

CRA-WIN Tool List

Corey Forman (digitalsleuth)

2023-03-04

Acquisition and Analysis

Active Disk Editor

Website: <https://www.disk-editor.org>

Description: File / Disk Editor and Template Manager

Author: LSoft Technologies

License: <https://www.lsoft.net/terms/>

Version: 23.0.1

Notes:

Arsenal Image Mounter

Website: <https://arsenalrecon.com>

Description: Forensic Image Mounter

Author: Arsenal Recon

License: <https://github.com/ArsenalRecon/Arsenal-Image-Mounter/blob/master/LICENSE.md>

Version: 3.9.228

Notes:

Autopsy

Website: <https://www.sleuthkit.org>

Description: GUI based application for image analysis

Author: Brian Carrier / Basis Technology

License: Apache 2.0 (<https://github.com/sleuthkit/autopsy/blob/master/README.txt>)

Version: 4.20.0

Notes:

Cerbero Suite

Website: <https://cerbero.io>

Description: Application Analysis for Reverse Engineering

Author: Cerbero.io

License:

Version: 6.1.1

Notes:

FTK Imager

Website: <https://www.exterro.com>

Description: Forensic Image Acquisition and Triage tool

Author: Exterro Inc / AccessData

License: EULA

Version: 4.7.1.2

Notes:

Magnet ACQUIRE

Website: <https://www.magnetforensics.com>

Description: Forensic Acquisition Tool

Author: Jad Saliba - Magnet Forensics

License: EULA

Version: 2.59.0.32716

Notes:

Magnet AXIOM

Website: <https://www.magnetforensics.com>

Description: Evidence Acquisition and Analysis toolset

Author: Jad Saliba - Magnet Forensics

License: EULA

Version: 6.8.0.33717

Notes:

Magnet Chromebook Acquisition Assistant

Website: <https://www.magnetforensics.com>

Description: Chromebook Acquisition Tool

Author: Magnet Forensics

License: EULA

Version: 1.06

Notes:

Tableau Imager

Website: <https://opentext.com>

Description: Disk / Device Imager

Author: OpenText

License: EULA

Version: 20.3.3

Notes:

X-Ways Forensics

Website: <https://x-ways.net>

Description: Forensic Analysis Software

Author: Stefan Fleischmann

License: License Dependent - <https://www.x-ways.net/terminology.html>

Version: 20.7 SR-2 x64

Notes:

Browsers

Firefox

Website: <https://www.mozilla.org>

Description: Mozilla web browser

Author: Mozilla Foundation

License: Mozilla Public License 2.0 (<https://www.mozilla.org/en-US/MPL/>)

Version: 107.0.1

Notes:

Google Chrome

Website: <https://www.google.com>

Description: Google Web Browser

Author: Google
License: <https://policies.google.com/terms>
Version: 108.0.5359.72
Notes:

Databases

DB Browser for SQLite

Website: <https://sqlitebrowser.org>
Description: SQLite Database Browser
Author: <https://sqlitebrowser.org/about/>
License: Mozilla Public License v2 (<https://github.com/sqlitebrowser/sqlitebrowser/blob/master/LICENSE>)
Version: 3.12.2
Notes:

dbeaver

Website: <https://dbeaver.io>
Description: Database analysis tool
Author: Serge Rider and Contributors (<https://github.com/dbeaver/dbeaver/graphs/contributors>)
License: Apache License 2.0 (<https://github.com/dbeaver/dbeaver/blob/devel/LICENSE.md>)
Version: 22.2.5
Notes:

SQLiteStudio

Website: <https://sqlitestudio.pl/>
Description: SQLite Database browser, creator, editor
Author: Pawel Salawa
License: GNU General Public License v3 (<https://github.com/pawelsalawa/sqlitestudio/blob/master/LICENSE>)
Version: 3.4.1
Notes:

SysTools SQL MDF Viewer

Website: <https://www.systoolsgroup.com>
Description: SQL MDF Viewer
Author: SysTools Group
License: EULA (<https://www.systoolsgroup.com/eula.html>)
Version: 11.0
Notes:

Document Analysis

ExifTool

Website: <https://exiftool.org>
Description: Tool for analysing EXIF data from files
Author: Phil Harvey
License: <https://exiftool.org/#license>
Version: 12.57
Notes:

msoffcrypto-crack.py

Website: <https://github.com/didierstevens/didierstevenssuite>
Description: MS Office Document Password Cracking utility
Author: Didier Stevens

License: Public Domain

Version: 0.0.5

Notes:

msoffcrypto-tool

Website: <https://github.com/nolze/msoffcrypto-tool>

Description: Python library for decrypting encrypted MS Office Files

Author: Nolze

License: MIT License (<https://github.com/nolze/msoffcrypto-tool/blob/master/LICENSE.txt>)

Version: 5.0.0

Notes:

OfficeMalScanner

Website: <http://www.reconstracter.org/main.html>

Description: Office Document analysis tool to detect implants and malware

Author: Frank Boldewin

License: Unknown

Version: 0.62

Notes:

OffVis

Website: <http://go.microsoft.com/fwlink/?LinkId=158791>

Description: Office document visualization tool

Author: Microsoft

License: EULA

Version: 1.1.0.0

Notes:

oledump.py

Website: <https://github.com/didierstevens/didierstevenssuite>

Description: Analyze OLE files

Author: Didier Stevens

License: Public Domain

Version: 0.0.71

Notes:

olefile

Website: <https://www.decalage.info/python/olefileio>

Description: Python module to read / write MS OLE2 files

Author: Philippe Lagadec

License: <https://github.com/decalage2/olefile/blob/master/LICENSE.txt>

Version: 0.46

Notes:

oletools

Website: <http://www.decalage.info/python/oletools>

Description: Package of tools to analyze MS OLE2 files

Author: Philippe Lagadec

License: <https://github.com/decalage2/oletools/blob/master/LICENSE.md>

Version: 0.60.1

Notes:

pdfid

Website: <https://github.com/didierstevens/didierstevenssuite>
Description: PDF Analysis Tool
Author: Didier Stevens
License: Public Domain
Version: 0.2.8
Notes:

pdf-parser

Website: <https://github.com/didierstevens/didierstevenssuite>
Description: PDF document parser
Author: Didier Stevens
License: Public Domain
Version: 0.7.7
Notes:

PDF Stream Dumper

Website: <https://github.com/dzzie/pdfstreamdumper>
Description: PDF Analysis Tool
Author: David Zimmer
License: None
Version: 0.9.624
Notes:

rtfdump.py

Website: <https://github.com/didierstevens/didierstevenssuite>
Description: Analyze RTF files
Author: Didier Stevens
License: Public Domain
Version: 0.0.12
Notes:

VSCode (Visual Studio Code)

Website: <https://code.visualstudio.com/>
Description: Open Source Code Editor and Debugger
Author: Microsoft
License: Code - MIT License (<https://github.com/microsoft/vscode/blob/main/LICENSE.txt>) / Product (<https://code.visualstudio.com/>)
Version: 1.73.1
Notes:

XLMMacroDeobfuscator

Website: <https://github.com/DissectMalware/XLMMacroDeobfuscator>
Description: Decode obfuscated XLM macros (aka Excel v4.0 macros)
Author: Malwrologist / DissectMalware
License: Apache License v2.0 (<https://github.com/DissectMalware/XLMMacroDeobfuscator/blob/master/LICENSE>)
Version: 0.2.7
Notes:

Document Viewers

LibreOffice

Website: <https://www.libreoffice.org>
Description: Document Processing Software

Author: LibreOffice - The Document Foundation
License: <https://www.libreoffice.org/about-us/licenses>
Version: 7.4.3
Notes:

Notepad++

Website: <https://notepad-plus-plus.org>
Description: Source Code and Text Editor
Author: Don Ho
License: GNU General Public License v2 (<https://notepad-plus-plus.org/>)
Version: 8.4.8
Notes:

Sublime Text

Website: <https://www.sublimetext.com>
Description: Text Editor for markup and code
Author: Sublime HQ Pty Ltd
License: EULA (<https://www.sublimehq.com/eula>)
Version: 4143
Notes:

Email

Forensic Email Collector

Website: <https://metaspike.com>
Description: Local and Remote email acquisition tool
Author: Arman Gungor - Metaspike
License:
Version: 3.86.0.21
Notes:

Kernel EDB Viewer

Website: <https://www.nucleustechnologies.com>
Description: Free Exchange EDB viewer
Author: Nucleus Technologies
License: EULA (<https://www.nucleustechnologies.com/eula.pdf>)
Version: 15.9
Notes:

Kernel OST Viewer

Website: <https://www.nucleustechnologies.com>
Description: Free Outlook OST viewer
Author: Nucleus Technologies
License: EULA (<https://www.nucleustechnologies.com/eula.pdf>)
Version: 21.1
Notes:

Kernel PST Viewer

Website: <https://www.nucleustechnologies.com>
Description: Free Outlook PST viewer
Author: Nucleus Technologies
License: EULA (<https://www.nucleustechnologies.com/eula.pdf>)
Version: 20.3
Notes:

SysTools Outlook PST Viewer

Website: <https://www.systoolsgroup.com>

Description: Outlook PST file parser

Author: SysTools

License: <https://www.systoolsgroup.com/eula.pdf>

Version: 5.0

Notes:

Executables

API Monitor v2 Alpha

Website: <http://www.rohitab.com/apimonitor>

Description: Tool to monitor API calls by applications

Author: Rohitab Batra

License:

Version: v2r13

Notes:

Bintext

Website: <https://mcafee.com>

Description: Finds Ascii, Unicode, and Resource strings in a file

Author: McAfee

License: Free

Version: 3.03

Notes:

File Insight

Website: <https://www.trellix.com>

Description: Static file analysis tool

Author: McAfee / Trellix

License: Software Royalty-Free License (<https://www.trellix.com/en-us/downloads/free-tools/terms-of-use.html>)

Version: 3.0

Notes:

MagnetProcessCapture

Website: <https://magnetforensics.com>

Description: Tool to dump a running process

Author: Magnet Forensics

License: EULA

Version: v13

Notes:

Process Hacker

Website: <https://processhacker.sourceforge.io>

Description: Process Monitoring Tool

Author: Steven G (dmex) / Wen Jia Liu / WinSiderss

License: GNU General Public License v3 - <https://processhacker.sourceforge.io/gpl.php>

Version: 2.39.0.124

Notes:

PSDecode

Website: <https://github.com/CyberCentreCanada/assemblyline-service-overpower>

Description: Powershell script to deobfuscate encoded Powershell scripts

Author: R3MRUM / CyberCentreCanada

License:

Version: 5.0

Notes:

Log Parsers

EventFinder

Website: <https://github.com/BeanBagKing/EventFinder2>

Description: Event Log Parser

Author: BeanBagKing

License: GNU General Public License v3 (<https://github.com/BeanBagKing/EventFinder2/blob/master/LICENSE>)

Version: 2.2.1

Notes:

evtx_dump

Website: <https://github.com/omerbenamram/evtx>

Description: EVTX Event Log Parser

Author: Omer BenAmram

License: Apache License v2 (<https://github.com/omerbenamram/evtx/blob/master/LICENSE-APACHE>) and MIT License (<https://github.com/omerbenamram/evtx/blob/master/LICENSE-MIT>)

Version: 0.8.0

Notes:

HTTP Log Browser

Website: <https://www.finalanalytics.com/products/httplogbrowser>

Description: Web server log analyzer

Author: FinalAnalytics

License: EULA - <https://www.finalanalytics.com/downloads/HttpLogBrowser-EULA.pdf>

Version: 4.6.2.0

Notes:

Log Parser

Website: <https://www.microsoft.com>

Description: Event Log Parser

Author: Microsoft

License:

Version: 2.2.10

Notes:

LogParser Studio

Website: https://techcommunity.microsoft.com/gxcuf89792/attachments/gxcuf89792/Exchange/16744/1/LPSV2.D2.zip?WT.mc_id=M365-MVP-5002016

Description: Graphical interface for Microsoft's log parser

Author: Microsoft

License:

Version: 2.0.0.100

Notes:

LogViewer2

Website: <https://github.com/woanware/LogViewer2>

Description: View large text / log files

Author: Mark Woan

License:
Version: 1.0.0
Notes:

Mobile Analysis

ALEAPP

Website: <https://github.com/abrignoni/aleapp>
Description: Android Logs Events and Protobuf Parser
Author: Alexis Brignoni
License: MIT License (<https://github.com/abrignoni/ALEAPP/blob/master/LICENSE>)
Version: 3.1.1
Notes:

Bytecode Viewer

Website: <https://github.com/konloch/bytecode-viewer>
Description: Android APK reverse engineering suite
Author: Konloch
License: GNU General Public License v3 (<https://github.com/Konloch/bytecode-viewer/blob/master/LICENSE>)
Version: 2.11.2
Notes:

ILEAPP

Website: <https://github.com/abrignoni/ileapp>
Description: iOS Logs Events and Plists Parser
Author: Alexis Brignoni
License: MIT License (<https://github.com/abrignoni/iLEAPP/blob/master/LICENSE>)
Version: 1.18.1
Notes:

iphoneanalyzer (iPhone Analyzer)

Website: <https://sourceforge.net/project/iphoneanalyzer/>
Description: Analyze iPhone backups
Author: leocrawford, matproud
License: GNU General Public License v3 (<https://sourceforge.net/directory/os:linux/license:gplv3/>)
Version: 2.1.0
Notes:

VLEAPP

Website: <https://github.com/abrignoni/vleapp>
Description: Vehicle Logs Events and Properties Parser
Author: Alexis Brignoni
License: MIT License (<https://github.com/abrignoni/VLEAPP/blob/main/LICENSE>)
Version: 1.0.0
Notes:

Network

Burp Suite Community Edition

Website: <https://portswigger.net>
Description: Packet Intercept and Analysis Tool
Author: PortSwigger
License: <https://portswigger.net/burp/tc-community>

Version: v2022.11.2

Notes:

Fiddler

Website: <https://www.telerik.com/fiddler>

Description: Web Proxy

Author: Telerik

License:

Version: 5.0.20211.51073

Notes:

PuTTY

Website: <https://www.chiark.greenend.org.uk/~sgtatham/putty/>

Description: Free SSH and Telnet Client

Author: Simon Tatham

License: <https://tartarus.org/~simon/putty-snapshots/htmldoc/AppendixD.html#licence>

Version: 0.78

Notes:

WebPageSaver

Website: <https://magnetforensics.com>

Description: Creates an HTML report containing a snapshot of each webpage at a specific point in time

Author: Magnet Forensics

License: EULA

Version: 3.4.0

Notes:

Wireshark

Website: <https://www.wireshark.org>

Description: Network packet capture and analysis tool

Author: The Wireshark Foundation (<https://gitlab.com/wireshark/wireshark/-/blob/master/AUTHORS>)

License: GNU General Public License v2 (<https://gitlab.com/wireshark/wireshark/-/blob/master/COPYING>)

Version: 4.0.1

Notes:

Raw Parsers / Decoders

Bulk Extractor

Website: https://digitalcorpora.org/downloads/bulk_extractor & https://github.com/simsong/bulk_extractor

Description: Tool for extracting artifacts from random data

Author: Simson L. Garfinkel

License: MIT License (https://github.com/simsong/bulk_extractor/blob/main/LICENSE.md)

Version: 1.5.5

Notes:

Cyberchef

Website: <https://github.com/gchq/cyberchef>

Description: Web app for encryption, encoding, compression and data analysis

Author: GCHQ

License: Apache License v2.0 (<https://github.com/gchq/CyberChef/blob/master/LICENSE>)

Version: 9.54.0

Notes:

Data Dump

Website: <https://www.digital-detective.net/datadump/>
Description: Tool to extract segments of data from an image or device
Author: Craig Wilson (<https://www.digital-detective.net>)
License:
Version: 2.1.23012.16
Notes: x86

DCode

Website: <https://www.digital-detective.net/dcode>
Description: Timestamp encoder/decoder
Author: Craig Wilson (<https://www.digital-detective.net>)
License:
Version: 5.5.21194.40
Notes:

Hex Editor Neo (Free)

Website: <https://www.hhdsoftware.com>
Description: Hex Editor
Author: HHD Software
License: EULA (<https://www.hhdsoftware.com/company/terms-of-use>)
Version: 7.09.01.8132
Notes:

HxD

Website: <https://mh-nexus.de>
Description: Hex Editor
Author: Mael Horz
License: <https://mh-nexus.de/en/about.php>
Version: 2.5.0.0
Notes:

iptools

Website: https://github.com/digitalsleuth/forensics_tools
Description: IP / Hex / Dec Conversion tool
Author: Corey Forman
License: GNU General Public License v3.0 (https://github.com/digitalsleuth/forensics_tools/blob/master/LICENSE)
Version: 1.1
Notes:

Passware Encryption Analyzer

Website: <https://www.passware.com>
Description: Encryption Analysis tool
Author: Passware - Dmitry Sumin
License: EULA - <https://www.passware.com/files/Passware-EULA.pdf>
Version: 2023.1.1.3432
Notes:

Redline

Website: <https://www.fireeye.com>
Description: Memory and File analysis tool
Author: FireEye
License: Software Royalty-Free License (<https://www.trellix.com/en-us/downloads/free-tools/terms-of-use.html>)

Version: 2.0

Notes:

time-decode

Website: https://github.com/digitalsleuth/time_decode

Description: Python timestamp encode / decode utility

Author: Corey Forman

License: MIT License (https://github.com/digitalsleuth/time_decode/blob/master/LICENSE)

Version: 4.2

Notes:

yara-python

Website: <https://github.com/VirusTotal/yara-python>

Description: Analyze files by generating rules around data to be found

Author: Victor M. Alvarez (plusvic)

License: Apache License v2.0 (<https://github.com/VirusTotal/yara-python/blob/master/LICENSE>)

Version: 4.2.3

Notes:

Terminals

MobaXterm

Website: <https://mobaxterm.mobatek.net>

Description: Enhanced Terminal for Windows

Author: Mobatek (<https://www.mobatek.net/aboutus.html>)

License: <https://mobaxterm.mobatek.net/license.html>

Version: 23.0

Notes: Home Edition

WSL Setup

Website: <https://microsoft.com>

Description: Windows Subsystem for Linux setup

Author: Microsoft

License: EULA

Version: 0.0

Notes:

Utilities

Encrypted Disk Detector (EDD)

Website: <https://www.magnetforensics.com>

Description: Detects encrypted disks

Author: Magnet Forensics

License: EULA

Version: 310

Notes: Standalone Utility

FastCopy

Website: <https://fastcopy.jp>

Description: Fast file copy software which can retain file details

Author: FastCopy Lab - <https://fastcopy.jp/company.html>

License: Copyright - All rights reserved - https://fastcopy.jp/help/fastcopy_eng.htm#license

Version: 4.2.1

Notes:

HashCheck

Website: <https://github.com/gurnec/HashCheck>

Description: Context-Menu / Shell Extension hash generator utility

Author: Christopher Gurnee / Kai Liu / David B. Trout / Tim Schlueter

License: <https://github.com/gurnec/HashCheck/blob/master/license.txt>

Version: 2.4.0.55

Notes:

IrfanView x64

Website: <https://www.irfanview.com/64bit.htm>

Description: IrfanView image viewer and editor

Author: Irfan Skiljan

License: <https://www.irfanview.com/eula.htm>

Version: 4.62

Notes:

IrfanView x64 Plugins

Website: <https://www.irfanview.com/64bit.htm>

Description: IrfanView Plugins

Author: Irfan Skiljan

License: <https://www.irfanview.com/eula.htm>

Version: 4.62

Notes:

megatools

Website: <https://megatools.megous.com>

Description: Mega.NZ downloader suite

Author: https://megatools.megous.com/man/megatools.html#_author

License: GNU General Public License v2 (<https://megous.com/git/megatools/tree/LICENSE>)

Version: 1.11.1

Notes:

Monolith Notes

Website: <https://www.monolithforensics.com/>

Description: Forensic note taking and tracking tool

Author: Monolith Forensics

License: EULA

Version: 1.0.1

Notes:

Nuix Evidence Mover

Website: <https://www.nuix.com/nuix-evidence-mover>

Description: File Transfer tool with source and destination hashing

Author: NUIX

License: <https://www.oracle.com/legal/terms.html>

Version: 6.2.1

Notes:

OpenHashTab

Website: <https://github.com/namazso/OpenHashTab>

Description: Shell Extension for File Hashing

Author: Namazso

License: GNU General Public License 3.0 (<https://github.com/namazso/OpenHashTab/blob/master/COPYING>)

Version: 3.0.2

Notes:

Rufus

Website: <https://rufus.ie>

Description: USB ISO Creator

Author: Pete Batard

License: GNU General Public License v3 - <https://github.com/pbatard/rufus/blob/master/LICENSE.txt>

Version: 3.21

Notes:

Tableau Firmware Update

Website: <https://www.opentext.com>

Description: Firmware update utility for Tableau forensic devices

Author: OpenText

License: EULA

Version: 22.3.2

Notes:

USB Registry Write Blocker

Website: <https://github.com/digitalsleuth/registry-write-block>

Description: USB Write Blocker for standard USB / UASP devices using Registry Modifications

Author: Corey Forman

License: MIT License (<https://github.com/digitalsleuth/Registry-Write-Block/blob/master/LICENSE>)

Version: 1.2

Notes:

VcXsrv Windows X Server

Website: <https://sourceforge.net/projects/vcxsrv/>

Description: Windows X-Server for interacting with X-Windows environments

Author: Marha

License: GNU General Public License v3

Version: 1.20.14.0

Notes:

WindowGrid

Website: <http://windowgrid.net>

Description: Tool to easily align windows and icons to a grid on the Windows Desktop

Author: Joshua Wilding

License: Unknown

Version: 1.3.1.1

Notes:

Windows Analysis

AccessData Registry Viewer

Website: <https://www.exterro.com>

Description: Registry Analysis Tool

Author: AccessData / Exterro

License: EULA

Version: 2.0.0.7

Notes:

amcache.py

Website: Original (<https://github.com/williballenthin/python-registry>)

Description: AmCache Registry Hive Parser

Author: Willi Ballenthin and Corey Forman

License: Apache License 2.0 (<https://github.com/williballenthin/python-registry/blob/master/LICENSE.TXT>)

Version: 2.0

Notes: This version has been modified from the original, and is not stored online at this time

Autorunner

Website: <https://github.com/woanware/autorunner>

Description: Checks for autorun applications on Windows

Author: Mark Woan

License: Public Domain

Version: 0.0.16

Notes:

autotimeliner

Website: <https://github.com/andreafortuna/autotimeliner>

Description: Timeline generator using Sleuthkit and Volatility

Author: Andrea Fortuna

License: MIT License (<https://github.com/andreafortuna/autotimeliner/blob/master/LICENSE>)

Version: 1.1.0

Notes:

bitsparser

Website: <https://github.com/digitalsleuth/bitsparser>

Description: A python tool to parse Windows BITS database files

Author: Corey Forman / FireEye

License: Apache License v2.0 (<https://github.com/digitalsleuth/BitsParser/blob/master/LICENSE>)

Version: 1.0

Notes:

Hindsight

Website: <https://github.com/obsidianforensics/hindsight>

Description: Web-based Chromium Browser artifact parser (Chrome origins)

Author: Obsidian Forensics

License: Apache v2.0 (<https://github.com/obsidianforensics/hindsight/blob/master/LICENSE.md>)

Notes:

Version: v2021.12

Kansa

Website: <https://github.com/davehull/kansa>

Description: Powershell Incident Response Framework

Author: Dave Hull

License: Apache License v2.0 (<https://github.com/davehull/Kansa/blob/master/LICENSE>)

Version: 18NOV2022 (No defined version)

Notes:

kape

Website: <https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape>

Description: Incident Response Artifact Parser and Extractor

Author: Eric Zimmerman / Kroll

License: <https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape>

Version: 1.3.0.2

Notes:

LogFileParser

Website: <https://github.com/jschicht/LogFileParser>

Description: NTFS \$LogFile Parser

Author: Joakim Schicht

License: MIT (<https://github.com/jschicht/LogFileParser/blob/master/LICENSE.md>)

Version: 2.0.0.49

Notes:

MagnetRamCapture (MRC)

Website: <https://magnetforensics.com>

Description: Windows memory capture utility

Author: Magnet Forensics

License: EULA

Version: 1.2.0

Notes:

MFT Browser

Website: https://github.com/kacos2000/MFT_Browser

Description: Graphical MFT Browser utility

Author: Costas K.

License: MIT License (https://github.com/kacos2000/MFT_Browser/blob/master/LICENSE)

Version: 0.0.68.0

Notes:

Mimikatz

Website: <https://github.com/gentilkiwi/mimikatz>

Description: Windows-based hash extraction tool

Author: Benjamin Delpy

License: Creative Commons BY 4.0

Version: 2.2.0-20220919

Notes: Detects as a virus in Windows - Exclusion gets added during install

MiTeC Tool Suite

Website: <https://mitec.cz>

Description: Suite of Windows-based analysis tools

Author: Michal Mutl (mitec)

License: Free to use for private, educational and non-commercial purposes

Version: Various

Notes:

Nirsoft

Website: <https://nirsoft.net>

Description: Suite of various Windows Analysis Tools

Author: Nir Sofer

License:

Version: 1.23.70

Notes:

NTFS Log Tracker

Website: <https://sites.google.com/site/forensicnote/ntfs-log-tracker>

Description: NTFS \$LogFile, *UsnJrnl* :J parser

Author: Junghoon Oh (blueangel)

License:

Version: 1.71

Notes:

Pilfer

Website: https://github.com/digitalsleuth/forensics_tools

Description: Rapid triage tool using Windows in-built binaries

Author: Corey Forman (digitalsleuth)

License: GNU General Public License v3 (https://github.com/digitalsleuth/forensics_tools/blob/master/LICENSE)

Version: 2.4

Notes:

regripper

Website: <https://github.com/keydet89/RegRipper3.0>

Description: Registry parsing toolsuite

Author: Harlan Carvey

License: MIT License (<https://github.com/keydet89/RegRipper3.0/blob/master/license.md>)

Version: 3.0

Notes: rr.exe

Shadow Explorer

Website: <https://www.shadowexplorer.com>

Description: Windows Volume Shadow Copy viewer

Author: ShadowExplorer

License:

Version: 0.9.462.0

Notes:

SilkETW

Website: <https://github.com/mandiant/SilkETW>

Description: Wrapper for ETW (Event Tracing for Windows)

Author: Mandiant

License: Apache License v2 (<https://github.com/mandiant/SilkETW/raw/master/LICENSE.txt>) 3rd-party license (<https://github.com/mandiant/SilkETW/blob/master/THIRD-PARTY-LICENSE.txt>)

Version: 0.8

Notes: Sample Usage - <https://www.mandiant.com/resources/blog/silketw-because-free-telemetry-is-free>

srum-dump

Website: <https://github.com/MarkBaggett/srum-dump>

Description: Tool to analyze data in the Windows System Resource Usage Monitor database

Author: Mark Baggett

License: GNU General Public License v3 (<https://github.com/MarkBaggett/srum-dump/blob/master/LICENSE>)

Version: 2.4

Notes:

Sysinternals

Website: <https://sysinternals.com>

Description: Suite of Windows Analysis and Management Tools

Author: Microsoft / Mark Russinovich

License: <https://learn.microsoft.com/en-us/sysinternals/license-terms>

Version: 2023.01.25 (date of last update - no specific version number identified)

Notes:

The Sleuth Kit

Website: <https://github.com/sleuthkit/sleuthkit/>

Description: Library and collection of command line DFIR tools

Author: Brian Carrier

License: Multiple Licenses (<https://www.sleuthkit.org/sleuthkit/licenses.php>)

Version: 4.12.0

Notes:

usbdeviceforensics

Website: <https://github.com/digitalsleuth/usbdeviceforensics>

Description: Track a USB device throughout a Windows system

Author: Corey Forman / Mark Woan

License: Public Domain

Version: 1.0.0

Notes:

USN Journal Parser

Website: <https://github.com/digitalsleuth/USN-Journal-Parser>

Description: Updated version of PoorBillionaire's USN-Journal-Parser

Author: Corey Forman / Adam Witt

License: MIT License (<https://github.com/digitalsleuth/USN-Journal-Parser/blob/main/LICENSE>)

Version: 5.0.0

Notes: Commands: usn, usn.py

Velociraptor

Website: <https://docs.velociraptor.app/>

Description: DFIR live acquisition tool

Author: Mike Cohen (scudette)

License: GNU Affero General Public License v3 (<https://github.com/Velocidex/velociraptor/blob/master/LICENSE>)

Version: 0.6.7-5

Notes:

Volatility

Website: <https://github.com/volatilityfoundation/volatility>

Description: Memory analysis toolset

Author: <https://github.com/volatilityfoundation/volatility/blob/master/AUTHORS.txt>

License: GNU General Public License v2 (<https://github.com/volatilityfoundation/volatility/blob/master/LICENSE.txt>)

Version: 2

Notes:

Volatility3

Website: <https://github.com/volatilityfoundation/volatility3>

Description: Memory analysis toolset

Author: Volatility Foundation

License: Volatility Software License (<https://www.volatilityfoundation.org/license/vsl-v1.0>)

Version: 3

Notes:

vssmount

Website: https://github.com/digitalsleuth/forensics_tools

Description: Windows Batch script to work with and mount Volume Shadow Copies

Author: Corey Forman (digitalsleuth)

License: GNU General Public License v3 (https://github.com/digitalsleuth/forensics_tools/blob/master/LICENSE)

Version: 2.0

Notes:

winpmem

Website: <https://github.com/velocidex/WinPmem>

Description: Memory Acquisition Tool

Author: Mike Cohen (scudette)

License: Apache License v2 (<https://github.com/Velocidex/WinPmem/blob/master/LICENSE>)

Version: 4.0.rc2

Notes:

WLEAPP

Website: <https://github.com/abrignoni/wleapp>

Description: Windows Logs Events and Properties Parser

Author: Alexis Brignoni

License: MIT License (<https://github.com/abrignoni/WLEAPP/blob/main/LICENSE>)

Version: 0.1

Notes:

WMI Parser

Website: <https://github.com/woanware/wmi-parser>

Description: Parse the WMI object database for persistence

Author: Mark Woan

License: Unknown

Version: 0.0.2

Notes:

Zimmerman Tools

Website: <https://ericzimmerman.github.io>

Description: Suite of Forensic Tools

Author: Eric Zimmerman

License: MIT License (<https://github.com/EricZimmerman/Issues/blob/master/LICENSE>)

Version: 2021-01-22

Notes:

Requirements

7-Zip

Website: <https://7-zip.org>

Description: Zip Compiler and Extractor

Author: Igor Pavlov

License: GNU LGPL (<https://www.7-zip.org/faq.html>)

Version: 22.00

Notes:

Adobe Reader DC Classic

Website: <https://www.adobe.com>

Description: Adobe PDF Document Reader

Author: Adobe

License: <https://helpx.adobe.com/ca/reader/acrobat-copyright-trademarks-third-party-notice.html>

Version: 22.003.20282

Notes:

Distorm3

Website: <https://github.com/gdabah/distorm>

Description: Disassembler Library for x86/x64

Author: Gil Dabah

License: <https://github.com/gdabah/distorm/blob/master/COPYING>

Version: 3.3.4

Notes:

Git for Windows

Website: <https://github.com/git-for-windows/git>

Description: Version Control System for Windows

Author: Git (git-scm.com)

License: GNU Public License and Lesser GNU Public License (<https://github.com/git-for-windows/git/blob/main/COPYING>, <https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html>)

Version: 2.38.1

Notes:

Java Runtime Environment

Website: <https://www.java.com>

Description: Java Engine

Author: Oracle

License: <https://www.oracle.com/legal/terms.html>

Version: 8u311

Notes:

Microsoft VC++ 2015 Build Tools

Website: <https://microsoft.com>

Description: Microsoft Visual C++ 2015 Build Tools

Author: Microsoft

License:

Version: 15.9.51

Notes:

Microsoft VC++ 2022 Build Tools

Website: <https://microsoft.com>

Description: Microsoft Visual C++ 2022 Build Tools

Author: Microsoft

License:

Version: 17.4.33122.133

Notes:

Microsoft Visual C++ Compiler for Python 2.7

Website: <https://visualstudio.microsoft.com/visual-cpp-build-tools/>

Description: Compiler for Python 2.7 to compile scripts on Windows

Author: Microsoft

License: EULA

Version: 9.0.1.30729

Notes:

.NET 3.5 Framework

Website: <https://download.visualstudio.microsoft.com/download/pr/b635098a-2d1d-4142-bef6-d237545123cb/2651b87007440a15209cac29>

Description: Microsoft .NET 3.5 Framework with .NET 2.0

Author: Microsoft

License:

Version: .NET 3.5 SP1

Notes:

.NET 6 Desktop Runtime

Website: <https://microsoft.com>

Description: Windows Runtime component

Author: Microsoft

License: EULA

Version: 6.0.7.31422

Notes:

Portals

Website: <https://portals-app.com>

Description: Desktop Organizer

Author: Ross Patterson

License: Free To Use - Terms and Conditions (<https://rosspat.dev/privacy/>)

Version: 2.1.0.6

Notes:

Pycryptodome

Website: <https://github.com/legrandin/pycryptodome>

Description: Python package of low-level cryptographic primitives

Author: Helder Eijs (Legrandin)

License: Public Domain / BSD (<https://github.com/Legrandin/pycryptodome/blob/master/LICENSE.rst>)

Version: 3.16.0

Notes: Python 2 and 3

Python 2

Website: <https://python.org>

Description: Python Programming Language

Author: Python Software Foundation

License: <https://docs.python.org/2.7/license.html>

Version: 2.7.18

Notes:

Python 3

Website: <https://python.org>

Description: Python Programming Language

Author: Python Software Foundation

License: Python Software Foundation License Version 2.0 (<https://docs.python.org/3.10/license.html>)

Version: 3.10.1150.0

Notes:

python-dateutil

Website: <https://github.com/dateutil/dateutil>

Description: Python module to use standard datetime features

Author: <https://github.com/dateutil/dateutil/blob/master/AUTHORS.md>

License: Apache License v2.0 (<https://github.com/dateutil/dateutil/blob/master/LICENSE>)

Version: 2.8.2

Notes:

Strawberry Perl

Website: <https://strawberryperl.com>

Description: Perl programming language environment for Windows

Author: Strawberry Perl

License: GNU General Public License 1+ (license found within software)

Version: 5.32.1.1

Notes:

Visual Studio Community Edition 2022

Website: <https://visualstudio.microsoft.com>

Description: Windows IDE for developing in multiple Windows-based programming languages

Author: Microsoft

License: <https://aka.ms/VSLicensingPaper>

Version: 17.0.4 (2022)

Notes: Installation and application are 17.0.4, but environment is 2022

WSL 2 System Update

Website: https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi

Description: Update for Windows Subsystem for Linux to version 2

Author: Microsoft

License: EULA

Version: 5.10.16

Notes: