



Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

rshipp / awesome-malware-analysis

Watch

497

★ Star

3,465

🍴 Fork

997

<> Code

! Issues 0

🔗 Pull requests 0

📁 Projects 0

📊 Insights

## Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

A curated list of awesome malware analysis tools and resources.

malware-analysis

awesome

awesome-list

list

malware-samples

analysis-framework

dynamic-analysis

static-analysis

threat-intelligence

automated-analysis

domain-analysis

network-traffic

threatintel

malware-collection

malware-research

threat-sharing

📁 527 commits

🔗 4 branches

📦 0 releases

👤 70 contributors

Branch: master ▼

New pull request






Find file

Clone or download ▼



rshipp Add @silascutler MalPipe ...

Latest commit c340128 17 hours ago

 <a href="#">.travis.yml</a>	Add openmalware to whitelist	2 years ago
 <a href="#">CONTRIBUTING.md</a>	Add to contributing guidelines	2 years ago
 <a href="#">LICENSE</a>	Add CC-BY-4.0 license	3 years ago
 <a href="#">README.md</a>	Add <a href="#">@silascutler</a> MalPipe	17 hours ago
 <a href="#">恶意软件分析大合集.md</a>	Chinese Translation update	a month ago

## README.md

# Awesome Malware Analysis



A curated list of awesome malware analysis tools and resources. Inspired by [awesome-python](#) and [awesome-php](#).

- [Awesome Malware Analysis](#)
  - [Malware Collection](#)
    - [Anonymizers](#)
    - [Honeypots](#)
    - [Malware Corpora](#)
  - [Open Source Threat Intelligence](#)
    - [Tools](#)
    - [Other Resources](#)
  - [Detection and Classification](#)
  - [Online Scanners and Sandboxes](#)

- [Domain Analysis](#)
  - [Browser Malware](#)
  - [Documents and Shellcode](#)
  - [File Carving](#)
  - [Deobfuscation](#)
  - [Debugging and Reverse Engineering](#)
  - [Network](#)
  - [Memory Forensics](#)
  - [Windows Artifacts](#)
  - [Storage and Workflow](#)
  - [Miscellaneous](#)
  - [Resources](#)
    - [Books](#)
    - [Twitter](#)
    - [Other](#)
  - [Related Awesome Lists](#)
  - [Contributing](#)
  - [Thanks](#)
- 

## Malware Collection

---

## Anonymizers

*Web traffic anonymizers for analysts.*

- [Anonymouse.org](#) - A free, web based anonymizer.
- [OpenVPN](#) - VPN software and hosting solutions.
- [Privoxy](#) - An open source proxy server with some privacy features.
- [Tor](#) - The Onion Router, for browsing the web without leaving traces of the client IP.

## Honeypots

*Trap and collect your own samples.*

- [Conpot](#) - ICS/SCADA honeypot.
- [Cowrie](#) - SSH honeypot, based on Kippo.
- [DemoHunter](#) - Low interaction Distributed Honeypots.
- [Dionaea](#) - Honeypot designed to trap malware.
- [Glastopf](#) - Web application honeypot.
- [Honeyd](#) - Create a virtual honeynet.
- [HoneyDrive](#) - Honeypot bundle Linux distro.
- [Honeytrap](#) - Opensource system for running, monitoring and managing honeypots.
- [Mnemosyne](#) - A normalizer for honeypot data; supports Dionaea.
- [Thug](#) - Low interaction honeyclient, for investigating malicious websites.

## Malware Corpora

*Malware samples collected for analysis.*

- [Clean MX](#) - Realtime database of malware and malicious domains.
- [Contagio](#) - A collection of recent malware samples and analyses.
- [Exploit Database](#) - Exploit and shellcode samples.

- [Infosec - CERT-PA](#) - Malware samples collection and analysis.
- [Malshare](#) - Large repository of malware actively scrapped from malicious sites.
- [MalwareDB](#) - Malware samples repository.
- [Open Malware Project](#) - Sample information and downloads. Formerly Offensive Computing.
- [Ragpicker](#) - Plugin based malware crawler with pre-analysis and reporting functionalities
- [theZoo](#) - Live malware samples for analysts.
- [Tracker h3x](#) - Agregator for malware corpus tracker and malicious download sites.
- [vduddu malware repo](#) - Collection of various malware files and source code.
- [VirusSign](#) - Malware database that detected by many anti malware programs except ClamAV.
- [VirusShare](#) - Malware repository, registration required.
- [VX Vault](#) - Active collection of malware samples.
- [Zeltser's Sources](#) - A list of malware sample sources put together by Lenny Zeltser.
- [Zeus Source Code](#) - Source for the Zeus trojan leaked in 2011.

## Open Source Threat Intelligence

---

### Tools

*Harvest and analyze IOCs.*

- [AbuseHelper](#) - An open-source framework for receiving and redistributing abuse feeds and threat intel.
- [AlienVault Open Threat Exchange](#) - Share and collaborate in developing Threat Intelligence.
- [Combine](#) - Tool to gather Threat Intelligence indicators from publicly available sources.
- [Fileintel](#) - Pull intelligence per file hash.
- [Hostintel](#) - Pull intelligence per host.

- [IntelMQ](#) - A tool for CERTs for processing incident data using a message queue.
- [IOC Editor](#) - A free editor for XML IOC files.
- [iocextract](#) - Advanced Indicator of Compromise (IOC) extractor, Python library and command-line tool.
- [ioc\\_writer](#) - Python library for working with OpenIOC objects, from Mandiant.
- [MalPipe](#) - Malware/IOC ingestion and processing engine, that enriches collected data.
- [Massive Octo Spice](#) - Previously known as CIF (Collective Intelligence Framework). Aggregates IOCs from various lists. Curated by the [CSIRT Gadgets Foundation](#).
- [MISP](#) - Malware Information Sharing Platform curated by [The MISP Project](#).
- [Pulsedive](#) - Free, community-driven threat intelligence platform collecting IOCs from open-source feeds.
- [PyIOCe](#) - A Python OpenIOC editor.
- [RiskIQ](#) - Research, connect, tag and share IPs and domains. (Was PassiveTotal.)
- [threataggregator](#) - Aggregates security threats from a number of sources, including some of those listed below in [other resources](#).
- [ThreatCrowd](#) - A search engine for threats, with graphical visualization.
- [ThreatTracker](#) - A Python script to monitor and generate alerts based on IOCs indexed by a set of Google Custom Search Engines.
- [TIQ-test](#) - Data visualization and statistical analysis of Threat Intelligence feeds.

## Other Resources

*Threat intelligence and IOC resources.*

- [Autoshun \(list\)](#) - Snort plugin and blocklist.
- [Bambenek Consulting Feeds](#) - OSINT feeds based on malicious DGA algorithms.
- [Fidelis Barncat](#) - Extensive malware config database (must request access).
- [CI Army \(list\)](#) - Network security blocklists.

- [Critical Stack- Free Intel Market](#) - Free intel aggregator with deduplication featuring 90+ feeds and over 1.2M indicators.
- [Cybercrime tracker](#) - Multiple botnet active tracker.
- [FireEye IOCs](#) - Indicators of Compromise shared publicly by FireEye.
- [FireHOL IP Lists](#) - Analytics for 350+ IP lists with a focus on attacks, malware and abuse. Evolution, Changes History, Country Maps, Age of IPs listed, Retention Policy, Overlaps.
- [hpfeeds](#) - Honeypot feed protocol.
- [Infosec - CERT-PA lists \(IPs - Domains - URLs\)](#) - Blocklist service.
- [Internet Storm Center \(DSHield\)](#) - Diary and searchable incident database, with a web [API](#). ([unofficial Python library](#)).
- [malc0de](#) - Searchable incident database.
- [Malware Domain List](#) - Search and share malicious URLs.
- [Metadefender Threat Intelligence Feeds](#) - List of the most looked up file hashes from Metadefender malware feed.
- [OpenIOC](#) - Framework for sharing threat intelligence.
- [Proofpoint Threat Intelligence](#) - Rulesets and more. (Formerly Emerging Threats.)
- [Ransomware overview](#) - A list of ransomware overview with details, detection and prevention.
- [STIX - Structured Threat Information eXpression](#) - Standardized language to represent and share cyber threat information. Related efforts from [MITRE](#):
  - [CAPEC - Common Attack Pattern Enumeration and Classification](#)
  - [CybOX - Cyber Observables eXpression](#)
  - [MAEC - Malware Attribute Enumeration and Characterization](#)
  - [TAXII - Trusted Automated eXchange of Indicator Information](#)
- [ThreatMiner](#) - Data mining portal for threat intelligence, with search.
- [threatRECON](#) - Search for indicators, up to 1000 free per month.
- [Yara rules](#) - Yara rules repository.
- [ZeuS Tracker](#) - ZeuS blocklists.

# Detection and Classification

---

## *Antivirus and other malware identification tools*

- [AnalyzePE](#) - Wrapper for a variety of tools for reporting on Windows PE files.
- [Assemblyline](#) - A scalable distributed file analysis framework.
- [BinaryAlert](#) - An open source, serverless AWS pipeline that scans and alerts on uploaded files based on a set of YARA rules.
- [chkrootkit](#) - Local Linux rootkit detection.
- [ClamAV](#) - Open source antivirus engine.
- [Detect-It-Easy](#) - A program for determining types of files.
- [ExifTool](#) - Read, write and edit file metadata.
- [File Scanning Framework](#) - Modular, recursive file scanning solution.
- [hashdeep](#) - Compute digest hashes with a variety of algorithms.
- [Loki](#) - Host based scanner for IOCs.
- [Malfunction](#) - Catalog and compare malware at a function level.
- [Manalyze](#) - Static analyzer for PE executables.
- [MASTIFF](#) - Static analysis framework.
- [MultiScanner](#) - Modular file scanning/analysis framework
- [nsrlookup](#) - A tool for looking up hashes in NIST's National Software Reference Library database.
- [packerid](#) - A cross-platform Python alternative to PEiD.
- [PEV](#) - A multiplatform toolkit to work with PE files, providing feature-rich tools for proper analysis of suspicious binaries.
- [Rootkit Hunter](#) - Detect Linux rootkits.
- [ssdeep](#) - Compute fuzzy hashes.
- [totalhash.py](#) - Python script for easy searching of the [TotalHash.cymru.com](#) database.



- [TrID](#) - File identifier.
- [YARA](#) - Pattern matching tool for analysts.
- [Yara rules generator](#) - Generate yara rules based on a set of malware samples. Also contains a good strings DB to avoid false positives.

## Online Scanners and Sandboxes

---

*Web-based multi-AV scanners, and malware sandboxes for automated analysis.*

- [anlyz.io](#) - Online sandbox.
- [any.run](#) - Online interactive sandbox.
- [AndroTotal](#) - Free online analysis of APKs against multiple mobile antivirus apps.
- [AVCaesar](#) - Malware.lu online scanner and malware repository.
- [Cryptam](#) - Analyze suspicious office documents.
- [Cuckoo Sandbox](#) - Open source, self hosted sandbox and automated analysis system.
- [cuckoo-modified](#) - Modified version of Cuckoo Sandbox released under the GPL. Not merged upstream due to legal concerns by the author.
- [cuckoo-modified-api](#) - A Python API used to control a cuckoo-modified sandbox.
- [DeepViz](#) - Multi-format file analyzer with machine-learning classification.
- [detux](#) - A sandbox developed to do traffic analysis of Linux malwares and capturing IOCs.
- [DRAKVUF](#) - Dynamic malware analysis system.
- [firmware.re](#) - Unpacks, scans and analyzes almost any firmware package.
- [HaboMalHunter](#) - An Automated Malware Analysis Tool for Linux ELF Files.
- [Hybrid Analysis](#) - Online malware analysis tool, powered by VxSandbox.
- [Intezer](#) - Detect, analyze, and categorize malware by identifying code reuse and code similarities.

- [IRMA](#) - An asynchronous and customizable analysis platform for suspicious files.
- [Joe Sandbox](#) - Deep malware analysis with Joe Sandbox.
- [Jotti](#) - Free online multi-AV scanner.
- [Limon](#) - Sandbox for Analyzing Linux Malware.
- [Malheur](#) - Automatic sandboxed analysis of malware behavior.
- [malsub](#) - A Python RESTful API framework for online malware and URL analysis services.
- [Malware config](#) - Extract, decode and display online the configuration settings from common malwares.
- [Malwr](#) - Free analysis with an online Cuckoo Sandbox instance.
- [Metadefender](#) - Scan a file, hash or IP address for malware (free).
- [NetworkTotal](#) - A service that analyzes pcap files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware using Suricata configured with EmergingThreats Pro.
- [Noriben](#) - Uses Sysinternals Procmon to collect information about malware in a sandboxed environment.
- [PacketTotal](#) - PacketTotal is an online engine for analyzing .pcap files, and visualizing the network traffic within.
- [PDF Examiner](#) - Analyse suspicious PDF files.
- [ProcDot](#) - A graphical malware analysis tool kit.
- [Recomposer](#) - A helper script for safely uploading binaries to sandbox sites.
- [sandboxapi](#) - Python library for building integrations with several open source and commercial malware sandboxes.
- [SEE](#) - Sandboxed Execution Environment (SEE) is a framework for building test automation in secured Environments.
- [SEKOIA Dropper Analysis](#) - Online dropper analysis (Js, VBScript, Microsoft Office, PDF).
- [VirusTotal](#) - Free online analysis of malware samples and URLs
- [Visualize\\_Logs](#) - Open source visualization library and command line tools for logs. (Cuckoo, Procmon, more to come...)
- [Zeltser's List](#) - Free automated sandboxes and services, compiled by Lenny Zeltser.

## Domain Analysis

*Inspect domains and IP addresses.*

- [badips.com](#) - Community based IP blacklist service.
- [boomerang](#) - A tool designed for consistent and safe capture of off network web resources.
- [Cymon](#) - Threat intelligence tracker, with IP/domain/hash search.
- [Desenmascara.me](#) - One click tool to retrieve as much metadata as possible for a website and to assess its good standing.
- [Dig](#) - Free online dig and other network tools.
- [dnstwist](#) - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
- [IPinfo](#) - Gather information about an IP or domain by searching online resources.
- [Machinae](#) - OSINT tool for gathering information about URLs, IPs, or hashes. Similar to Automator.
- [mailchecker](#) - Cross-language temporary email detection library.
- [MaltegoVT](#) - Maltego transform for the VirusTotal API. Allows domain/IP research, and searching for file hashes and scan reports.
- [Multi rbl](#) - Multiple DNS blacklist and forward confirmed reverse DNS lookup over more than 300 RBLs.
- [NormShield Services](#) - Free API Services for detecting possible phishing domains, blacklisted ip addresses and breached accounts.
- [SpamCop](#) - IP based spam block list.
- [SpamHaus](#) - Block list based on domains and IPs.
- [Sucuri SiteCheck](#) - Free Website Malware and Security Scanner.
- [Talos Intelligence](#) - Search for IP, domain or network owner. (Previously SenderBase.)
- [TekDefense Automater](#) - OSINT tool for gathering information about URLs, IPs, or hashes.
- [URLQuery](#) - Free URL Scanner.
- [urlscan.io](#) - Free URL Scanner & domain information.
- [Whois](#) - DomainTools free online whois search.

- [Zeltser's List](#) - Free online tools for researching malicious websites, compiled by Lenny Zeltser.
- [ZScalar Zulu](#) - Zulu URL Risk Analyzer.

## Browser Malware

---

Analyze malicious URLs. See also the [domain analysis](#) and [documents and shellcode](#) sections.

- [Firebug](#) - Firefox extension for web development.
- [Java Decompiler](#) - Decompile and inspect Java apps.
- [Java IDX Parser](#) - Parses Java IDX cache files.
- [JSDetox](#) - JavaScript malware analysis tool.
- [jsunpack-n](#) - A javascript unpacker that emulates browser functionality.
- [Krakatau](#) - Java decompiler, assembler, and disassembler.
- [Malzilla](#) - Analyze malicious web pages.
- [RABCDasm](#) - A "Robust ActionScript Bytecode Disassembler."
- [swftools](#) - Tools for working with Adobe Flash files.
- [xxxswf](#) - A Python script for analyzing Flash files.

## Documents and Shellcode

---

Analyze malicious JS and shellcode from PDFs and Office documents. See also the [browser malware](#) section.

- [AnalyzePDF](#) - A tool for analyzing PDFs and attempting to determine whether they are malicious.
- [box-js](#) - A tool for studying JavaScript malware, featuring JScript/WScript support and ActiveX emulation.
- [diStorm](#) - Disassembler for analyzing malicious shellcode.
- [JS Beautifier](#) - JavaScript unpacking and deobfuscation.

- [JS Deobfuscator](#) - Deobfuscate simple Javascript that use eval or document.write to conceal its code.
- [libemu](#) - Library and tools for x86 shellcode emulation.
- [malpdfobj](#) - Deconstruct malicious PDFs into a JSON representation.
- [OfficeMalScanner](#) - Scan for malicious traces in MS Office documents.
- [olevba](#) - A script for parsing OLE and OpenXML documents and extracting useful information.
- [Origami PDF](#) - A tool for analyzing malicious PDFs, and more.
- [PDF Tools](#) - pdfid, pdf-parser, and more from Didier Stevens.
- [PDF X-Ray Lite](#) - A PDF analysis tool, the backend-free version of PDF X-RAY.
- [peepdf](#) - Python tool for exploring possibly malicious PDFs.
- [QuickSand](#) - QuickSand is a compact C framework to analyze suspected malware documents to identify exploits in streams of different encodings and to locate and extract embedded executables.
- [Spidermonkey](#) - Mozilla's JavaScript engine, for debugging malicious JS.

## File Carving

---

*For extracting files from inside disk and memory images.*

- [bulk\\_extractor](#) - Fast file carving tool.
- [EVTXtract](#) - Carve Windows Event Log files from raw binary data.
- [Foremost](#) - File carving tool designed by the US Air Force.
- [hachoir3](#) - Hachoir is a Python library to view and edit a binary stream field by field.
- [Scalpel](#) - Another data carving tool.
- [SFlock](#) - Nested archive extraction/unpacking (used in Cuckoo Sandbox).

## Deobfuscation

---

*Reverse XOR and other code obfuscation methods.*

- [Balbuzard](#) - A malware analysis tool for reversing obfuscation (XOR, ROL, etc) and more.
- [de4dot](#) - .NET deobfuscator and unpacker.
- [ex\\_pe\\_xor](#) & [iheartxor](#) - Two tools from Alexander Hanel for working with single-byte XOR encoded files.
- [FLOSS](#) - The FireEye Labs Obfuscated String Solver uses advanced static analysis techniques to automatically deobfuscate strings from malware binaries.
- [NoMoreXOR](#) - Guess a 256 byte XOR key using frequency analysis.
- [PackerAttacker](#) - A generic hidden code extractor for Windows malware.
- [unpacker](#) - Automated malware unpacker for Windows malware based on WinAppDbg.
- [unxor](#) - Guess XOR keys using known-plaintext attacks.
- [VirtualDeobfuscator](#) - Reverse engineering tool for virtualization wrappers.
- [XORBruteForcer](#) - A Python script for brute forcing single-byte XOR keys.
- [XORSearch](#) & [XORStrings](#) - A couple programs from Didier Stevens for finding XORed data.
- [xortool](#) - Guess XOR key length, as well as the key itself.

## Debugging and Reverse Engineering

---

*Disassemblers, debuggers, and other static and dynamic analysis tools.*

- [angr](#) - Platform-agnostic binary analysis framework developed at UCSB's Seclab.
- [bamfdetect](#) - Identifies and extracts information from bots and other malware.
- [BAP](#) - Multiplatform and open source (MIT) binary analysis framework developed at CMU's Cylab.
- [BARF](#) - Multiplatform, open source Binary Analysis and Reverse engineering Framework.
- [binnavi](#) - Binary analysis IDE for reverse engineering based on graph visualization.
- [Binary ninja](#) - A reversing engineering platform that is an alternative to IDA.

- [Binwalk](#) - Firmware analysis tool.
- [Bokken](#) - GUI for Pyew and Radare. ([mirror](#))
- [Capstone](#) - Disassembly framework for binary analysis and reversing, with support for many architectures and bindings in several languages.
- [codebro](#) - Web based code browser using clang to provide basic code analysis.
- [DECAF \(Dynamic Executable Code Analysis Framework\)](#) - A binary analysis platform based on QEMU. DroidScope is now an extension to DECAF.
- [dnSpy](#) - .NET assembly editor, decompiler and debugger.
- [Evan's Debugger \(EDB\)](#) - A modular debugger with a Qt GUI.
- [Fibratus](#) - Tool for exploration and tracing of the Windows kernel.
- [FPort](#) - Reports open TCP/IP and UDP ports in a live system and maps them to the owning application.
- [GDB](#) - The GNU debugger.
- [GEF](#) - GDB Enhanced Features, for exploiters and reverse engineers.
- [hackers-grep](#) - A utility to search for strings in PE executables including imports, exports, and debug symbols.
- [Hopper](#) - The macOS and Linux Disassembler.
- [IDA Pro](#) - Windows disassembler and debugger, with a free evaluation version.
- [Immunity Debugger](#) - Debugger for malware analysis and more, with a Python API.
- [ILSpy](#) - ILSpy is the open-source .NET assembly browser and decompiler.
- [Kaitai Struct](#) - DSL for file formats / network protocols / data structures reverse engineering and dissection, with code generation for C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby.
- [LIEF](#) - LIEF provides a cross-platform library to parse, modify and abstract ELF, PE and MachO formats.
- [ltrace](#) - Dynamic analysis for Linux executables.
- [objdump](#) - Part of GNU binutils, for static analysis of Linux binaries.
- [OllyDbg](#) - An assembly-level debugger for Windows executables.

- [PANDA](#) - Platform for Architecture-Neutral Dynamic Analysis.
- [PEDA](#) - Python Exploit Development Assistance for GDB, an enhanced display with added commands.
- [pestudio](#) - Perform static analysis of Windows executables.
- [Pharos](#) - The Pharos binary analysis framework can be used to perform automated static analysis of binaries.
- [plasma](#) - Interactive disassembler for x86/ARM/MIPS.
- [PPEE \(puppy\)](#) - A Professional PE file Explorer for reversers, malware researchers and those who want to statically inspect PE files in more detail.
- [Process Explorer](#) - Advanced task manager for Windows.
- [Process Hacker](#) - Tool that monitors system resources.
- [Process Monitor](#) - Advanced monitoring tool for Windows programs.
- [PSTools](#) - Windows command-line tools that help manage and investigate live systems.
- [Pyew](#) - Python tool for malware analysis.
- [PyREBox](#) - Python scriptable reverse engineering sandbox by the Talos team at Cisco.
- [QKD](#) - QEMU with embedded WinDbg server for stealth debugging.
- [Radare2](#) - Reverse engineering framework, with debugger support.
- [RegShot](#) - Registry compare utility that compares snapshots.
- [RetDec](#) - Retargetable machine-code decompiler with an [online decompilation service](#) and [API](#) that you can use in your tools.
- [ROPMEMU](#) - A framework to analyze, dissect and decompile complex code-reuse attacks.
- [SMRT](#) - Sublime Malware Research Tool, a plugin for Sublime 3 to aid with malware analysis.
- [strace](#) - Dynamic analysis for Linux executables.
- [Triton](#) - A dynamic binary analysis (DBA) framework.
- [Udis86](#) - Disassembler library and tool for x86 and x86\_64.
- [Vivisect](#) - Python tool for malware analysis.



- [WinDbg](#) - multipurpose debugger for the Microsoft Windows computer operating system, used to debug user mode applications, device drivers, and the kernel-mode memory dumps.
- [X64dbg](#) - An open-source x64/x32 debugger for windows.

## Network

---

*Analyze network interactions.*

- [Bro](#) - Protocol analyzer that operates at incredible scale; both file and network protocols.
- [BroYara](#) - Use Yara rules from Bro.
- [CapTipper](#) - Malicious HTTP traffic explorer.
- [chopshop](#) - Protocol analysis and decoding framework.
- [CloudShark](#) - Web-based tool for packet analysis and malware traffic detection.
- [Fiddler](#) - Intercepting web proxy designed for "web debugging."
- [Hale](#) - Botnet C&C monitor.
- [Haka](#) - An open source security oriented language for describing protocols and applying security policies on (live) captured traffic.
- [HTTPReplay](#) - Library for parsing and reading out PCAP files, including TLS streams using TLS Master Secrets (used in Cuckoo Sandbox).
- [INetSim](#) - Network service emulation, useful when building a malware lab.
- [Laika BOSS](#) - Laika BOSS is a file-centric malware analysis and intrusion detection system.
- [Malcom](#) - Malware Communications Analyzer.
- [Maltrail](#) - A malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails and featuring an reporting and analysis interface.
- [mitmproxy](#) - Intercept network traffic on the fly.

- [Moloch](#) - IPv4 traffic capturing, indexing and database system.
- [NetworkMiner](#) - Network forensic analysis tool, with a free version.
- [ngrep](#) - Search through network traffic like grep.
- [PcapViz](#) - Network topology and traffic visualizer.
- [Python ICAP Yara](#) - An ICAP Server with yara scanner for URL or content.
- [Squidmagic](#) - squidmagic is a tool designed to analyze a web-based network traffic to detect central command and control (C&C) servers and malicious sites, using Squid proxy server and Spamhaus.
- [Tcpdump](#) - Collect network traffic.
- [tcpick](#) - Track and reassemble TCP streams from network traffic.
- [tcpextract](#) - Extract files from network traffic.
- [Wireshark](#) - The network traffic analysis tool.

## Memory Forensics

---

*Tools for dissecting malware in memory images or running systems.*

- [BlackLight](#) - Windows/MacOS forensics client supporting hiberfil, pagefile, raw memory analysis.
- [DAMM](#) - Differential Analysis of Malware in Memory, built on Volatility.
- [evolve](#) - Web interface for the Volatility Memory Forensics Framework.
- [FindAES](#) - Find AES encryption keys in memory.
- [inVtero.net](#) - High speed memory analysis framework developed in .NET supports all Windows x64, includes code integrity and write support.
- [Muninn](#) - A script to automate portions of analysis using Volatility, and create a readable report.
- [Rekall](#) - Memory analysis framework, forked from Volatility in 2013.
- [TotalRecall](#) - Script based on Volatility for automating various malware analysis tasks.

- [VolDiff](#) - Run Volatility on memory images before and after malware execution, and report changes.
- [Volatility](#) - Advanced memory forensics framework.
- [VolUtility](#) - Web Interface for Volatility Memory Analysis framework.
- [WDBGARK](#) - WinDBG Anti-RootKit Extension.
- [WinDbg](#) - Live memory inspection and kernel debugging for Windows systems.

## Windows Artifacts

---

- [AChoir](#) - A live incident response script for gathering Windows artifacts.
- [python-evt](#) - Python library for parsing Windows Event Logs.
- [python-registry](#) - Python library for parsing registry files.
- [RegRipper](#) ([GitHub](#)) - Plugin-based registry analysis tool.

## Storage and Workflow

---

- [Aleph](#) - Open Source Malware Analysis Pipeline System.
- [CRITs](#) - Collaborative Research Into Threats, a malware and threat repository.
- [FAME](#) - A malware analysis framework featuring a pipeline that can be extended with custom modules, which can be chained and interact with each other to perform end-to-end analysis.
- [Malwarehouse](#) - Store, tag, and search malware.
- [Polichombr](#) - A malware analysis platform designed to help analysts to reverse malwares collaboratively.
- [stoQ](#) - Distributed content analysis framework with extensive plugin support, from input to output, and everything in between.
- [Viper](#) - A binary management and analysis framework for analysts and researchers.

## Miscellaneous

---

- [al-khaser](#) - A PoC malware with good intentions that aims to stress anti-malware systems.
- [DC3-MWCP](#) - The Defense Cyber Crime Center's Malware Configuration Parser framework.
- [FLARE VM](#) - A fully customizable, Windows-based, security distribution for malware analysis.
- [MalSploitBase](#) - A database containing exploits used by malware.
- [Malware Museum](#) - Collection of malware programs that were distributed in the 1980s and 1990s.
- [Malware Organiser](#) - A simple tool to organise large malicious/benign files into a organised Structure.
- [Pafish](#) - Paranoid Fish, a demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do.
- [REMnux](#) - Linux distribution and docker images for malware reverse engineering and analysis.
- [Santoku Linux](#) - Linux distribution for mobile forensics, malware analysis, and security.

## Resources

---

### Books

---

*Essential malware analysis reading material.*

- [Malware Analyst's Cookbook and DVD](#) - Tools and Techniques for Fighting Malicious Code.
- [Practical Malware Analysis](#) - The Hands-On Guide to Dissecting Malicious Software.
- [Practical Reverse Engineering](#) - Intermediate Reverse Engineering.
- [Real Digital Forensics](#) - Computer Security and Incident Response.
- [The Art of Memory Forensics](#) - Detecting Malware and Threats in Windows, Linux, and Mac Memory.

- [The IDA Pro Book](#) - The Unofficial Guide to the World's Most Popular Disassembler.
- [The Rootkit Arsenal](#) - The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System

## Twitter

---

*Some relevant Twitter accounts.*

- Adamb [@Hexacorn](#)
- Andrew Case [@attrc](#)
- Binni Shah [@binitamshah](#)
- Claudio [@botherder](#)
- Dustin Webber [@mephux](#)
- Glenn [@hiddenillusion](#)
- jekil [@jekil](#)
- Jurriaan Bremer [@skier\\_t](#)
- Lenny Zeltser [@lennyzeltser](#)
- Liam Randall [@hectaman](#)
- Mark Schloesser [@repmovsb](#)
- Michael Ligh (MHL) [@iMHLv2](#)
- Monnappa [@monnappa22](#)
- Open Malware [@OpenMalware](#)
- Richard Bejtlich [@taosecurity](#)
- Volatility [@volatility](#)

## Other

---

- [APT Notes](#) - A collection of papers and notes related to Advanced Persistent Threats.
- [File Formats posters](#) - Nice visualization of commonly used file format (including PE & ELF).
- [Honeynet Project](#) - Honeypot tools, papers, and other resources.
- [Kernel Mode](#) - An active community devoted to malware analysis and kernel development.
- [Malicious Software](#) - Malware blog and resources by Lenny Zeltser.
- [Malware Analysis Search](#) - Custom Google search engine from [Corey Harrell](#).
- [Malware Analysis Tutorials](#) - The Malware Analysis Tutorials by Dr. Xiang Fu, a great resource for learning practical malware analysis.
- [Malware Samples and Traffic](#) - This blog focuses on network traffic related to malware infections.
- [Practical Malware Analysis Starter Kit](#) - This package contains most of the software referenced in the Practical Malware Analysis book.
- [RPISEC Malware Analysis](#) - These are the course materials used in the Malware Analysis course at Rensselaer Polytechnic Institute during Fall 2015.
- [WindowsIR: Malware](#) - Harlan Carvey's page on Malware.
- [Windows Registry specification](#) - Windows registry file format specification.
- [/r/csirt\\_tools](#) - Subreddit for CSIRT tools and resources, with a [malware analysis](#) flair.
- [/r/Malware](#) - The malware subreddit.
- [/r/ReverseEngineering](#) - Reverse engineering subreddit, not limited to just malware.
- [Ember](#) - Endgame Malware BENCHMARK for Research, a repository that makes it easy to (re)create a machine learning model that can be used to predict a score for a PE file based on static analysis.

## Related Awesome Lists

---

- [Android Security](#)

- [AppSec](#)
- [CTFs](#)
- [Forensics](#)
- ["Hacking"](#)
- [Honeypots](#)
- [Industrial Control System Security](#)
- [Incident-Response](#)
- [Infosec](#)
- [PCAP Tools](#)
- [Pentesting](#)
- [Security](#)
- [Threat Intelligence](#)
- [YARA](#)

## Contributing

---

Pull requests and issues with suggestions are welcome! Please read the [CONTRIBUTING](#) guidelines before submitting a PR.

## Thanks

---

This list was made possible by:

- Lenny Zeltser and other contributors for developing REMnux, where I found many of the tools in this list;

- Michail Hale Ligh, Steven Adair, Blake Hartstein, and Mather Richard for writing the *Malware Analyst's Cookbook*, which was a big inspiration for creating the list;
- And everyone else who has sent pull requests or suggested links to add here!

Thanks!

