- What is?
  - https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/
  - https://en.wikipedia.org/wiki/Malware_analysis
  - https://sectigostore.com/blog/malware-analysis-what-it-is-how-it-works/
  - https://digitalguardian.com/blog/what-malware-analysis-defining-and-outlining-process-malware-analysis
  - https://www.sans.org/reading-room/whitepapers/malicious/paper/2103
  - https://www.sans.org/blog/how-you-can-start-learning-malware-analysis/
  - https://www.logsign.com/blog/malware-analysis-things-you-should-know/
  - https://www.first.org/global/sigs/malware/
  - https://www.opswat.com/solutions/malware-analysis
  - https://medium.com/techiepedia/malware-analysis-the-art-of-understanding-malware-ffc5e69feb3e
  - https://www.jigsawacademy.com/blogs/cyber-security/malware-analysis/
  - https://astromachineworks.com/what-is-reverse-engineering/#:~:text=Reverse%20engineering%2C%20sometimes%20called%20back,individual%20components%20of%20larger%20products.
  - https://www.youtube.com/watch?v=oxo1FBScEAs
  - https://www.youtube.com/watch?v=a2EkORFcSZo
  - https://www.youtube.com/watch?v=7v7UaMsgg_c
  - https://www.wevolver.com/article/what-is-reverse-engineering-
  - https://www.computerworld.com/article/2585652/reverse-engineering.html
  - https://www.geeksforgeeks.org/software-engineering-reverse-engineering/
- 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.
  - MHN - MHN is a centralized server for management and data collection of honeypots. MHN allows you to deploy sensors quickly and to collect data immediately, viewable from a neat web interface.
  - 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.
  - InQuest Labs - Evergrowing searchable corpus of malicious Microsoft documents.
  - Javascript Mallware Collection - Collection of almost 40.000 javascript malware samples
  - Malpedia - A resource providing rapid identification and actionable context for malware investigations.
  - Malshare - Large repository of malware actively scrapped from malicious sites.
  - 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.
  - VirusBay - Community-Based malware repository and social network.
  - ViruSign - 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.
  - VX Underground - Massive and growing collection of free malware samples.

- Open Source Threat Intelligence
  - 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.
  - ThreatConnect - TC Open allows you to see and share open source threat data, with support and validation from our free community.
  - ThreatCrowd - A search engine for threats, with graphical visualization.
  - ThreatIngestor - Build automated threat intel pipelines sourcing from Twitter, RSS, GitHub, and more.
  - 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.
  - 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.
  - HoneyDB - Community driven honeypot sensor data collection and aggregation.
  - hpfeeds - Honeypot feed protocol.
  - Infosec - CERT-PA lists (IPs - Domains - URLs) - Blocklist service.
  - InQuest REPdb - Continuous aggregation of IOCs from a variety of open reputation sources.
  - InQuest IOCdb - Continuous aggregation of IOCs from a variety of blogs, Github repos, and Twitter.
  - 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 Feed - List of the most looked up file hashes from MetaDefender Cloud.
  - 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
  - SystemLookup - SystemLookup hosts a collection of lists that provide information on the components of legitimate and potentially unwanted programs.
  - ThreatMiner - Data mining portal for threat intelligence, with search.
  - threatRECON - Search for indicators, up to 1000 free per month.
  - ThreatShare - C2 panel tracker
  - Yara rules - Yara rules repository.
  - YETI - Yeti is a platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository.
  - ZeuS Tracker - ZeuS blocklists.

- Detection and Classification
  - 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.
  - capa - Detects capabilities in executable files.
  - chkrootkit - Local Linux rootkit detection.
  - ClamAV - Open source antivirus engine.
  - Detect It Easy(DiE) - A program for determining types of files.
  - Exeinfo PE - Packer, compressor detector, unpack info, internal exe tools.
  - ExifTool - Read, write and edit file metadata.
  - File Scanning Framework - Modular, recursive file scanning solution.
  - fn2yara - FN2Yara is a tool to generate Yara signatures for matching functions (code) in an executable program.
  - Generic File Parser - A Single Library Parser to extract meta information,static analysis and detect macros within the files.
  - hashdeep - Compute digest hashes with a variety of algorithms.
  - HashCheck - Windows shell extension to compute 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
  - Nauz File Detector(NFD) - Linker/Compiler/Tool detector for Windows, Linux and MacOS.
  - nsrllookup - A tool for looking up hashes in NIST's National Software Reference Library database.
  - packerid - A cross-platform Python alternative to PEiD.
  - PE-bear - Reversing tool for PE files.
  - PEframe - PEframe is an open source tool to perform static analysis on Portable Executable malware and malicious MS Office documents.
  - PEV - A multiplatform toolkit to work with PE files, providing feature-rich tools for proper analysis of suspicious binaries.
  - PortEx - Java library to analyse PE files with a special focus on malware analysis and PE malformation robustness.
  - Quark-Engine - An Obfuscation-Neglect Android Malware Scoring System
  - 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.
  - Yara Finder - A simple tool to yara match the file against various yara rules to find the indicators of suspicion.
  - 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.
  - BoomBox - Automatic deployment of Cuckoo Sandbox malware lab using Packer and Vagrant.
  - 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.

- Talks
  - https://www.youtube.com/watch?v=NCO9F7U3d6c
  - https://www.youtube.com/watch?v=LQDRophNaRU
  - https://www.youtube.com/watch?v=285b_DEmvHY
  - https://www.youtube.com/watch?v=kx2xp7IQNSc
  - https://www.youtube.com/watch?v=irhcfHBkfe0
  - https://www.youtube.com/watch?v=D4pc63SeHxI
  - https://www.youtube.com/watch?v=IR0nh-TdpVg
  - https://www.youtube.com/watch?v=mhOWdH2zwMk
  - https://www.youtube.com/watch?v=yf6J8XO_wpY
  - https://www.youtube.com/watch?v=3aCLFzCzPFI
  - https://www.youtube.com/watch?v=q7VZtCUphgg
  - https://www.youtube.com/watch?v=OeG4KBWB-EY
  - https://www.youtube.com/watch?v=QhCzYdqHIrs
  - https://www.youtube.com/watch?v=IF4vJVzk68Y
  - https://www.youtube.com/watch?v=v7XcyCjUTWk&t=8s
  - https://www.youtube.com/watch?v=upe2-1UfEaM
  - https://www.youtube.com/watch?v=xcicWCxdmSU
  - https://www.youtube.com/watch?v=3pH13DxClag
  - https://www.youtube.com/watch?v=qLCE8spVX9Q
  - https://www.youtube.com/watch?v=-cZ7eDV2n5Y
  - https://www.youtube.com/watch?v=B-XELDUtaa8
  - https://www.youtube.com/watch?v=i3I8wtrjYY4
  - https://www.youtube.com/watch?v=9fAnRkJ6N3s
  - https://www.youtube.com/watch?v=TDk2RId8LFo
  - https://www.youtube.com/watch?v=6Chp12sEnWk
  - https://www.youtube.com/watch?v=-MaO-ImteeQ
  - https://www.youtube.com/watch?v=FGCIe6T0Jpc
  - https://www.youtube.com/watch?v=2NawGCUOYT4
  - https://www.youtube.com/watch?v=KSA2ZIDS1ec
  - https://www.youtube.com/watch?v=3pH13DxClag
  - https://www.youtube.com/watch?v=L8lA1pNvcz4
  - https://www.youtube.com/watch?v=BMFCdAGxVN4
  - https://www.youtube.com/watch?v=bU1F5TdzLDM
  - https://www.youtube.com/watch?v=zm7CLH4qrWE
  - https://www.youtube.com/watch?v=VBuWOPHQnZI
  - https://www.youtube.com/watch?v=j_DRFWg1arw
  - https://www.youtube.com/watch?v=y2IhY18f578
  - https://www.youtube.com/watch?v=l5sMPCjtKn0&t=10s
  - https://www.youtube.com/watch?v=Hw2HclZV2Kw
  - https://www.youtube.com/watch?v=EDBtJhQlr_0
  - https://www.youtube.com/watch?v=sObGrnesxv4
  - https://www.youtube.com/watch?v=wDNQ-8aWLO0
  - https://www.youtube.com/watch?v=2kyFLB9aK8Q
  - https://www.youtube.com/watch?v=OcuzaOLs7dM
  - https://www.youtube.com/watch?v=Y6e_ctKqSqM
  - https://www.youtube.com/watch?v=N0Ne623fKWc
  - https://www.youtube.com/watch?v=HlUe0TUHOIc
  - https://www.youtube.com/watch?v=s0Tqi7fuOSU
  - https://www.youtube.com/watch?v=g6dtjtYOw2w
  - https://www.youtube.com/watch?v=Iyeko1GILU4
  - https://www.youtube.com/watch?v=q9KWeXRk8UU
  - https://www.youtube.com/watch?v=icJ8HV22cbc
  - https://www.youtube.com/watch?v=hOKWTeiyy-Q
  - https://www.youtube.com/watch?v=cHo0zI8gtrU
  - https://www.youtube.com/watch?v=YM5I8yR7yCw
  - https://www.youtube.com/watch?v=hbqVNIwfjxo
  - https://www.youtube.com/watch?v=HlUe0TUHOIc

- Online Scanners and Sandboxes
  - 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.
  - malice.io - Massively scalable malware analysis framework.
  - 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.
  - MalwareAnalyser.io - Online malware anomaly-based static analyser with heuristic detection engine powered by data mining and machine learning.
  - Malwr - Free analysis with an online Cuckoo Sandbox instance.
  - MetaDefender Cloud - Scan a file, hash, IP, URL or domain address for malware for 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
  - AbuseIPDB - AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet.
  - 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.
  - PhishStats - Phishing Statistics with search for IP, domain and website title
  - Spyse - subdomains, whois, realted domains, DNS, hosts AS, SSL/TLS info,
  - SecurityTrails - Historical and current WHOIS, historical and current DNS records, similar domains, certificate information and other domain and IP related API and tools.
  - 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.
  - URLhaus - A project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.
  - 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.

Malware and Reverse Engineering Complete Collection by Joas

- Awesome Malware Analysis
  - https://github.com/rshipp/awesome-malware-analysis
  - Browser Malware
    - 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."
    - SWF Investigator - Static and dynamic analysis of SWF applications.
    - swftools - Tools for working with Adobe Flash files.
    - xxxswf - A Python script for analyzing Flash files.
  - Documents and Shellcode
    - 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.
    - InQuest Deep File Inspection - Upload common malware lures for Deep File Inspection and heuristical analysis.
    - JS Beautifier - JavaScript unpacking and deobfuscation.
    - 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
    - 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.
    - PyInstaller Extractor - A Python script to extract the contents of a PyInstaller generated Windows executable file. The contents of the pyz file (usually pyc files) present inside the executable are also extracted and automatically fixed so that a Python bytecode decompiler will recognize it.
    - uncompyle6 - A cross-version Python bytecode decompiler. Translates Python bytecode back into equivalent Python source code.
    - un(i)packer - Automatic and platform-independent unpacker for Windows binaries based on emulation.
    - 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.
  - 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.
- Reverse Engineering
  - https://project-awesome.org/carpedm20/awesome-hacking
  - https://github.com/wtsxDev/reverse-engineering
  - https://github.com/mytechnotalent/Reverse-Engineering
  - https://github.com/tylerha97/awesome-reversing
- Pavel Yosifovich
  - https://www.youtube.com/watch?v=6FzGGKnzO20
  - https://www.youtube.com/watch?v=DHsqb2poGII&t=128s
  - https://www.youtube.com/watch?v=2NawGCUOYT4&t=4s
  - https://www.youtube.com/watch?v=hABj_mrP-no
  - https://www.youtube.com/watch?v=HsievGJQG0w
  - https://www.youtube.com/watch?v=ZDXTdgfC5HE
  - https://www.youtube.com/watch?v=LAkYW5ixvhg
  - https://www.youtube.com/watch?v=h6BXMcRqYhA
  - https://www.youtube.com/watch?v=gBkvAOO2qUY
  - https://twitter.com/zodiacon
  - https://github.com/zodiacon
  - https://www.pluralsight.com/authors/pavel-yosifovich
  - https://www.youtube.com/watch?v=AsSMKL5vaXw
  - https://scorpiosoftware.net/recorded-talks/
  - https://www.youtube.com/watch?v=dXSUrCyWqfw
  - https://www.youtube.com/watch?v=k7nAtrwPhR8
  - https://channel9.msdn.com/Shows/Defrag-Tools/Defrag-Tools-177-Windows-Internals-7th-Edition-Part-1
  - https://www.amazon.it/Pavel-Yosifovich/e/B00A2OTORO
- Filipi Pires
  - https://github.com/filipi86
  - https://twitter.com/FilipiPires?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor
  - https://www.youtube.com/watch?v=HYut-Xaapow
  - https://www.youtube.com/watch?v=TGNtFUkmdBg
  - https://www.youtube.com/watch?v=IqFOL7etSCc&t
  - https://www.youtube.com/watch?v=yAjvfTYEhOw
  - https://www.youtube.com/watch?v=nxlqxLWO16k
  - https://www.youtube.com/watch?v=ixtzZdDvJZA&t
  - https://www.youtube.com/watch?v=9S41xfTGQDo
  - https://www.youtube.com/watch?v=NVXpBy3RNTE
  - https://www.youtube.com/watch?v=bEyzxrLqX6Y
  - https://www.youtube.com/watch?v=F2CIgsBZiFk
  - https://www.youtube.com/watch?v=cev5YF64H58
- My Social Networks
  - https://www.linkedin.com/in/joas-antonio-dos-santos
  - https://twitter.com/C0d3Cr4zy
  - https://medium.com/@joasantonio108
- Vendor Research
  - https://www.youtube.com/c/KasperskyLab/videos
  - https://www.youtube.com/user/TrendMicroInc
  - https://www.youtube.com/user/SecureNetworks
- Mente Binaria
  - https://www.mentebinaria.com.br/treinamentos/programa%C3%A7%C3%A3o-moderna-em-c/
  - https://www.mentebinaria.com.br/treinamentos/an%C3%A1lise-de-malware-online-amo-r11/
  - https://www.mentebinaria.com.br/treinamentos/curso-de-engenharia-reversa-online-cero-r6/
  - https://www.mentebinaria.com.br/treinamentos/curso-de-explora%C3%A7%C3%A3o-de-bin%C3%A1rios-ceb-r8/
  - https://www.mentebinaria.com.br/treinamentos/curso-de-ghidra-r9/
  - https://github.com/mentebinaria/
  - https://github.com/mentebinaria/fundamentos-engenharia-reversa
- Sysinternals
  - http://index-of.co.uk/Malware/WINDOWS%20SYSINTERNALS%20ADMINISTRATOR'S%20REFERENCE.pdf
  - https://ptgmedia.pearsoncmg.com/images/9780735684447/samplepages/9780735684447.pdf
  - https://neprisstore.blob.core.windows.net/sessiondocs/doc_c67d889c-039a-4977-8266-3e025c1408e3.pdf
  - https://docs.microsoft.com/en-us/sysinternals/downloads/
  - https://www.ebooks.com/en-us/book/95824138/troubleshooting-with-the-windows-sysinternals-tools/mark-e-russinovich/
  - https://repo.zenk-security.com/Linux%20et%20systemes%20d.exploitations/Windows%20Internals%20Part%201_6th%20Edition.pdf
  - http://index-of.es/Linux/Other/Windows%20Internals%20Part%202_6th%20Edition.pdf

- C Language
  - https://www.unf.edu/~wkloster/2220/ppts/cprogramming_tutorial.pdf
  - https://www.microsoft.com/en-us/research/wp-content/uploads/1998/01/pal-manual.pdf
  - http://cosmicsoftware.com/pdf/Clanguage.pdf
  - https://public.support.unisys.com/framework/publicterms.aspx?returnurl=%2faseries%2fdocs%2fclearpath-mcp-17.0%2fpdf%2f86002268-206.pdf
  - https://www-personal.acfr.usyd.edu.au/tbailey/ctext/ctext.pdf
  - http://www.cs.columbia.edu/~sedwards/papers/sgi1999c.pdf
  - https://www.tutorialspoint.com/cprogramming/cprogramming_tutorial.pdf
  - http://cslibrary.stanford.edu/101/EssentialC.pdf
  - https://www.engr.uvic.ca/~mech410/ACAD_and_C/c_reference.pdf
  - https://www.gnu.org/software/gnu-c-manual/gnu-c-manual.pdf
  - https://www.youtube.com/watch?v=KJgsSFOSQv0
  - https://www.youtube.com/watch?v=8PopR3x-VMY
  - https://www.youtube.com/watch?v=iT_553vTyzI
  - https://www.youtube.com/watch?v=EjavYOFoJJ0
  - https://www.youtube.com/watch?v=-CpG3oATGIs
  - https://www.youtube.com/watch?v=ZSPZob_1TOk
- Assembly
  - https://www.ic.unicamp.br/~pannain/mc404/aulas/pdfs/Art%20Of%20Intel%20x86%20Assembly.pdf
  - https://www.ic.unicamp.br/~ducatte/mc404/2009/docs/beginner_avr.pdf
  - https://www.tutorialspoint.com/assembly_programming/assembly_tutorial.pdf
  - http://www.ece.utep.edu/courses/web3376/Notes_files/ee3376-assembly.pdf
  - http://www.egr.unlv.edu/~ed/assembly64.pdf
  - https://docs.oracle.com/cd/E19457-01/801-7045/801-7045.pdf
  - http://www.staroceans.org/kernel-and-driver/The.Art.of.Assembly.Language.2nd.Edition.pdf
  - http://index-of.co.uk/Assembly/Assembly_Language_Step_by_Step_en.pdf
  - https://www.cs.princeton.edu/courses/archive/spr18/cos217/lectures/13_Assembly1.pdf
  - http://arantxa.ii.uam.es/~gdrivera/sed/docs/ARMBook.pdf
  - https://en.wikipedia.org/wiki/X86_assembly_language
  - https://github.com/Maijin/awesome-asm
  - https://www.youtube.com/watch?v=75gBFiFtAb8
  - https://www.youtube.com/watch?v=ViNnfoE56V8
  - https://hackr.io/tutorials/learn-assembly-language
  - https://www.coursera.org/lecture/build-a-computer/unit-6-1-assembly-languages-and-assemblers-l4EGm
  - https://www.dca.fee.unicamp.br/~leopini/DISCIPLINAS/EA869/2018-1/c3-ARM-3.pdf
  - https://www.ic.unicamp.br/~ducatte/mc404/2009/docs/beginner_pt.pdf
  - http://www.inf.furb.br/~maw/arquitetura/aula16x4.pdf
  - http://www4.inf.puc-rio.br/~inf1018//corrente/aulas/Assembly-Introducao.pdf
  - https://www.ic.unicamp.br/~pannain/mc404/aulas/pdfs/Art%20Of%20Intel%20x86%20Assembly.pdf
  - https://www.tutorialspoint.com/assembly_programming/assembly_tutorial.pdf
  - http://www1.cs.columbia.edu/~sedwards/classes/2002/w4995-02/assembly.9up.pdf
  - https://home.adelphi.edu/~siegfried/cs174/174l2.pdf
  - https://home.adelphi.edu/~siegfried/cs174/174l3.pdf
  - https://www2.southeastern.edu/Academics/Faculty/kyang/2009/Fall/CMPS293&290/ClassNotes/CMPS293&290ClassNotesChap03.pdf
  - https://www.cs.dartmouth.edu/~sergey/cs258/tiny-guide-to-x86-assembly.pdf
- Debugging and Reverse Engineering
  - Binwalk - Firmware analysis tool.
  - BluePill - Framework for executing and debugging evasive malware and protected executables.
  - 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.
  - Cutter - GUI for Radare2.
  - 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.
  - dotPeek - Free .NET Decompiler and Assembly Browser.
  - 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.
  - Ghidra - A software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate.
  - 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.
  - IDR - Interactive Delphi Reconstructor is a decompiler of Delphi executable files and dynamic libraries.
  - 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.
  - mac-a-mal - An automated framework for mac malware hunting.
  - objdump - Part of GNU binutils, for static analysis of Linux binaries.
  - OllyDbg - An assembly-level debugger for Windows executables.
  - OllyDumpEx - Dump memory from (unpacked) malware Windows process and store raw or rebuild PE file. This is a plugin for OllyDbg, Immunity Debugger, IDA Pro, WinDbg, and x64dbg.
  - 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.
  - Scylla Imports Reconstructor - Find and fix the IAT of an unpacked / dumped PE32 malware.
  - ScyllaHide - An Anti-Anti-Debug library and plugin for OllyDbg, x64dbg, IDA Pro, and TitanEngine.
  - SMRT - Sublime Malware Research Tool, a plugin for Sublime 3 to aid with malware analyis.
  - strace - Dynamic analysis for Linux executables.
  - StringSifter - A machine learning tool that automatically ranks strings based on their relevance for malware analysis.
  - 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
  - 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.
  - FakeNet-NG - Next generation dynamic network analysis tool.
  - 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.
  - Malcolm - Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files) and Zeek logs.
  - 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 - Trach and reassemble TCP streams from network traffic.
  - tcpxtract - Extract files from network traffic.
  - Wireshark - The network traffic analysis tool.
- Memory Forensics
  - 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.
- 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.

- Resources
  - al-khaser - A PoC malware with good intentions that aimes to stress anti-malware systems.
  - CryptoKnight - Automated cryptographic algorithm reverse engineering and classification framework.
  - 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.
  - Tsurugi Linux - Linux distribution designed to support your DFIR investigations, malware analysis and OSINT (Open Source INTelligence) activities.
  - Santoku Linux - Linux distribution for mobile forensics, malware analysis, and security.
  - Learning Malware Analysis - Learning Malware Analysis: Explore the concepts, tools, and techniques to analuze and investigate Windows malware
  - Malware Analyst's Cookbook and DVD - Tools and Techniques for Fighting Malicious Code.
  - Mastering Malware Analysis - Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercime, and IoT attacks
  - Mastering Reverse Engineering - Mastering Reverse Engineering: Re-engineer your ethical hacking skills
  - 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.
  - Rootkits and Bootkits - Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats
  - 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
  - APT Notes - A collection of papers and notes related to Advanced Persistent Threats.
  - 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.
  - 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 Analysis, Threat Intelligence and Reverse Engineering - Presentation introducing the concepts of malware analysis, threat intelligence and reverse engineering. Experience or prior knowledge is not required. Labs link in description.
  - Malware Persistence - Collection of various information focused on malware persistence: detection (techniques), response, pitfalls and the log collection (tools).
  - Malware Samples and Traffic - This blog focuses on network traffic related to malware infections.
  - Malware Search+++ Firefox extension allows you to easily search some of the most popular malware databases
  - 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 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.
  - Android Security
  - AppSec
  - CTFs
  - Forensics
  - "Hacking"
  - Honeypots
  - Industrial Control System Security
  - Incident-Response
  - Infosec
  - PCAP Tools
  - Pentesting
  - Security
  - Threat Intelligence
  - YARA

https://github.com/fabacab/awesome-malware

https://medium.com/@progression.official/awesome-malware-analysis-24266e0cc348

Alexandre Borges

- https://www.youtube.com/watch?v=rcA2tPp4nSU
- https://www.youtube.com/watch?v=uyjMgzqlLoo
- https://www.youtube.com/watch?v=LIBaE6DEgM4
- https://www.youtube.com/watch?v=UB3pVTOSizU
- https://www.youtube.com/watch?v=aYQ4TlcGD2o
- https://www.youtube.com/watch?v=67vesKcxQOQ
- https://www.youtube.com/watch?v=i_xwrmDVzJU
- https://www.youtube.com/watch?v=bCaMuHAJcHw
- https://www.youtube.com/watch?v=1fklt7wL1uI
- https://www.youtube.com/watch?v=WUOVRSZ9Kq4
- https://www.youtube.com/watch?v=20xYpxe8mBg
- https://twitter.com/ale_sp_brazil

T.me/Library_Sec

Fernando Mercês

- https://twitter.com/mer0x36
- https://blog.trendmicro.com.br/author/fernandom/
- https://www.youtube.com/watch?v=I06wFfgn5eE
- https://www.youtube.com/watch?v=cpU9U0sqzh4
- https://www.youtube.com/watch?v=PG510bhFgXY
- https://www.youtube.com/watch?v=bEV9Sc8ONXw
- https://www.youtube.com/watch?v=L_WRNs2IAdY
- https://www.youtube.com/watch?v=fnIzyA047EA
- https://www.youtube.com/watch?v=Sp6Y83rdI5o
- https://www.youtube.com/watch?v=T-EqzfafU80
- https://www.youtube.com/watch?v=p7nGGaTW9CQ

System Architecture

- http://web.mit.edu/6.976/www/notes/Notes1.pdf
- https://www.incose.org/docs/default-source/wasatch-chapter-documents/the-big-happy-family-of-architectures-r0.pdf?sfvrsn=613696c6_2
- https://www.gaudisite.nl/SystemArchitectureProcessPaper.pdf
- https://mitocw.ups.edu.ec/courses/aeronautics-and-astronautics/16-842-fundamentals-of-systems-engineering-fall-2015/lecture-notes/MIT16_842F15_Ses4_Con_Syn.pdf
- https://www.regjeringen.no/contentassets/0de9ab36c5244c3ba9cbafa74c1876a2/securityarchitecture-ecountingofpvotesv1_1.pdf
- https://www.kean.edu/~gchang/tech2920/http___professor.wiley.com_CGI-BIN_JSMPROXY_DOCUMENTDIRECTORDEV+DOCUMENTID&0471715425+DOCUMENTSUBID&1+PRFVALNAME&pdfs_ch02.pdf
- https://incoseuk.org/Documents/zGuides/Z8_System_Architecture.pdf
- https://hal.archives-ouvertes.fr/hal-01407372/document
- https://en.wikipedia.org/wiki/Systems_architecture#:~:text=A%20system%20architecture%20is%20the,and%20behaviors%20of%20the%20system.
- https://thenewstack.io/primer-understanding-software-and-system-architecture/
- https://www.sebokwiki.org/wiki/System_Architecture

Memory Management

- https://www.cs.sjtu.edu.cn/~kzhu/cs490/9/9_MemMan.pdf
- http://mit.bme.hu/~micskeiz/opre/files/eng/03-operating-systems-windows-memory-management.pdf
- https://madoc.bib.uni-mannheim.de/3148/1/InternalsOfWindowsMemoryMangement2.pdf
- https://www.intellectualheaven.com/Articles/WinMM.pdf
- http://efreidoc.fr/L3/Operating%20System/Cours/PDF/2010-11/2010-11.cours.13.memory-management-in-windows-and-linux.op.pdf
- https://www.dc.fi.udc.es/~so-grado/2020-21/Temas/SO-Memoria.pdf
- https://warwick.ac.uk/fac/sci/physics/research/condensedmatt/imr_cdt/students/david_goodwin/teaching/operating_systems/l12_realos.pdf
- http://www.tfzr.uns.ac.rs/Content/files/0/Lab08.pdf
- https://www2.latech.edu/~box/os/ch08.pdf
- https://dcc.ufrj.br/~valeriab/SO-VirtualMemory.pdf
- http://www.cs.umsl.edu/~sanjiv/classes/cs4760/lectures/memory.pdf
- http://www.ifsc.usp.br/~lattice/oldlattice/mod9.1.pdf