- <http://fmv.jku.at/boolector/>
- <http://mathsat.fbk.eu/>

Probabilistic Logic

- <http://alchemy.cs.washington.edu/>
- <https://github.com/opcode81/ProbCog/wiki>
- <http://hazy.cs.wisc.edu/hazy/tuffy/>
- <https://code.google.com/p/thebeast/>

Datalog

- Alias Analysis for Assembly - http://users.ece.cmu.edu/~dbrumley/pdf/Brumley,%20Newsome_2006_Alias%20
- Dyna: Extending Datalog For Modern AI
- <http://cs.jhu.edu/~jason/papers/eisner+filardo.datalog11-long.pdf> and <http://www.cs.jhu.edu/~nwf/datalog20>
paper.pdf
- Using Datalog for fast and easy program analysis
- <http://cgi.di.uoa.gr/~smaragd/door-datalog2.0.pdf>
- Implementing Dataflow Analyses for Pegasus in Datalog
- <http://www.cs.cmu.edu/~drl/course/compilers/report.pdf>
- Using Datalog and binary decision diagrams for program analysis - <http://people.csail.mit.edu/mcarbin/papers/>
- Datalog for decompilation - <https://media.blackhat.com/us-13/US-13-Cesare-Bugalyze.com-Detecting-Bugs-Using-Decompilation-Slides.pdf>
- On Abstraction Refinement for Program Analyses in Datalog - <http://www.cs.ox.ac.uk/people/hongseok.yang/pa>
submitted.pdf

-
- Scaling Datalog for Machine Learning on Big Data
 - <http://arxiv.org/pdf/1203.0160.pdf>
 - Relational Representation of the LLVM Intermediate Language
 - <http://cgi.di.uoa.gr/~smaragd/theses/psallida.pdf>
 - <http://docs.datomic.com/query.html>
 - Using Datalog for Fast and Easy Program Analysis
 - <http://cgi.di.uoa.gr/~smaragd/door-datalog2.0.pdf>
 - An Efficient Engine for Fixed Points with Constraints
 - <http://research.microsoft.com/en-us/um/people/leonardo/muze.pdf>
 - On Abstraction Refinement for Program Analyses in Datalog
 - <http://www.cs.ox.ac.uk/people/hongseok.yang/paper/pldi14c-submitted.pdf>
 - Efficient Top-Down Computation Of Queries Under The Well-Founded Semantics - <http://citeseerx.ist.psu.edu/v>
 - Dedalus: Datalog in Time and Space
 - <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-173.pdf>
 - Strictly Declarative Specification of Sophisticated Points-to Analyses
 - <http://cgi.di.uoa.gr/~smaragd/door-oopsla09prelim.pdf>
 - Pregelix: Big(ger) Graph Analytics on A Dataflow Engine
 - <http://arxiv.org/pdf/1407.0455.pdf>

String Solvers

- <http://webblaze.cs.berkeley.edu/2010/kaluza/>
- <http://people.csail.mit.edu/akiezun/hampi/>
- <http://www.cs.purdue.edu/homes/zheng16/str/>
- A DPLL(T) Theory Solver for a Theory of Strings and Regular Expressions
- <http://www.divms.uiowa.edu/ftp/tinelli/papers/LiaEtAl-CAV-14.pdf> and <http://cvc4.cs.nyu.edu/papers/CAV2011/strings/>

Datasets

- <https://svn.sosy-lab.org/software/sv-benchmarks/tags/svcomp13/>
- <http://samate.nist.gov/SRD/testsuite.php>
- http://www.nec-labs.com/research/system/systems_SAV-website/benchmarks.php
- <http://www.debian.org/distrib/packages>
- <https://github.com/offensive-security/exploit-database>
- 1.2k bugs discovered by Mayhem - <https://bugs.debian.org/cgi-bin/pkgreport.cgi?submitter=alexandre%40cmu.edu>

Ground Truth

- <http://dwarfstd.org/>

Obfuscators

- <http://vxheaven.org/vx.php?id=eidx>
- <http://cansecwest.com/core03/shiva.ppt>
- http://diablo.elis.ugent.be/obf_deobfuscation_byhand
- <http://blog.yurichev.com/node/58>
- <https://github.com/enferex/GOAT-Plugs>
- <https://github.com/0vercl0k/stuffz/blob/master/llvm-funz/kryptonite/llvm-functionpass-kryptonite-obfuscater.cpp>
- <http://code.google.com/p/pescrambler/>
- <http://www.phrack.org/issues.html?id=13&issue=63>
- <https://github.com/obfuscator-llvm/obfuscator/wiki> (<https://github.com/obfuscator-llvm/obfuscator/tree/clarif> 425.0.24)
- Binary code obfuscation through C++ template metaprogramming - <https://www.cisuc.uc.pt/publication/showf>
- <https://github.com/xoreaxeaxeax/movfuscator>
- <https://github.com/xoreaxeaxeax/REpsych>

Hidden Computation

- <http://mainisusuallyafunction.blogspot.com.es/2014/02/x86-is-turing-complete-with-no-registers.html>
- <https://github.com/jbangert/trapcc>
- <http://www.cl.cam.ac.uk/~sd601/papers/mov.pdf>
- C++ Templates are Turing Complete - <http://ubietylab.net/ubigraph/content/Papers/pdf/CppTuring.pdf>
- <https://github.com/elitheeli/stupid-machines>

Deobfuscation

- Using optimization algorithms for malware deobfuscation - http://os2.zemris.fer.hr/ns/malware/2010_spasojev
- Unpacking Virtualization Obfuscators - http://static.usenix.org/event/woot09/tech/full_papers/rolles.pdf
- <https://code.google.com/p/optimice/>

Disassemblers

- <http://code.google.com/p/gdsl-toolkit/wiki/Overview>
- <http://www.beaengine.org/>
- <http://code.google.com/p/distorm/>
- <https://hex-rays.com/products/ida/index.shtml>
- <http://www.gnu.org/software/binutils/>
- <https://github.com/vmt/udis86>
- <http://software.intel.com/en-us/articles/pintool-downloads>
- <http://capstone-engine.org/>
- winSRDF <https://github.com/AmrThabet/winSRDF>
- Udis86 <http://udis86.sourceforge.net/>

Decompilers

- <http://users.ece.cmu.edu/~ejschwar/papers/usenix13.pdf>
- <http://dagger.repzret.org/>
- <http://www.cl.cam.ac.uk/~mom22/thesis.pdf>
- <http://code.google.com/p/arm-thumb-decompiler-plugin/>
- <https://github.com/EiNSTeiN-/ida-decompiler>
- <http://boomerang.sourceforge.net/>
- Retargetable Decompiler <https://retdec.com/>
- C4Decompiler <http://www.c4decompiler.com>
- SmartDec decompiler <http://decompilation.info/>
- REC Studio 4 <http://www.backerstreet.com/rec/rec.htm>
- List of .Net Decompilers: <https://code.google.com/p/facile-api/wiki/ListOfDotNetDecompilers>
- <https://github.com/zneak/fcd>

Virtual Machines

- <http://klee.llvm.org/>
- <https://s2e.epfl.ch/>
- <https://github.com/feliam/pysymemu>
- <http://pages.cs.wisc.edu/~davidson/fie/>
- <http://www.megalith.co.uk/8086tiny/>

Videos

- 30C3 - Triggering Deep Vulnerabilities Using Symbolic Execution (2013)
- Automated Test Generation using Symbolic Execution: Three Decades Later (2012)
- Concolic Execution, Jonathan Salwan, LSE Week 2013
- DART: Directed Automated Random Testing and Concolic Testing (2013)
- Unleashing Mayhem on Binary Code (2012)
- David Brumley - Safe Software (2013)
- GoogleTechTalks - Symbolic Execution and Model Checking for Testing (2007)
- BlackHat USA - How to grow a TREE (Taint-Enabled Reverse Engineering Environment) from a CBASS (2013)
- <https://archive.org/details/Recon2012Keynote-TheCaseForSemantics-basedMethodsInReverseEngineering>
- Applying Taint Analysis and Theorem Proving to Exploit Development (2010)
- Mozilla - Tales from Verification History (2012)
- New Directions in Random Testing - From Mars Rovers to JavaScript Engines (2013)

Model Checkers

- <http://nusmv.fbk.eu/>
- <http://www.cprover.org/cbmc/>
- <http://mtc.epfl.ch/software-tools/blast/index-epfl.php>
- <http://research.microsoft.com/en-us/projects/slam/>
- <https://bitbucket.org/ariieg/ufo/wiki/Home>
- <http://www.cprover.org/boom/>

Reasoning About Finite-state and Pushdown Automata

- <http://research.cs.wisc.edu/wpis/papers/CAV05-tool-demo.pdf>
- <http://www.cs.binghamton.edu/~dima/hpca13.pdf>
- <http://www2.informatik.uni-stuttgart.de/fmi/szs/tools/moped/>
- <http://www2.informatik.uni-stuttgart.de/fmi/szs/tools/wpds/>
- <http://research.cs.wisc.edu/wpis/wpds/opennwa-index.php>
- <http://rise4fun.com/rex>
- <http://www.cs.bham.ac.uk/~hxt/research/rxxr.shtml>

Debuggers

- <https://bitbucket.org/khooy/expositor>

-
- <http://www.eresi-project.org/>
 - <http://redmine.corelan.be/projects/mona>
 - <https://github.com/BinaryAnalysisPlatform/qira>

Interactive Theorem Provers

- <http://research.microsoft.com/en-us/um/people/akenn/coq/LOLA2012.pdf>
- <http://research.microsoft.com/en-us/um/people/nick/coqasm.pdf>
- <http://research.microsoft.com/en-us/um/people/akenn/coq/HLSL.pdf>
- <http://dream.inf.ed.ac.uk/>
- <http://www.cs.chalmers.se/%7Ehallgren/Alfa/>
- <http://coq.inria.fr/>
- <http://www.dcs.ed.ac.uk/home/lego>
- <http://wiki.portal.chalmers.se/agda/pmwiki.php>
- <http://www.comlab.ox.ac.uk/archive/formal-methods/hol.html>
- <http://www.cl.cam.ac.uk/Research/HVG/Isabelle/>
- <http://www.csl.sri.com/pvs.html>
- <http://mizar.org/>
- http://www.lama.univ-savoie.fr/sitelama/Membres/pages_web/RAFFALLI/af2.html
- <http://cvs.metaprl.org:12000/metaprl/>
- <http://www.cs.ru.nl/~janz/yarrow/>

Control Flow Integrity

- A Retargettable CFI implementation in LLVM. Authors: Joseph Battaglia and Oulin Yao
- <https://github.com/dbrumley/recfi>
- BinCFI: Control Flow Integrity for COTS Binaries
- <http://www.seclab.cs.sunysb.edu/seclab/bincfi/>
- <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/Zhang>
- <http://lenx.100871.net/papers/FPGate-bluehat.pdf>
- <http://lists.cs.uiuc.edu/pipermail/llvmdev/2014-February/070210.html>
- Enforcing Forward-Edge Control-Flow Integrity in GCC & LLVM by Caroline Tice, Tom Roeder, Peter Collingbourne, Stephen Checkoway, Úlfar Erlingsson, Luis Lozano, and Geoff Pike - <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-tice.pdf>
- Control-Flow Integrity Principles, Implementations, and Applications - <http://research.microsoft.com/pubs/692cfi.pdf>

C Code / C++ Code (Need to split these at some point)

- <http://why3.lri.fr/>
- <http://pp.ipd.kit.edu/firm/>
- <https://code.google.com/p/tanalysis/>
- <http://frama-c.com/>
- http://goto.ucsd.edu/~rjhala/papers/liquid_types.html
- <http://www.cs.umd.edu/~jfoster/cqual/>
- <http://sourceforge.net/projects/cil/>
- <https://github.com/kframework/c-semantics>
- <http://sixgill.org>
- <https://bitbucket.org/khooy/otter>
- <http://boogie.codeplex.com/>
- <https://github.com/jirislaby/stanse>
- <https://github.com/dsw/oink-stack/>
- <http://delta.tigris.org/>
- <http://embed.cs.utah.edu/csmith/>
- <http://css.csail.mit.edu/stack/>
- <http://embed.cs.utah.edu/creduce/>

Quantitative Analysis

- Daikon detects likely program invariants - <http://plse.cs.washington.edu/daikon/>
- DIG: A Dynamic Invariant Generator for Polynomial and Array Invariants - <https://bitbucket.org/nguyenthanhvuh>
- <http://www.prismmodelchecker.org/>
- <http://software.imdea.org/projects/cacheaudit/>
- <http://www-verimag.imag.fr/~tripakis/openkronos.html>
- <http://turnersr.github.io/measurements/properties.html>

Assisted Exploit Engineering

Return-oriented Programming

- <http://users.ece.cmu.edu/~ejschwar/papers/usenix11.pdf>
- <https://github.com/programa-stic/ropc-llvm>
- <https://github.com/pakt/ropc>
- <https://github.com/JonathanSalwan/ROPgadget>
- <https://github.com/Overcl0k/rp>

-
- <https://github.com/trailofbits/bisc>
 - Blind Return Oriented Programming (BROP) - <http://www.scs.stanford.edu/~sorbo/brop/>

Random Testing (Fuzzing)

- <http://embed.cs.utah.edu/csmith/>
- <https://code.google.com/p/american-fuzzy-lop/>
- <https://bitbucket.org/blackaura/browserfuzz>

Dynamic Analysis is an interpretation of the static semantics

- <https://github.com/mrmee/heapster>
- <https://github.com/neuroo/runtime-tracer>
- <https://github.com/CTSRD-SOAAP/taintgrind>
- https://minemu.org/mediawiki/index.php?title=Main_Page
- <https://github.com/neuroo/runtime-tracer>
- <https://github.com/wirepair/IDAPinLogger>

To be categorized

- https://github.com/pdasilva/vtrace_scripts
- <https://github.com/rapid7/metasploit-framework/tree/master/external/source/byakugan>
- <https://code.google.com/p/narly/>
- <https://code.google.com/p/viscope/>
- <https://github.com/isislab/Catfish>
- <https://github.com/aaronportnoy/toolbag>
- <http://www.rise4fun.com/>
- Apimonitor <http://www.rohitab.com/apimonitor>
- efl32mod <http://deroko.phearless.org/rce.html>
- Insight <http://www.bttr-software.de/products/insight/>
- Malwasm <https://code.google.com/p/malwasm/>
- pev <http://pev.sourceforge.net/>
- mona.py <http://redmine.corelan.be/projects/mona>
- <http://mlsec.org/>

Disassemblers & Debuggers

x86 only

- Ollydbg <http://www.ollydbg.de/>
- Immunity Debugger <https://www.immunityinc.com/products-immdbg.shtml>
- Syser <http://www.sysersoft.com/>
- GDB for Windows <http://www.equation.com/servlet/equation.cmd?fa=gdb>

x64

- FDBG <http://fdbg.x86asm.net/>
- Nanomite <https://github.com/zer0fl4g/Nanomite>
- x64dbg <http://x64dbg.com/#start>
- ArkDasm <http://www.arkdasm.com/>
- VirtDbg <https://code.google.com/p/virtdbg/>
- BugDbg <http://pespin.w.interia.pl/>
- MDebug <http://www.mdebug.org/>
- Visual DuxDebugger <http://www.duxcore.com/index.php/prod/visual-duxdebugger/overview>
- PEBrowseDbg64 Interactive <http://www.smidgeonsoft.prohosting.com/pebrowse-pro-interactive-debugger>

Multi-Architecture

- IDA Pro <https://www.hex-rays.com/products/ida/>
- BinaryNinja <http://binary.ninja/>
- Hopper <http://www.hopperapp.com/>
- radare <http://radare.org>
- GUI: Bokken <http://inguma.eu/projects/bokken>
- VDB <http://visi.kenshoto.com/wiki/Vdb>
- Frida <https://github.com/frida>
- Online Disassembler (ODA) <http://www.onlinedisassembler.com/odaweb/>

Java

- Procyon <https://bitbucket.org/mstrobels/procyon>
- SecureTeam Java Decompiler <http://www.secureteam.net/Java-Decompiler.aspx>

-
- Luyten <https://github.com/deathmarine/Luyten>
 - Krakatau Bytecode Tools <https://github.com/Storyyeller/Krakatau>
 - DJ Java Decompiler <http://www.neshkov.com/>
 - reJ <http://rejava.sourceforge.net/>
 - JSwat <https://code.google.com/p/jswat/>
 - Dr. Garbage Tools <http://www.drgarbage.com/index.html>
 - JD-GUI <http://jd.benow.ca/>
 - JAD [http://en.wikipedia.org/wiki/JAD_\(JAvA_Decompiler\)](http://en.wikipedia.org/wiki/JAD_(JAvA_Decompiler))
 - dirtyJOE <http://dirty-joe.com/>

Type and Data Structure Recovering

- Struct Builder: Tool commonly used in game hacking to reverse data structures. This tool is closed source. - <http://www.mpcforum.com/showthread.php?128430-Release-StructBuild>

Miscellaneous Tools

Binary Manipulation Frameworks

Deobfuscation/Unpacking

- PROTECTiON iD: Detects most common application protectors. This tool is closed source. - <http://pid.gamecopyworld.com/>

Cryptography

Visualization

- <http://www2.in.tum.de/votum>
- <http://worrydream.com/MediaForThinkingTheUnthinkable/>
- Cantor Dust - <http://www.youtube.com/watch?v=4bM3Gut1hIk>
- GraphDice: A System for Exploring Multivariate Social Networks - <http://www.aviz.fr/graphdice/>
- Gephi: Open Source Graph Visualization Platform - <https://gephi.org/>

Anti-Debugging / Anti-Reversing

Acknowledgements

- https://events.ccc.de/congress/2013/wiki/Session:Binary_Analysis
- http://www.reddit.com/r/ReverseEngineering/comments/1pvqv5/program_analysis_technology_additions_a
- Original source of list: https://github.com/REMath/literature_review