WIN-FOR Tool List

Corey Forman (digitalsleuth)

2023-03-18

Acquisition and Analysis

Tools used for the acquisition and bulk processing / analysis of evidence items

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: 3.9.239
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: 6.2.1
Notes:

Elcomsoft Forensic Disk Decryptor

Website: https://www.elcomsoft.com/
Description: Tool for decrypting disks or extracting encryption keys from memory
Author: Elcomsoft
License: EULA (https://www.elcomsoft.com/legal.html)
Version: 2.19.999.6400
Notes: Available, but not installed by default

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: Evidence Acquisition tool
Author: Jad Saliba - Magnet Forensics
License: EULA
Version: 2.61.0.33597
Notes:

Magnet AXIOM

Website: https://www.magnetforensics.com
Description: Evidence Acquisition and Analysis toolset
Author: Jad Saliba - Magnet Forensics
License: EULA
Version: 6.11.0.34807
Notes:

Magnet Chromebook Acquisition

Website: https://www.magnetforensics.com
Description: Evidence Acquisition for Chromebook
Author: Jad Saliba - Magnet Forensics
License: EULA
Version: 1.06
Notes:

Magnet RAM Capture (MRC)

Website: https://magnetforensics.com
Description: Windows memory capture utility
Author: Magnet Forensics
License: EULA
Version: 1.2.0
Notes:

Magnet RESPONSE

Website: https://magnetforensics.com
Description: Tool to collect data relevant to incident response investigations
Author: Magnet Forensics
License: EULA
Version: 1.5
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:

Tableau Imager

Website: https://opentext.com
Description: Disk / Device Imager
Author: OpenText
License: EULA
Version: 20.3.3
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:

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

Web browsers

Chrome

Website: https://www.google.com
Description: Google Web Browser
Author: Google
License: https://policies.google.com/terms
Version: 108.0.5359.72
Notes:

Firefox

Website: https://www.mozilla.org/en-US/firefox/new/
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:

Databases

Database browsers

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://github.com/dbeaver/dbeaver
Description: SQL Database tool and client
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:

RazorSQL

Website: https://razorsql.com
Description: SQL Database analysis tool
Author: Richardson Software LLC
License: https://razorsql.com/license.txt
Version: 10.1.1
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 analysis tool
Author: SysTools
License: EULA (https://www.systoolsgroup.com/eula.html)
Version: 11.0
Notes:

Documents / Editors

Applications to create, modify, disassemble, and analyze document files.

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:

ExifToolGui

Website: https://exiftool.org
Description: Graphical EXIF analysis tool
Author: Phil Harvey
License: https://exiftool.org/#license
Version: 5.16
Notes:

Libre Office

Website: https://www.libreoffice.org
Description: Open Source Office Document suite
Author: LibreOffice
License: Mozilla Public License (https://www.libreoffice.org/download/license/)
Version: 7.5.2
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:

Notepad++

Website: https://notepad-plus-plus.org
Description: Free source code / text editor
Author: Don Ho
License: GNU General Public License 2.0 (https://notepad-plus-plus.org/)
Version: 8.4.8
Notes:

OfficeMalScanner

Website: http://www.reconstructer.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:

pcodedmp

Website: https://github.com/bontchev/pcodedmp
Description: Python VBA p-code disassembler
Author: Vesselin Bontchev
License: GNU General Public License v3 (https://github.com/bontchev/pcodedmp/blob/master/LICENSE)
Version: 1.2.6
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/didierstevensssuite
Description: PDF document parser
Author: Didier Stevens
License: Public Domain
Version: 0.7.8
Notes:

PDFStream Dumper

Website: https://github.com/dzzie/pdfstreamdumper
Description: PDF Analysis tool
Author: David Zimmer (dzzie)
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:

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:

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/License/)
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:

Email

Analyze email artifacts

4n6 Email Forensics

Website: https://forensiksoft.com
Description: Email forensics utility
Author: 4n6 Software
License: https://forensiksoft.com/terms/
Version: 7.5
Notes:

BitRecover EML File Viewer

Website: https://www.bitrecover.com
Description: EML file viewer
Author: BitRecover
License: EULA - https://www.bitrecover.com/terms.html
Version: 5.0
Notes:

Email Header Analyzer

Website: https://github.com/cyberdefenders/email-header-analyzer
Description: Python-based Email Header Analysis Tool
Author: Ahmed Shawky (lnxg33k)
License: GNU General Public License v3.0 (https://github.com/cyberdefenders/email-header-analyzer/blob/master/LICENSE.md)
Version: v1
Notes:

Forensic Email Collector (FEC)

Website: https://metaspike.com
Description: Local and Remote email acquisition tool
Author: Arman Gungor - Metaspike
License:
Version: 3.86.0.21
Notes: Available, but not installed by default

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:

PST Walker

Website: https://www.pstwalker.com/
Description: Forensic GUI Tool for PST, OST
Author: PST Walker
License: GNU General Public License (GPL) (https://www.pstwalker.com/licensing-policy.html)

Version: 7.06
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

Reverse engineering, static, and dynamic analysis of 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:

capa

Website: https://github.com/mandiant/capa
Description: FLARE tool to identify capabilities in executables
Author: Mandiant
License: Apache License 2.0 (https://github.com/mandiant/capa/blob/master/LICENSE.txt)
Version: 4.0.1
Notes:

Cutter

Website: https://github.com/rizinorg/cutter
Description: Reverse Engineering Platform powered by rizin
Author: Rizin Organization
License: GNU General Public License v3 (https://github.com/rizinorg/cutter/blob/dev/COPYING)
Version: 2.1.2
Notes:

Decompyle3

Website: https://github.com/rocky/python-decompile3/
Description: Python3 bytecode decompiler
Author: Rocky R. Bernstein
License: GNU General Public License v3 (https://github.com/rocky/python-decompile3/blob/master/COPYING)

Version: 3.9.0
Notes:

densityscout

Website: https://cert.at
Description: Tool to identify entropy within files
Author: Christian Wojner / CERT.at (https://cert.at/en/about-us/overview/)
License: Internet Software Consortium License (ISCL - https://cert.at/en/downloads/software/software-densityscout)
Version: Build 45
Notes:

DIE (Detect It Easy)

Website: https://github.com/horsicq/DIE-engine
Description: Reverse Engineering Engine
Author: Hors (horsicq)
License: MIT License (https://github.com/horsicq/DIE-engine/blob/master/LICENSE)
Version: 3.06
Notes: Detect It Easy - DIE

dotPeek

Website: https://www.jetbrains.com
Description: .NET Decompiler and Assembly Browser
Author: JetBrains
License: EULA (https://www.jetbrains.com/legal/docs/toolbox/license_personal/)
Version: 2022.2.4
Notes:

exeinfope

Website: https://github.com/ExeinfoASL/ASL
Description: EXE, Packer, Compiler detection
Author: ExeinfoASL
License: None Listed
Version: 0.0.7.6
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:

FLOSS (FLARE Obfuscated String Solver)

Website: https://github.com/mandiant/flare-floss
Description: Extract obfuscated strings from malware
Author: Mandiant
License: Apache License v2.0 (https://github.com/mandiant/flare-floss/blob/master/LICENSE.txt)
Version: 2.1.0
Notes:

hollows_hunter

Website: https://github.com/hasherezade/hollows_hunter
Description: Scans running processes for implants and dumps them if found
Author: hasherezade
License: BSD 2-Clause Simplified License (https://github.com/hasherezade/hollows_hunter/blob/master/LICENSE)
Version: 0.3.5
Notes:

ilspy

Website: https://github.com/icsharpcode/ilspy
Description: .NET Decompiler
Author: ICSharpCode (https://github.com/orgs/icsharpcode/people)
License: MIT License (https://github.com/icsharpcode/ILSpy/blob/master/doc/ILSpyAboutPage.txt)
Version: 7.2.1.6856
Notes:

KsDumper 11

Website: https://github.com/mastercodeon314/KsDumper-11
Description: Kernel Space Dumper utility
Author: mastercodeon314
License: None at this time
Version: 1.0
Notes:

MagnetProcessCapture

Website: https://magnetforensics.com
Description: Tool to dump a running process
Author: Magnet Forensics
License: EULA
Version: v13
Notes:

MalCat

Website: https://malcat.fr
Description: Malware Analysis Tool
Author: Malcat EL
License: https://malcat.fr/index.html#faq6
Version: 0.9.0
Notes:

mal_unpack

Website: https://github.com/hasherezade/mal_unpack
Description: Dynamic unpacker based on PE-sieve
Author: hasherezade
License: BSD 2-Clause Simplified License (https://github.com/hasherezade/mal_unpack/blob/master/LICENSE)
Version: 0.9.6
Notes:

Noriben

Website: https://github.com/rurik/noriben
Description: Malware Analysis Sandbox based on Python
Author: Brian Baskin (Rurik)
License: Apache License v2 (https://github.com/Rurik/Noriben/blob/master/LICENSE)

Version: 1.8.7
Notes:

NTCore Explorer Suite

Website: https://ntcore.com
Description: PE Analysis tool suite
Author: Erik Pistelli
License:
Version: IV
Notes:

PE-bear

Website: https://github.com/hasherezade/pe-bear
Description: Portable Executable reversing tool with a GUI
Author: hasherezade
License: GNU General Public License v2 (https://github.com/hasherezade/pe-bear/blob/main/LICENSE)
Version: 0.6.1
Notes:

PEiD

Website: https://github.com/wolfram77web/app-peid
Description: Portable Executable identifier
Author: snaker / Qwerton / Jibz
License: All Rights Reserved
Version: 0.95
Notes:

pe-sieve

Website: https://github.com/hasherezade/pe-sieve
Description: Scans a process and dumps possible implants
Author: hasherezade
License: BSD 2-Clause Simplified License (https://github.com/hasherezade/pe-sieve/blob/master/LICENSE)
Version: 0.3.5
Notes:

PEStudio

Website: https://www.winitor.com
Description: PE Analysis Tool
Author: Marc Ochsenmeier
License: As-Is, without warranty (https://www.winitor.com/tools/pestudio/changes.log)
Version: 9.48
Notes:

pev

Website: https://github.com/merces/pev
Description: PE Analysis toolkit
Author: Fernando Merces
License: GNU General Public License v2.0 (https://github.com/merces/pev/blob/master/LICENSE)
Version: 0.81
Notes:

PPEE (puppy)

Website: https://www.mzrst.com/
Description: Professional PE file Explorer
Author: Zaderostam
License:
Version: 1.12
Notes:

ProcDOT

Website: https://www.procdot.com
Description: Visual analysis of Windows-based malware
Author: Christian Wojner
License: Internet Systems Consortium (ISC - https://www.procdot.com/faqs.htm, https://www.procdot.com/webhelp/index.html?license.htm)
Version: 1.22 (build 57)
Notes: Requires Windows Graphviz and Windump/TCPDump, but Windump/TCPDump are not supported on Win10+

Process Hacker

Website: https://processhacker.sourceforge.io
Description: Process analysis and dumping 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:

Resource Hacker

Website: http://www.angusj.com/resourcehacker
Description: Compiler and Decompiler for Windows applications
Author: Angus Johnson
License: Freeware (http://www.angusj.com/resourcehacker - License to Use)
Version: 5.1.7
Notes:

scdbg

Website: http://sandsprite.com/blogs/index.php?uid=7&pid=152
Description: Shellcode analysis tool
Author: https://github.com/dzzie/VS_LIBEMU/blob/master/AUTHORS
License:
Version: 2022.11.1
Notes:

Scylla

Website: https://github.com/ntquery/scylla
Description: Imports Reconstructor written in C/C++
Author: NtQuery
License: GNU General Public License v3 (https://github.com/NtQuery/Scylla/blob/master/LICENSE)

Version: 0.9.8
Notes: May not work well on later versions of Windows 10 and any version of Windows 11

setdllcharacteristics

Website: https://blog.didierstevens.com/2010/10/17/setdllcharacteristics/
Description: Manually edit the characteristics of DLL’s
Author: Didier Stevens
License: Public Domain
Version: 0.0.0.1
Notes:

UPX

Website: https://github.com/upx/upx
Description: The Ultimate Packer for eXecutables
Author: Markus Oberhumer, Laszlo Molnar, John Reiser
License: Multiple Licenses (https://github.com/upx/upx/blob/devel/LICENSE)
Version: 4.0.1
Notes:

VB-Decompiler

Website: https://www.vb-decompiler.org
Description: Visual Basic Decompiler
Author: DotFix Software
License: https://www.vb-decompiler.org/license.htm
Version: 12.0
Notes:

WinDbg

Website: https://www.microsoft.com
Description: Windows Debugger
Author: Microsoft
License: Third-party notices within app
Version: 1.2210.3001.0
Notes: Installed via winget

Windows Sandbox

Website: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview
Description: Windows-based Sandbox Environment
Author: Microsoft
License:
Version: 10.0.19041.985
Notes:

x64dbg

Website: https://sourceforge.net/projects/x64dbg/
Description: Open Source x64/x32 debugger for Windows
Author: Duncan Ogilvie (mrexodia)
License: GNU General Public License v3 (https://github.com/x64dbg/x64dbg/blob/development/LICENSE)
Version: 2023-03-04_02-26
Notes:

Installers

Decompile and deconstruct installers

AutoIt Extractor

Website: https://github.com/digitalsleuth/autoit-extractor
Description: AutoIt installer extractor
Author: x0r19x91
License: GNU General Public License v3.0
Version: 1.0.0
Notes:

InnoExtract

Website: https://constexpr.org/innoextract
Description: A tool to unpack installers created by Inno Setup
Author: Daniel Scharrer
License: https://github.com/dscharrer/innoextract/blob/master/LICENSE
Version: 1.9
Notes:

Innounp

Website: https://innounp.sourceforge.net
Description: Unpacker of executables packed by InnoSetup
Author: Ariman_ua, quickener
License: GNU General Public License v3 (https://innounp.sourceforge.net/#Copyrights)
Version: 0.50
Notes:

lessmsi

Website: https://github.com/activescott/lessmsi
Description: View and Extract the contents of a Windows MSI file
Author: Scott Willeke (activescott)
License: MIT License (https://github.com/activescott/lessmsi/blob/master/LICENSE)
Version: 1.10.0
Notes:

Py2ExeDecompiler

Website: https://github.com/endgameinc/Py2ExeDecompiler
Description: Decompiles executables originally compiled by Py2Exe
Author: Amanda Rousseau
License: MIT License (https://github.com/endgameinc/Py2ExeDecompiler/blob/master/LICENSE.txt)
Version: 1.0
Notes:

PyInstaller Extractor

Website: https://github.com/extremecoders-re/pyinstxtractor
Description: Python script to extract contents of PyInstallers
Author: ExtremeCoders-RE
License: GNU General Public License v3.0 (https://github.com/extremecoders-re/pyinstxtractor/blob/master/LICENSE)
Version: 2023.02
Notes:

UnAutoIt

Website: https://github.com/digitalsleuth/UnAutoIt
Description: AutoIt extractor
Author: Corey Forman (digitalsleuth) / x0r19x91
License: GNU General Public License v3 (https://github.com/digitalsleuth/UnAutoIt/blob/main/LICENSE)
Version: 1.1.1
Notes:

UniExtract2

Website: https://github.com/Bioruebe/UniExtract2
Description: Tool to extract files from installers
Author: William Engelmann
License: GNU General Public License v2 (https://github.com/Bioruebe/UniExtract2/blob/master/LICENSE)
Version: 2.0.0-rc3
Notes:

Logs

Event and Web log analysis

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:

Hayabusa

Website: https://github.com/Yamato-Security/hayabusa
Description: Windows event log fast forensics timeline generator and threat hunting tool
Author: Yamato Security
License: GNU General Public License v3.0 (https://github.com/Yamato-Security/hayabusa/blob/main/LICENSE.txt)
Version: 2.3.1
Notes:

HttpLogBrowser

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

Analysis of mobile devices and applications

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:

dex2jar

Website: https://github.com/pxb1988/dex2jar
Description: Android .dex and .class file analysis
Author: Bob Pan (pxb1988)
License: Apache License v2.0 (https://github.com/pxb1988/dex2jar/blob/2.x/LICENSE.txt)
Version: 2.1
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:

jd-gui

Website: https://github.com/java-decompiler/jd-gui
Description: GUI-based Java Decompiler
Author: Emmanuel Dupuy (emmanue1)
License: GNU General Public License v3 (https://github.com/java-decompiler/jd-gui/blob/master/LICENSE)
Version: 1.6.6
Notes:

Plist Editor

Website: https://www.icopybot.com
Description: Mac PList viewing tool
Author: VOW Software Studio
License: End User License Agreement
Version: 2.5.0
Notes: Free Trial

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

Network traffic analysis tools

Brim

Website: https://www.brimdata.io/
Description: Network Forensic GUI Tool using Zeek and Suricata
Author: Brim Data
License: GNU General Public License (GPL) (https://github.com/brimdata/brim/blob/main/LICENSE.txt)
Version: 0.31.0
Notes:

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:

Fakenet-NG

Website: https://github.com/mandiant/flare-fakenet-ng
Description: Next Generation Dynamic Network Analysis Tool
Author: https://github.com/mandiant/flare-fakenet-ng/blob/master/AUTHORS
License: Apache License 2.0 (https://github.com/mandiant/flare-fakenet-ng/blob/master/LICENSE.txt)
Version: 1.4.12
Notes:

NAFT - Network Appliance Forensic Toolkit

Website: https://github.com/digitalsleuth/naft
Description: Updated version of Didier Stevens Network Appliance memory dump analyzer
Author: Corey Forman / Gabriel Cossette / Didier Stevens
License: MIT License (https://github.com/digitalsleuth/naft/blob/main/LICENSE.md)
Version: 1.0.0b1
Notes:

Network Miner

Website: https://www.netresec.com/
Description: Network traffic analysis tool
Author: NETRESEC AB
License: GNU General Public License (GPL) v2.0 (https://www.netresec.com/?page=NetworkMinerSourceCode)
Version: 2.8
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:

Telerik Fiddler

Website: https://www.telerik.com
Description: Web debugging proxy tool
Author: Telerik
License:
Version: 5.0.20211.51073
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

Basic tools for byte-level analysis of data blobs

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: 9.55.0
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:

MemProcFS

Website: https://github.com/ufrisk/MemProcFS
Description: Memory Process File System
Author: Ulf Frisk
License: GNU Affero GPL v3.0 - https://github.com/ufrisk/MemProcFS/blob/master/LICENSE
Version: 5.4.2
Notes:

Passware Encryption Analyzer

Website: https://www.passware.com
Description: Encryption detection tool for various file types
Author: Passware - Dmitry Sumin
License: EULA (https://support.passware.com/hc/en-us/articles/221742768-What-are-the-terms-of-the-end-user-license-agreement-for-Passware-software-)
Version: 2023.1.1.3432
Notes:

photorec / testdisk

Website: https://www.cgsecurity.org/
Description: Raw data parsing tool
Author: Christophe Grenier
License: GNU General Public License v2.0 (https://git.cgsecurity.org/cgit/testdisk/tree/COPYING)
Version: 7.1
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:

smi-parser

Website: https://github.com/digitalsleuth/smi-parser
Description: Parses Caroolive SMI GPS files
Author: Corey Forman
License: GNU General Public License v3.0 (https://github.com/digitalsleuth/smi-parser/blob/main/LICENSE)
Version: 1.1.0
Notes: Available, but not installed by default

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:

Registry

Analysis of Windows registry artifacts

Registry Explorer

Website: https://ericzimmerman.github.io
Description: Registry analysis tool (part of EZ Tools / Zimmerman Tools)
Author: Eric Zimmerman
License: MIT License (https://github.com/EricZimmerman/Issues/blob/master/LICENSE)
Version: 2.0.0.0
Notes:

Registry Viewer

Website: https://exterro.com
Description: Windows Registry hive viewer
Author: AccessData / Exterro
License: EULA
Version: 2.0.0.7
Notes: Installable, but not currently installed - no longer supported

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

regshot

Website: https://sourceforge.net/projects/regshot/
Description: Registry snapshot utility to compare snapshots
Author: maddes, regshot, xhmikosr
License: GNU Lesser General Public License (https://sourceforge.net/p/regshot/code/HEAD/tree/branches/1.9.0/files/license_lgpl-2.1.txt)
Version: 1.9.0
Notes:

Terminals

Use of Linux-emulated terminals on Windows

Cygwin

Website: https://cygwin.com
Description: Linux Terminal Emulator for Windows
Author: https://cygwin.com/faq.html#faq.what.who
License: GNU General Public License (GPL) (https://cygwin.com/licensing.html)
Version: 3.4.6
Notes: Retcode is set to '2' for success because the Cygwin installer (even though on Windows) attempts to search for /etc/setup/setup.rc or /etc/setup/installed.db and fails with retcode 2. This causes Saltstack to read an ERROR and result: False, even though the pkg state returns 'install success'.

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

Windows Terminal

Website: https://github.com/microsoft/terminal
Description: Terminal Emulator
Author: Microsoft
License: MIT License (https://github.com/microsoft/terminal/blob/main/LICENSE)
Version: 1.16.(10261|10262).0
Notes: Version depends on Windows OS version

WSL Setup

Website: https://microsoft.com
Description: Windows Subsystem for Linux setup
Author: Microsoft
License: EULA
Version: 0.0
Notes:

Utilities

Basic utilities to assist in data analysis or transfer

Agent Ransack

Website: https://www.mythicsoft.com/agentransack/
Description: File Search utility
Author: Mythicsoft
License: End User License Agreement
Version: 9.0.3349.1
Notes:

Apple iTunes

Website: https://www.apple.com
Description: Media viewer and Apple device manager
Author: Apple
License: EULA
Version: 12.11.3.17
Notes: Available, but not installed by default

Aurora Incident Response

Website: https://github.com/cyb3rfox/Aurora-Incident-Response
Description: Incident Response Tracking tool
Author: Mathias Fuchs
License: Apache License 2.0 (https://github.com/cyb3rfox/Aurora-Incident-Response/blob/master/LICENSE)
Version: 0.6.6
Notes:

Bulk Rename Utility

Website: https://www.bulkrenameutility.co.uk
Description: Tool to rename multiple files with similar names
Author: TGRMN Software
License: EULA (https://www.bulkrenameutility.co.uk/License.php)
Version: 3.4.4
Notes: Available, but not installed by default

CAINE (Computer Aided INvestigative Environment)

Website: https://www.caine-live.net/
Description: USB bootable forensic environment
Author: Nanni Bassetti (https://www.caine-live.net/page4/page4.html)
License: GNU General Public License v2.1+ (https://www.caine-live.net/)
Version: 12.4
Notes: Available, but not downloaded by default

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:

Glossary Generator

Website: (nil - in house tool)
Description: Tool to generate a glossary for forensic reports
Author: Jad Saliba
License: None Provided
Version: 1.1
Notes: Available, but not installed by default

Google Earth Pro

Website: https://www.google.com/earth/about/versions/?gl=CA&hl=en#download-pro
Description: Tool for viewing Google Maps through installed application
Author: Google
License: Terms of Service (https://www.google.com/help/terms_maps/)
Version: 7.3.4.8642
Notes: Available, but not installed by default

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:

Hex2GUID

Website: (nil - in house)
Description: Batch script to convert hex/on-disk GUID to GUID format
Author: Mark Southby
License: Free To Use
Version: 2022050a
Notes: Available, but not installed by default

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:

Microsoft PowerToys

Website: https://github.com/microsoft/powertoys
Description: Windows productivity system utilities
Author: Microsoft
License: MIT (https://github.com/microsoft/PowerToys/blob/main/LICENSE)
Version: 0.64.1
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 (https://sourceforge.net/p/vcxsrv/code/ci/master/tree/COPYING)
Version: 1.20.14.0
Notes:

Veracrypt

Website: https://www.veracrypt.fr/code/VeraCrypt/
Description: Encrypted container creation and management
Author: https://github.com/veracrypt/VeraCrypt/blob/master/doc/html/Authors.html
License: Apache License v2 (https://github.com/veracrypt/VeraCrypt/blob/master/License.txt)
Version: 1.25.9
Notes: Available, but not installed by default

Virtualbox

Website: https://www.virtualbox.org/
Description: Desktop virtualization software
Author: Oracle
License: https://www.oracle.com/html/terms.html
Version: 7.0.4-154605
Notes: Available, but not installed by default

VLC Media Player

Website: https://www.videolan.org/
Description: Media Player
Author: VideoLAN
License: GNU General Public License v2 (https://www.videolan.org/legal.html)
Version: 3.0.18
Notes: Available, but not installed by default

Wiebetech Write Blocking Validation Utility

Website: https://wiebetech.com
Description: Write blocker capability testing
Author: Wiebetech
License: Free To Use
Version: 2.1.0.7
Notes: Available, but not installed by default

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 Winget

Website: https://github.com/microsoft/winget-cli
Description: Windows Package Manager
Author: Microsoft
License: MIT License (https://github.com/microsoft/winget-cli/blob/master/LICENSE)
Version: 1.4.10173
Notes:

WinMerge

Website: https://winmerge.org
Description: File Differencing Tool
Author: Dean P. Grimm (Thingamahoocie Software)
License: GNU General Public License v2.0 (https://github.com/WinMerge/winmerge/blob/master/LICENSE.md)
Version: 2.16.25
Notes:

Windows Analysis

Tools to conduct forensic analysis on various Windows artifacts

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:

bmc-tools

Website: https://github.com/ANSSI-FR/bmc-tools
Description: Parse Bitmap Cache RDP files
Author: ANSSI-FR
License: CeCILL Free Software License Agreement v2.1 (https://github.com/ANSSI-FR/bmc-tools/blob/master/LICENCE.txt)
Version: 3.02
Notes:

Event Log Explorer

Website: https://eventlogxp.com/
Description: Windows Event Log Parser
Author: FSPro
License: Multiple (https://eventlogxp.com/order.html)
Version: 5.3
Notes: 30 Day Trial

Hibernation-Recon

Website: https://arsenalrecon.com
Description: Tool to parse a Windows hibernation file
Author: Arsenal Recon
License: EULA
Version: 1.2.2.85
Notes: Available, but not installed by default

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)
Version: 2021.12
Notes:

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:

Live Response Collection (Cedarpelta)

Website: https://www.brimorlabs.com/tools/
Description: Incident Response Artifact Parser and Extractor
Author: Brian Moran
License: GNU General Public License v3.0 (see COPYING in zip file)
Version: Cedarpelta - 20190905
Notes: Also does macOS and Linux collection

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:

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:

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/Sil
3RD-PARTY.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: 2023.03.09 (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:

ThumbCache Viewer

Website: https://thumbcacheviewer.github.io/
Description: Windows Thumbnail Cache parser
Author: Eric Kutcher

License: GNU General Public License v3.0 (identified within program)
Version: 1.0.3.7
Notes:

USB Detective

Website: https://usbdetective.com
Description: Windows USB analysis tool
Author: Jason Hale
License: Software License Agreement (https://usbdetective.com/docs/usbdla.pdf)
Version: 1.6.3
Notes: Available, but not installed by default

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:

Windows Timeline

Website: https://github.com/kacos2000/WindowsTimeline
Description: Windows Timeline / Activities Cache parser
Author: Costas K.
License: Mozilla Public License v2.0 (https://github.com/kacos2000/WindowsTimeline/blob/master/LICENSE)
Version: 2.0.81.0
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

Applications required to make everything else work

.NET 3.5 Framework

Website: https://download.visualstudio.microsoft.com/download/pr/b635098a-2d1d-4142-bef6-d237545123cb/2651b87007440a15209cac296
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:

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-notices.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://github.com/git-for-windows/git/blob/main/LGPL-2.1)
Version: 2.38.1
Notes:

Graphviz

Website: https://graphviz.org
Description: Open source graph visualization software
Author: https://gitlab.com/graphviz/graphviz/-/blob/main/AUTHORS
License: Eclipse Public License (https://gitlab.com/graphviz/graphviz/-/blob/main/LICENSE)
Version: 7.0.3
Notes:

Java Runtime Environment

Website: https://www.java.com
Description: Java Engine
Author: Oracle

License: https://www.oracle.com/legal/terms.html
Version: 8u361
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:

Microsoft VC++ 2015 Build Tools

Website: https://microsoft.com
Description: Microsoft Visual C++ 2015 Build Tools
Author: Microsoft
License:
Version: 15.9.51
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

Website: https://www.python.org
Description: Python Programming Language Framework
Author: Python Software Foundation
License: Python Software Foundation License Version 2.0 (https://docs.python.org/2.7/license.html)
Version: 2.7.18
Notes:

Python 3

Website: https://www.python.org
Description: Python Programming Language Framework
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: