**Videos/Learning/Certifications**

X86 Assembly Crash Course (<https://www.youtube.com/watch?v=75gBFiFtAb8>)

Intro to x86 Assembly Language (Part 1) (6 part series) (<https://www.youtube.com/watch?v=wLXIWKUWpSs>)

Modern x64 Assembly Language (<https://www.youtube.com/playlist?list=PLKK11Ligqitg9MOX3-0tFT1Rmh3uJp7kA>)

CS6038/CS5138 Malware Analysis; Department of Electrical Engineering and Computing Systems; College of Engineering and Applied Science; University of Cincinnati (<https://class.malware.re/>)

* YouTube videos (<https://www.youtube.com/playlist?list=PLFvh_k-n27CnAyfsMDowQmogkG5MbZkXz>)

Malware Analysis for N00bs (<https://drive.google.com/file/d/1lSEps7jDX6an_iXJ0Wokdjh0rnBgY9l7/view>)

A reversing tutorial for newbies by lena151 (Part 1 of series) (<https://www.youtube.com/watch?v=wqzZB31zDSs&list=PLcFUp5WYCxVYeR7AgsmjzGW6PjamaY6JO>)

Introduction to Windbg and Debugging Windows (<https://www.youtube.com/playlist?list=PLhx7-txsG6t6n_E2LgDGqgvJtCHPL7UFu>)

Ten Process Injection Techniques (<https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process>)

Hasherezade Injection Techniques Demos (<https://github.com/hasherezade/demos>)

* PE Injection Demos (<https://gist.github.com/hasherezade/e6daa4124fab73543497b6d1295ece10#file-injection_demos-md>)

Black Hat Process Injection Techniques (<https://www.youtube.com/watch?v=xewv122qxnk>)

Odzhan Injection Methods (<https://github.com/odzhan/injection>)

MalwareTech Inline Hooking for Programmers

* Part 1 (<https://www.malwaretech.com/2015/01/inline-hooking-for-programmers-part-1.html>)
* Part 2 (<https://www.malwaretech.com/2015/01/inline-hooking-for-programmers-part-2.html>)

Red Teaming Techniques & Experiments: Code & Process Injection (<https://www.ired.team/offensive-security/code-injection-process-injection>)

Hasherezade’s Windows Kernel Exploitation

* Part 1 (<https://hshrzd.wordpress.com/2017/05/28/starting-with-windows-kernel-exploitation-part-1-setting-up-the-lab/>)
* Part 2 (<https://hshrzd.wordpress.com/2017/06/05/starting-with-windows-kernel-exploitation-part-2/>)
* Part 3 (<https://hshrzd.wordpress.com/2017/06/22/starting-with-windows-kernel-exploitation-part-3-stealing-the-access-token/>)

SpecterOps Methodology for Static Reverse Engineering of Windows Kernel Drivers (<https://posts.specterops.io/methodology-for-static-reverse-engineering-of-windows-kernel-drivers-3115b2efed83>)

Reverse Engineering for Beginners (<https://www.begin.re/>)

R4ndom’s Beginning Reverse Engineering Tutorials (<https://legend.octopuslabs.io/sample-page.html>)

Malware Unicorn (<https://malwareunicorn.org/#/workshops>)

Attack Defense ([https://attackdefense.com](https://attackdefense.com/members))

Pentester Academy (<https://www.pentesteracademy.com/>)

Root-me (<https://www.root-me.org/>)

Pluralsight (<https://www.pluralsight.com/>)

Cybrary (<https://www.cybrary.it/>)

Zero2Automated (<https://courses.zero2auto.com/>)

eCRE (<https://elearnsecurity.com/product/ecre-certification/>)

eCMAP (<https://elearnsecurity.com/product/ecmap-certification/>)

FOR610 (<https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/>)

* GREM (<https://www.giac.org/certification/reverse-engineering-malware-grem>)

CREA (<https://www.iacertification.org/crea_certified_reverse_engineering_analyst.html>)

CREST (<https://crest-approved.org/professional-qualifications/crest-exams/index.html>)

Binary Bomb Lab (<http://zpalexander.com/binary-bomb-lab-phase-1/>)

INE (<https://ine.com/>)

Hasherezade Malware Training Vol 1 (<https://github.com/hasherezade/malware_training_vol1>)

ThisIsSecurity (<https://thisissecurity.stormshield.com/>)

FireEye Trainings (<https://www.fireeye.com/services/training/courses.html>)

InfoSec Institute Skills (<https://www.infosecinstitute.com/skills/>)

Android App Reverse Engineering 101 (<https://www.ragingrock.com/AndroidAppRE/>)

MalwareAnalysisForHedgehogs (<https://www.youtube.com/channel/UCVFXrUwuWxNlm6UNZtBLJ-A>)

OALabs (<https://oalabs.openanalysis.net/>)

* YouTube Videos (<https://www.youtube.com/channel/UC--DwaiMV-jtO-6EvmKOnqg>)

Open Security Training (<https://opensecuritytraining.info/Training.html>)

HackerSploit Malware Analysis Bootcamp (<https://www.youtube.com/watch?v=uHhKkLwT4Mk&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io>)

Nightmare by guyinatuxedo (<https://guyinatuxedo.github.io/>)

Win32 Assembly Tutorials (<https://web.archive.org/web/20171110201344/http://win32assembly.programminghorizon.com/tutorials.html>)

Win32 Assembler Coding for Crackers (<http://woodmann.com/accessroot/arteam/site/e107_plugins/download/download.php?action=view&id=173>)

OverTheWire Wargames (<https://overthewire.org/wargames/>)

* Maze (<https://overthewire.org/wargames/maze/>)
* Vortex (<https://overthewire.org/wargames/vortex/>)
* Semtex (<https://overthewire.org/wargames/semtex/>)
* Manpage (<https://overthewire.org/wargames/manpage/>)
* Drifter (<https://overthewire.org/wargames/drifter/>)

Anarplex.net (<https://anarplex.net/>)

Try Hack Me Malware Analysis (<https://tryhackme.com/module/malware-analysis>)

Blue Team Labs (<https://blueteamlabs.online/>)

PentesterLab (<https://pentesterlab.com/>)

CTF Time (<https://ctftime.org/>)

CNIT 126: Practical Malware Analysis (<https://samsclass.info/126/126_S17.shtml>)

0xPat Malware Development Tutorial (<https://0xpat.github.io/>)

Colin Hardy Malware Videos (<https://www.youtube.com/c/ColinHardy/playlists>)

DuMp-GuY TrIcKsTeR Videos (<https://www.youtube.com/c/DuMpGuYTrIcKsTeR/playlists>)

Hasherezade Videos (<https://www.youtube.com/c/hasherezade/playlists>)

BOLO:Reverse Engineering

* Part 1 (<https://infosecwriteups.com/bolo-reverse-engineering-part-1-basic-programming-concepts-f88b233c63b7>)
* Part 2 (<https://medium.com/@danielabloom/bolo-reverse-engineering-part-2-advanced-programming-concepts-b4e292b2f3e>)

GuidedHacking What is reverse engineering? (<https://guidedhacking.com/threads/ghb2-beginners-guide-to-reverse-engineering.13446/>)

**Samples/Crackmes**

PWN.TN (<https://pwn.tn/>)

crackmes.one (<https://crackmes.one/>)

MalwareBazaar Database (<https://bazaar.abuse.ch/browse/>)

MalShare (<https://malshare.com/index.php>)

TekDefense (<http://www.tekdefense.com/downloads/malware-samples/>)

theZoo AKA Malware DB (<https://thezoo.morirt.com/>)

VirusShare (<https://virusshare.com/>)

Cantagio Malware Dump (<https://contagiodump.blogspot.com/>)

Das Malwerk (<https://dasmalwerk.eu/>)

VXVault (<http://vxvault.net/ViriList.php>)

VirusSign (<https://www.virussign.com/downloads.html>)

MalwareMustDie (<https://www.mediafire.com/malwaremustdie>)

Volatility Memory Samples (<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>)

InQuest Labs ([https://labs.inquest.net/dfi/search/ext/ext\_code##eyJyZXN1bHRzIjpbIn4iLCJmaXJzdFNlZW4iLDEsIiIsW11dfQ==](https://labs.inquest.net/dfi/search/ext/ext_code#eyJyZXN1bHRzIjpbIn4iLCJmaXJzdFNlZW4iLDEsIiIsW11dfQ==))

InQuest Labs Malware Samples (<https://github.com/InQuest/malware-samples>)

Mr. Malware MalwareSamples (<https://github.com/MalwareSamples>) and (<https://www.virussamples.com/>)

Objective-See Mac Malware (<https://objective-see.com/malware.html>)

PolySwarm (<https://polyswarm.network/>)

Yomi by Yoroi (<https://yomi.yoroi.company/submissions/public>)

Practical Malware Analysis Labs for Book (<https://practicalmalwareanalysis.com/labs/>)

ESET Research Malware IoCs (<https://github.com/eset/malware-ioc>)

ANY.RUN Malware Trends (<https://any.run/malware-trends/>)

CyberCrime Tracker (<http://cybercrime-tracker.net/vx.php>)

The Flare-On Challenge (<http://flare-on.com/>)

Reverse Engineering Challenges (<https://challenges.re/>)

Practical Malware Analysis Labs (<https://practicalmalwareanalysis.com/labs/>)

VX Underground (<https://vx-underground.org/samples.html>)

Malware Traffic Analysis (<https://www.malware-traffic-analysis.net/>)

VirusBay (<https://beta.virusbay.io/>)

Malpedia (<https://malpedia.caad.fkie.fraunhofer.de/>)

MalwareTech Beginner Malware Reversing Challenges (<https://www.malwaretech.com/beginner-malware-reversing-challenges>)

Malwarebytes CrackMe (<https://blog.malwarebytes.com/malwarebytes-news/2017/11/how-to-solve-the-malwarebytes-crackme-a-step-by-step-tutorial/>)

Malwarebytes CrackMe 2 (<https://blog.malwarebytes.com/security-world/2018/04/malwarebytes-crackme-2-another-challenge/>)

* Malwarebytes CrackMe2 Sumary (<https://blog.malwarebytes.com/malwarebytes-news/2018/05/malwarebytes-crackme-2-contest-summary/>)

SANS Holiday Hack Challenge (Insert year) (<https://holidayhackchallenge.com/2020/>)

Tuts4you (<https://forum.tuts4you.com/files/categories/>)

Reverse Shell Generator (<https://www.revshells.com/>)

**Tools**

**Debuggers/Disassemblers**

IDA (<https://hex-rays.com/>)

Ghidra (<https://ghidra-sre.org/>)

Binary Ninja (<https://binary.ninja/>)

X64dbg (<https://x64dbg.com/#start>)

Immunity Debugger (<https://www.immunityinc.com/products/debugger/>)

Radare2 (<https://rada.re/n/>)

WinDBG (<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools>)

OllyDbg (<https://www.ollydbg.de/>)

GDB GNU Debugger (<https://www.gnu.org/software/gdb/>)

Capstone (<https://www.capstone-engine.org/>)

Hopper (<https://www.hopperapp.com/>)

dnSpy (<https://github.com/dnSpy/dnSpy>)

Python Dumpers and Decompilers

* Py2Exe Dumper (<https://sourceforge.net/projects/py2exedumper/>)
* Easy Python Decompiler (<https://sourceforge.net/projects/easypythondecompiler/>)
* Py2Exe Binary Editor (<https://sourceforge.net/projects/p2ebe/>)

VB Decompiler (<https://www.vb-decompiler.org/>)

Java Decompiler Project (<https://java-decompiler.github.io/>)

JPEXS (<https://github.com/jindrapetrik/jpexs-decompiler>)

Hiew (<http://hiew.ru/>)

Cutter (<https://cutter.re/>)

.NET Reflector (<https://www.red-gate.com/products/dotnet-development/reflector/>)

JustDecompile (<https://www.telerik.com/products/decompiler.aspx>)

dotPeek (<https://www.jetbrains.com/decompiler/>**)**

Simple Assembly Explorer (<https://github.com/wickyhu/simple-assembly-explorer/releases>)

DisSharp .NET Decompiler (<http://netdecompiler.com/>)

ReFox (<http://www.refox.net/>)

VB Decompiler (<https://www.vb-decompiler.org/>)

IDR (<https://github.com/crypto2011/IDR>)

Dotnet IL Editor (DILE) (<https://sourceforge.net/projects/dile/>)

dirtyJOE (<http://dirty-joe.com/>)

CFR (<http://www.benf.org/other/cfr/>)

ILSpy (<https://github.com/icsharpcode/ILSpy#ilspy------->)

**String and Metadata Tools**

ExifTool (<https://www.sno.phy.queensu.ca/~phil/exiftool/>)

HxD (<https://mh-nexus.de/en/hxd/>)

Free Hex Editor Neo (<https://www.hhdsoftware.com/free-hex-editor>)

StringSifter (<https://github.com/mandiant/stringsifter>)

Hex Workshop (<http://www.hexworkshop.com/overview.html>)

Beyond Compare (<https://www.scootersoftware.com/>)

**Static Analysis Tools**

Exeinfo PE (<http://www.exeinfo.xn.pl/>)

PEiD (<https://www.aldeid.com/wiki/PEiD>)

CFF Explorer Suite (<https://ntcore.com/?page_id=388>)

Cerbero Suite (<https://cerbero.io/>)

Dependency Walker (<http://dependencywalker.com/>)

PE Studio (<https://www.winitor.com/>)

Resource Hacker (<http://angusj.com/resourcehacker/>)

Resource Tuner (<http://www.heaventools.com/resource-tuner.htm>)

ASPack (<http://www.aspack.com/downloads.html>)

Amber (<https://github.com/EgeBalci/Amber>)

Capa (<https://github.com/mandiant/capa>)

FileAlyzer (<https://www.safer-networking.org/products/filealyzer/>)

AnalyzePE (<https://github.com/hiddenillusion/AnalyzePE>)

Chkrootkit (<http://www.chkrootkit.org/>)

Pefile (<https://pypi.org/project/pefile/>)

Hashdeep (<https://github.com/jessek/hashdeep>)

Ssdeep (<https://ssdeep-project.github.io/ssdeep/>)

Malfunction (<https://github.com/Dynetics/Malfunction>)

Nsrllookup (<https://github.com/rjhansen/nsrllookup>)

Pev (<https://pev.sourceforge.io/>)

Rootkit Hunter (<https://sourceforge.net/p/rkhunter/rkh_code/ci/master/tree/files/FAQ>)

TrID (<https://mark0.net/soft-trid-e.html>)

PPEE (puppy) (<https://www.mzrst.com/>)

PE Explorer (<http://www.heaventools.com/PE_Explorer_resource_editor.htm>)

PE Internals (<http://www.andreybazhan.com/pe-internals.html>)

ProtectionID (<https://web.archive.org/web/20210331144912/https://protectionid.net/>)

LordPE (<https://www.aldeid.com/wiki/LordPE>)

Scylla (<https://github.com/NtQuery/Scylla>)

Import REConstructor (<https://www.aldeid.com/wiki/ImpREC>)

DBeaver (<https://dbeaver.io/>)

Total Uninstall (<https://www.martau.com/>)

BinText (<https://www.aldeid.com/wiki/BinText>)

7-Zip (<https://www.7-zip.org/>)

**Dynamic Analysis Tools**

Windows Sysinternals (<https://docs.microsoft.com/en-us/sysinternals/>)

RegShot (<https://sourceforge.net/projects/regshot/>)

API Monitor (<http://www.rohitab.com/apimonitor#Download>)

Noriben (<https://github.com/Rurik/Noriben>)

Reflective DLL Injection (<https://github.com/stephenfewer/ReflectiveDLLInjection>)

Rundll32 (LOLBin) (<https://lolbas-project.github.io/lolbas/Binaries/Rundll32/>)

* Other LOLBin binaries and scripts: <https://lolbas-project.github.io/>

**Memory Forensics Tools**

RAM Capture (<https://docs.microsoft.com/en-us/sysinternals/>)

Belkasoft Live RAM Capturer (<https://belkasoft.com/ram-capturer>)

Comae DumpIt (<https://www.comae.com/dumpit/>)

Nirsoft Memdump (<https://nircmd.nirsoft.net/memdump.html>)

FireEye Redline (<https://www.fireeye.com/services/freeware/redline.html>)

WinPmem (<https://github.com/Velocidex/WinPmem>)

Volatility3 (<https://github.com/volatilityfoundation/volatility3/>)

* Malhunt (<https://github.com/andreafortuna/malhunt>)
* AutoTimeliner (<https://github.com/andreafortuna/autotimeliner>**)**

Rekall (<http://www.rekall-forensic.com/releases>)

**Incident Response Tools**

FireEye IOC Editor (<https://www.fireeye.com/services/freeware/ioc-editor.html>)

GRR Rapid Response (<https://github.com/google/grr>)

Velociraptor (<https://github.com/Velocidex/velociraptor>)

YARA (<https://virustotal.github.io/yara/>)

* Yara Rules (<https://github.com/Yara-Rules>)
* Yara\_Merger (<https://github.com/lsoumille/Yara_Merger>)
* Yara-Endpoint (<https://github.com/Yara-Rules/yara-endpoint>)
* Loki (<https://github.com/Neo23x0/Loki>)
* OsQuery (<https://osquery.io/>)

ClamAV (<https://www.clamav.net/>)

BinaryAlert (<https://github.com/airbnb/binaryalert>)

yarGen (<https://github.com/Neo23x0/yarGen>)

**Network Tools**

Wireshark (<https://www.fireeye.com/services/freeware/ioc-editor.html>)

Fiddler (<https://www.telerik.com/fiddler>)

Xplico (<https://www.xplico.org/>)

FireEye ApateDNS (<https://www.fireeye.com/services/freeware/apatedns.html>)

WinDump (<https://www.winpcap.org/windump/install/default.htm>)

CaptureBAT (<https://www.honeynet.org/projects/old/capture-bat/>)

NetworkMiner (<https://www.netresec.com/?page=NetworkMiner>)

PassiveDNS (<https://github.com/gamelinux/passivedns>)

Stenographer (<https://github.com/google/stenographer>)

Burp Suite (<https://portswigger.net/burp>)

Paessler PRTG Network Monitor (<https://www.paessler.com/packet_capture>)

TCPDump (<https://www.tcpdump.org/>)

WinDump (<https://www.winpcap.org/windump/>)

Fiddler (<https://www.telerik.com/fiddler>)

Capsa Free Network Analyzer (<https://www.colasoft.com/capsa-free/>)

CapAnalysis (<https://www.capanalysis.net/ca/>)

TCPView (<https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview>)

HTTP Analyzer (<https://www.ieinspector.com/httpanalyzer/>)

Mitmproxy (<https://mitmproxy.org/>)

**Visual Analysis Tools**

ProcDOT (<https://procdot.com/index.htm>)

Graphviz (<https://graphviz.org/download/>)

XDot (<https://github.com/jrfonseca/xdot.py>)

**Frameworks**

Viper Framework (<https://github.com/viper-framework/viper>)

Assemblyline (<https://bitbucket.org/cse-assemblyline/assemblyline/src/master/>)

File Scanning Framework (<https://github.com/EmersonElectricCo/fsf>)

Mastiff (<https://github.com/KoreLogicSecurity/mastiff>)

MultiScanner (<https://github.com/mitre/multiscanner>)

**Extractors/(De)obfuscators/(Un)packers**

Universal Extractor (<https://www.legroom.net/software/uniextract>)

MultiExtractor (<https://www.multiextractor.com/>)

UPX (<https://upx.github.io/>)

Qunpack (<https://www.npmjs.com/package/qunpack>)

GUnPacker (<https://webscene.ir/tools/show/GUnPacker-v0.5>)

Innoextract (<https://constexpr.org/innoextract/>)

RDG Packer Detector (<http://www.rdgsoft.net/>)

De4dot (<https://github.com/de4dot/de4dot>)

Heavily Obfuscated UnConfuserEx Tool (<https://gist.github.com/Rottweiler/44fe4461a4552acf303a>)

**Security Researcher Toolsets**

FireEye Freeware (<https://www.fireeye.com/services/freeware.html>)

Horsicq Tools (<https://horsicq.github.io/>)

Novirusthanks Tools (<https://www.novirusthanks.org/browse-by/malware-analysis-tools/>)

Hasherezade Tools (<https://hasherezade.github.io/>)

Eric Zimmerman’s Tools (<https://ericzimmerman.github.io/#!index.md>)

Didier Stevens Tools (<https://blog.didierstevens.com/my-software/>)

The Malware Analyst Pack (<http://sandsprite.com/iDef/MAP/>**)**

**Editors**

Notepad++ (<https://notepad-plus-plus.org/downloads/>)

Atom (<https://atom.io/>)

Sublime Text (<https://www.sublimetext.com/>)

010 Editor (<https://www.sweetscape.com/010editor/>)

**Online Sandboxes/Analyzers**

**File Analyzers**

VirusTotal (<https://www.virustotal.com/gui/home/upload>)

Hybrid Analysis (<https://www.hybrid-analysis.com/>)

Yomi By Yoroi (<https://yomi.yoroi.company/upload>)

CAPE Sandbox (<https://capesandbox.com/>)

Intezer Analyze (<https://analyze.intezer.com/>)

ANY.RUN (<https://any.run/>)

Jotti’s Malware Scan (<https://virusscan.jotti.org/>)

PolySwarm (<https://polyswarm.network/>)

Manalyzer (<https://manalyzer.org/>)

UnpacMe (<https://www.unpac.me/#/>)

Hatching Triage (<https://tria.ge/>)

Joe Sandbox (<https://www.joesandbox.com/#windows>)

IRIS-H Digital Forensics (<https://iris-h.services/pages/submit>)

Valkyrie (<https://valkyrie.comodo.com/>)

FileScan.IO (<https://www.filescan.io/scan>)

GateWatcher Intelligence (<https://intelligence.gatewatcher.com/upload_sample/>)

InQuest Labs (<https://labs.inquest.net/>)

Cuckoo Sandbox (<https://sandbox.pikker.ee/>)

ThreatPoint (<https://threatpoint.checkpoint.com/ThreatPortal/emulation>)

SecondWrite DeepView Sandbox (<https://www.secondwrite.com/products/deepview-sandbox/>)

OPSWAT MetaDefender Cloud (<https://metadefender.opswat.com/?lang=en>)

Analz (<https://sandbox.anlyz.io/dashboard>)

TyLabs Quicksand (<https://scan.tylabs.com/>)

Kaspersky OpenTip (<https://opentip.kaspersky.com/>)

IOBit (<https://cloud.iobit.com/index.php>)

FortiGuard Online Scanner (<https://www.fortiguard.com/faq/onlinescanner>)

VirScan (<https://www.virscan.org/>)

F-Secure (<https://www.f-secure.com/us-en/business/support-and-downloads/submit-a-sample>)

Dr. Web Scan File (<https://vms.drweb.com/scan_file/?lng=en>)

CheckPoint Research SandBlast (<https://threatpoint.checkpoint.com/ThreatPortal/emulation>)

**Packet Analyzers**

A-Packets (<https://apackets.com/upload>)

PacketTotal (<https://packettotal.com/>)

MyCERT PCAP Analyzer (<https://pcap.honeynet.org.my/v1/>)

Online PCAP Viewer ([https://fileproinfo.com/tools/viewer/pcap#](https://fileproinfo.com/tools/viewer/pcap))

**Domain/URL/IP Analyzers**

Dr. Web Check Link (<https://vms.drweb.com/online/>)

Talos IP & Domain Reputation (<https://talosintelligence.com/reputation_center>)

IPVoid (<https://www.ipvoid.com/>)

BrightCloud (<https://www.brightcloud.com/tools/url-ip-lookup.php>)

Google Safe Browsing Status (<https://transparencyreport.google.com/safe-browsing/search?hl=en>)

DomainTools Whois Lookup (<https://whois.domaintools.com/>)

MXToolbox (<https://mxtoolbox.com/domain/>)

IPQualityScore Domain Reputation Test (<https://www.ipqualityscore.com/domain-reputation>)

WhoisXMLAPI (<https://main.whoisxmlapi.com/>)

URLVoid (<https://www.urlvoid.com/>)

Pulsedive (<https://pulsedive.com/>)

VirusTotal (<https://www.virustotal.com/gui/home/url>)

AbuseIPDB (<https://www.abuseipdb.com/>)

CheckPhish (<https://checkphish.ai/>)

Desenmascara.me (<http://desenmascara.me/>)

Netcore Tools Blocklist Checker (<https://grademyemail.co/email-blocklist-checker>)

FortiGuard Labs Web Filter Lookup (<https://www.fortiguard.com/webfilter>)

IBM X-Force Exchange (<https://exchange.xforce.ibmcloud.com/>)

Joe Sandbox URL Lookup (<https://www.joesandbox.com/#windows>)

IronScales Phishing URL Scanner (<https://ironscales.com/free-url-scanner/#/>)

Is It Hacked? (<https://www.isithacked.com/>)

IsItPhishing (<https://isitphishing.org/>)

Kaspersky Lookup (<https://opentip.kaspersky.com/>)

Norton SafeWeb (<https://safeweb.norton.com/>)

Palo Alto Networks Test a Site (<https://urlfiltering.paloaltonetworks.com/>)

PhishTank (<https://www.phishtank.com/>)

OpenPhish (<https://openphish.com/phishing_feeds.html>)

Email Veritas (<https://www.emailveritas.com/url-checker>)

Polyswarm.Network (<https://polyswarm.network/>)

MalwareDomainList (<https://www.malwaredomainlist.com/mdl.php>)

MalwareURL (<https://www.malwareurl.com/listing-urls.php>)

McAfee TrustSource (<https://www.trustedsource.org/>)

AlienVault (<https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1>)

RiskIQ (<https://community.riskiq.com/home>)

Quttera (<https://quttera.com/>)

ScamAdviser (<https://www.scamadviser.com/>)

SecurityTrails (<https://securitytrails.com/#search>)

Sucuri (<https://sitecheck.sucuri.net/>)

TrendMicro (<https://global.sitesafety.trendmicro.com/>)

ThreatSTOP (<https://www.threatstop.com/check-ioc>)

URLScan (<https://urlscan.io/>)

ThreatMiner (<https://www.threatminer.org/>)

Symantec BlueCoat (<https://sitereview.bluecoat.com/#/>)

ZScaler (<https://zulu.zscaler.com/>)

zveloLIVE (<https://tools.zvelo.com/>)

ICANN Lookup (<https://lookup.icann.org/>)

GoDaddy Whois Lookup (<https://www.godaddy.com/whois>)

Who.is (<https://who.is/>)

Network Tools WHOIS lookup tool (<https://network-tools.com/whois/>)

WHOis.net (<https://www.whois.net/>)

Whois.com (<https://www.whois.com/whois/>)

Network Solutions WHOIS Lookup (<https://www.networksolutions.com/domains/whois?s_tnt=576480%3A0%3A0&adobe_mc_sdid=SDID%3D72114F1D8522FDF2-4CEE8AA19184213D%7CMCORGID%3DA8B5776A5245B4360A490D44%40AdobeOrg%7CTS%3D1633911841&adobe_mc_ref=https%3A%2F%2Fwww.networksolutions.com%2F>)

**Ransomware Analyzers/Tools**

ID Ransomware (<https://id-ransomware.malwarehunterteam.com/>)

No More Ransom Crypto Sheriff (<https://www.nomoreransom.org/crypto-sheriff.php?lang=en>)

No More Ransom Decryption Tools (<https://www.nomoreransom.org/en/decryption-tools.html>)

Emsisoft Free Ransomware Decryption Tool (<https://www.emsisoft.com/ransomware-decryption-tools/>)

Kaspersky Ransomware Decryptors (<https://noransom.kaspersky.com/>)

Trend Micro Ransomware File Decryptor (<https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor>)

**Online Hash Checkers**

Malware Hash Registry (<https://hash.cymru.com/>)

Talos File Reputation (<https://talosintelligence.com/talos_file_reputation>)

Name That Hash (<https://nth.skerritt.blog/>)

Hashdd (<https://hashdd.com/>)

**Virtual Machines/Linux Distros**

Virtualbox (<https://www.virtualbox.org/>)

VMWare (<https://www.vmware.com/>)

SIFT Workstation (<https://www.sans.org/tools/sift-workstation/>)

Tsuguri (<https://tsurugi-linux.org/>)

Kali (<https://www.kali.org/>)

REMnux (<https://remnux.org/>)

Security Onion (<https://securityonionsolutions.com/>)

FLARE VM (<https://github.com/mandiant/flare-vm>)

CSI Linux (<https://csilinux.com/>)

Parrot OS (<https://www.parrotsec.org/>)

BackBox (<https://www.backbox.org/>)

BlackArch Linux (<https://blackarch.org/index.html>)

CAINE (<https://www.caine-live.net/>)

ForLEx (<http://www.forlex.it/>)

Network Security Toolkit (<https://www.networksecuritytoolkit.org/nst/index.html>)

ADIA (<https://forensics.cert.org/appliance/README.html>)

Pentoo (<https://www.pentoo.ch/>)

Fedora Security Spin (<https://fedoraproject.org/wiki/Security_Lab>)

ArchStrike (<https://archstrike.org/>)

Sandboxie (<https://sandboxie-plus.com/sandboxie/>)

Re\_lab (<https://github.com/cboin/re_lab>)

**Books/PDFs**

Intel 64 and IA-32 Architectures Software Developer’s Manual Volume 2 (<https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf>)

Practical Malware Analysis (<https://nostarch.com/malware>)

Reversing Secrets of Reverse Engineering (<https://www.amazon.com/Reversing-Secrets-Engineering-Eldad-Eilam/dp/0764574817>)

RE4B/Understanding Assembly Language (challenges.re handbook) (<https://beginners.re/>)

The Art of Assembly Language (<https://nostarch.com/assembly2.htm>)

Learning Malware Analysis (<https://www.packtpub.com/product/learning-malware-analysis/9781788392501>)

Malware Analyst’s Cookbook (<https://www.amazon.com/dp/0470613033>)

Mastering Malware Analysis (<https://www.packtpub.com/product/mastering-malware-analysis/9781789610789>)

Mastering Reverse Engineering (<https://www.packtpub.com/product/mastering-reverse-engineering/9781788838849>)

Practical Reverse Engineering (<https://www.amazon.com/gp/product/1118787315/>)

Real Digital Forensics (<https://www.amazon.com/gp/product/0321240693>)

Rootkits and Bootkits (<https://nostarch.com/rootkits>)

The Art of Memory Forensics (<https://www.amazon.com/dp/1118825098>)

Malware Reverse Engineering Handbook (<https://ccdcoe.org/library/publications/malware-reverse-engineering-handbook/>)

The IDA Pro Book (<https://nostarch.com/idapro2.htm>)

The Rootkit Arsenal (<https://www.amazon.com/dp/144962636X>)

Rootkits: Subverting the Windows Kernel (<https://www.amazon.com/Rootkits-Subverting-Windows-Greg-Hoglund/dp/0321294319/ref=sr_1_1?s=books&ie=UTF8&qid=1347658166&sr=1-1&keywords=Rootkits>)

Malware Data Science (<https://nostarch.com/malwaredatascience>)

Practical Forensic Imaging (<https://nostarch.com/forensicimaging>)

Practical Binary Analysis (<https://nostarch.com/binaryanalysis>)

Practical Linux Forensics (<https://nostarch.com/practical-linux-forensics>)

Practical Packet Analysis (<https://nostarch.com/packetanalysis3>)

The Art of Mac Malware (<https://nostarch.com/art-mac-malware>)

The Ghidra Book (<https://nostarch.com/GhidraBook>)

Gray Hat Python (<https://nostarch.com/ghpython.htm>)

Windows Malware Analysis Essentials (<https://www.amazon.com/Windows-Malware-Analysis-Essentials-Victor/dp/1785281518>)

Malware Analysis Techniques (<https://www.amazon.com/Malware-Analysis-Techniques-adversarial-software-ebook/dp/B093QJ9Q2B>)

Malware Analysis and Detection Engineering (<https://www.amazon.com/Malware-Analysis-Detection-Engineering-Comprehensive/dp/1484261925>)

X86 Opcode and Instruction Reference (<http://ref.x86asm.net/>)

X86-64 Intel Instruction set in JSON format (<https://github.com/astocko/json-x86-64>)

X86 and amd64 instruction reference (<https://www.felixcloutier.com/x86/>)

iOSAppReverseEngineering (<https://github.com/iosre/iOSAppReverseEngineering>)

Reversing iOS Apps (<https://s3.amazonaws.com/s3.synack.com/T2_reversingIOSApps.pdf>)

Corkami PE File Infographics (<https://github.com/corkami/pics>)

* PE101 (<https://raw.githubusercontent.com/corkami/pics/master/binary/PE101.png>)
* PE102 (<https://raw.githubusercontent.com/corkami/pics/master/binary/PE102.png>)

Windows Internals Part 1 (<https://www.microsoftpressstore.com/store/windows-internals-part-1-system-architecture-processes-9780735684188>)

Windows Internals Part 2 (<https://www.microsoftpressstore.com/store/windows-internals-part-2-9780135462331>)

Ero Carrera’s PE File Format Graphs (<http://blog.dkbza.org/>)

CodeBreakers Magazine Portable Executable File Format – A Reverse Engineer View (<http://index-of.es/Windows/pe/CBM_1_2_2006_Goppit_PE_Format_Reverse_Engineer_View.pdf>)

C Programming Language (<https://www.amazon.com/Programming-Language-2nd-Brian-Kernighan/dp/0131103628>)

C++ Programming Language (<https://www.amazon.com/C-Programming-Language-4th/dp/0321563840>)

Safebreach Labs Windows Process Injection in 2019 (<https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf>)

Windows Kernel Programming (<https://leanpub.com/windowskernelprogramming>)

* Samples (<https://github.com/zodiacon/windowskernelprogrammingbook>)

Sekoia Rootkit Analysis Use Case on HideDRV (<http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf>)

Art of Computer Virus Research and Defense (<https://www.amazon.com/SZOR-VIRUS-DEFENSE-Symantec-Press-ebook/dp/B003DQ4WLQ/>)

Hacker Disassembling Uncovered (<https://www.amazon.com/Hacker-Disassembling-Uncovered-Kris-Kaspersky/dp/1931769648/>)

Windows System Programming (<https://www.amazon.com/Programming-Paperback-Addison-Wesley-Microsoft-Technology/dp/0134382250>)

Katjahahn Master’s Thesis: Robust Static Analysis of Portable Executable Malware (<https://github.com/katjahahn/PortEx/blob/master/masterthesis/masterthesis.pdf>)

* PortEx (<https://github.com/katjahahn/PortEx>)

Programming Windows (<https://www.amazon.com/Programming-Windows%C2%AE-Fifth-Microsoft/dp/157231995X/ref=ntt_at_ep_dpt_3/185-4090500-7860862>**)**

**PE Header Resources**

Microsoft Docs PE Format (<https://docs.microsoft.com/en-us/windows/win32/debug/pe-format>)

Corkami PE File Infographics (<https://github.com/corkami/pocs/tree/master/PE>)

* PE Format page (<https://github.com/corkami/docs/blob/master/PE/PE.md>)

Malwology PE Structure (<https://malwology.com/category/pe-structure/>)

Ivanlef0u PE File Structure (<https://ivanlef0u.fr/repo/madchat/vxdevl/papers/winsys/pefile/pefile.htm>)

LIEF Format Tutorials (<https://lief-project.github.io/doc/stable/tutorials/01_play_with_formats.html>)

Johannes Plachy PE File Format (<https://blog.kowalczyk.info/articles/pefileformat.html>)

Infosec Institute’s Malware Researcher’s Handbook (<https://resources.infosecinstitute.com/topic/2-malware-researchers-handbook-demystifying-pe-file/>)

An In-Depth Look into the Win32 Portable Executable File Format, Part 1 (<https://bytepointer.com/resources/pietrek_in_depth_look_into_pe_format_pt1.htm>)

An In-Depth Look into the Win32 Portable Executable File Format, Part 2 (<https://bytepointer.com/resources/pietrek_in_depth_look_into_pe_format_pt2.htm>)

Peering Inside the PE: A Tour of the Win32 Portable Executable File Format (<https://docs.microsoft.com/en-us/previous-versions/ms809762(v=msdn.10)?redirectedfrom=MSDN>)

**Packers/Anti-Debug Resources**

Hasherezade’s Malware Unpacking Series (<https://www.youtube.com/playlist?list=PL3CZ2aaB7m83eYTAVV2knNglB8I4y5QmH>)

Check Point Research Anti-Debug Tricks (<https://anti-debug.checkpoint.com/>)

The Art of Unpacking (<https://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf>)

Malware Crypters – the Deceptive First Layer (<https://blog.malwarebytes.com/threat-analysis/2015/12/malware-crypters-the-deceptive-first-layer/>)

Tuts4You IDA Disassembler and Debugging Tutorials (<https://forum.tuts4you.com/files/category/78-tutorials-documents/>)

The “Ultimate” Anti-Debugging Reference (<https://anti-reversing.com/Downloads/Anti-Reversing/The_Ultimate_Anti-Reversing_Reference.pdf>)

Pafish (<https://github.com/a0rtega/pafish>)

**Misc. Resources**

MITRE ATT&CK Matrix (<https://attack.mitre.org/>)

Regex Tools:

* RegExr (<https://regexr.com/>)
* RegEx Tester (<https://www.regextester.com/>)
* Regex101 (<https://regex101.com/>)
* Debuggex (<https://www.debuggex.com/>)
* MyRegexTester (<https://myregextester.com/index.php>)
* Regexper (<https://regexper.com/>)
* RexV.2 (<http://www.rexv.org/>)
* RegexGenerator++ (<http://regex.inginf.units.it/>)
* RegExLib (<https://regexlib.com/?AspxAutoDetectCookieSupport=1>)
* RegexGuide (<https://regex.guide/>)

Hex/Decimal/ASCII/Binary Converters:

* Rapid Tables (<https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html>)
* OnlineHexTools (<https://onlinehextools.com/>)
* Branah (<https://www.branah.com/ascii-converter>)
* IBM (<https://www.ibm.com/docs/en/aix/7.1?topic=adapters-ascii-decimal-hexadecimal-octal-binary-conversion-table>)
* Calculators.tech (<https://www.calculators.tech/ascii-to-decimal>)
* CalculatorX (<https://www.calculatorx.com/convert/number/ascii-hex-bin-dec-converter.htm>)
* EasyUnitConverter (<https://www.easyunitconverter.com/ascii-hex-binary-decimal-converter>**)**

MalwareTech Creating a Simple Free Malware Analysis Environment (<https://www.malwaretech.com/2017/11/creating-a-simple-free-malware-analysis-environment.html>)

Kernelmode.Info Forum (<https://www.kernelmode.info/forum/>)

Todd Cullum Research GIANT Intro of Windows Malware Analysis Tools (<https://toddcullumresearch.com/2017/07/01/todds-giant-intro-of-windows-malware-analysis-tools/>)

Hack+ (<https://hack.plus/>)

MÖBIUS STRIP REVERSE ENGINEERING (<https://www.msreverseengineering.com/>)

Maltiverse (<https://maltiverse.com/search>)