



Forensics Tools

Forensics Tools

A list of free and open source forensics analysis tools and other resources.

- Forensics Tools
- Collections
- Tools
 - Distributions
 - Frameworks
 - Live forensics
 - Acquisition
 - Imageing
 - Carving
 - Memory Forensics
 - Network Forensics
 - Windows Artifacts
 - ★ NTFS/MFT Processing
 - OS X Forensics
 - Mobile Forensics
 - Docker Forensics

-
- Browser Artifacts
 - Timeline Analysis
 - Disk image handling
 - Decryption
 - Management
 - Picture Analysis
 - Steganography
 - Metadata Forensics
 - Website Forensics
 - Learn Forensics
 - CTFs
 - Resources
 - Books
 - File System Corpora
 - Twitter
 - Blogs
 - Other
 - Related Awesome Lists

Collections

- DFIR – The definitive compendium project - Collection of forensic resources for learning and research. Offers lists of certifications, books, blogs, challenges and more
- DFIR-SQL-Query-Repo - Collection of SQL queries templates for digital forensics use by platform and application.
- dfir.training - Database of forensic resources focused on events, tools and more
- :star: ForensicArtifacts.com Artifact Repository - Machine-readable knowledge base of forensic artifacts

Tools

- Forensics tools on Wikipedia
- Eric Zimmerman's Tools

Challenges

- Blue Team Labs Online

Distributions

- bitscout - LiveCD/LiveUSB for remote forensic acquisition and analysis
- CAINE
- GRML-Forensic
- Remnux - Distro for reverse-engineering and analyzing malicious software
- :star:SANS Investigative Forensics Toolkit (sift) - Linux distribution for forensic analysis
- Santoku Linux - Santoku is dedicated to mobile forensics, analysis, and security, and packaged in an easy to use, Open Source platform.
- Sumuri Paladin - Linux distribution that simplifies various forensics tasks in a forensically sound manner via the PALADIN Toolbox
- Tsurugi Linux - Linux distribution for forensic analysis
- WinFE - Windows Forensics environment

Frameworks

- :star:Autopsy - SleuthKit GUI
- dff - Forensic framework
- dexter - Dexter is a forensics acquisition framework designed to be extensible and secure
- IntelMQ - IntelMQ collects and processes security feeds
- Kuiper - Digital Investigation Platform
- Laika BOSS - Laika is an object scanner and intrusion detection system
- RegRippy - is a framework for reading and extracting useful forensics data from Windows registry hives.
- PowerForensics - PowerForensics is a framework for live disk forensic analysis
- :star: The Sleuth Kit - Tools for low level forensic analysis
- turbinia - Turbinia is an open-source framework for deploying, managing, and running forensic workloads on cloud platforms
- IPED - Indexador e Processador de Evidências Digitais - Brazilian Federal Police Tool for Forensic Investigations

Live forensics

- grr - GRR Rapid Response: remote live forensics for incident response

-
- Linux Expl0rer - Easy-to-use live forensics toolbox for Linux endpoints written in Python & Flask
 - mig - Distributed & real time digital forensics at the speed of the cloud
 - osquery - SQL powered operating system analytics

Acquisition

- artifactcollector - A customizable agent to collect forensic artifacts on any Windows, macOS or Linux system
- ArtifactExtractor - Extract common Windows artifacts from source images and VSCs
- AVML - A portable volatile memory acquisition tool for Linux
- DFIR ORC - Forensics artefact collection tool for systems running Microsoft Windows
- DumpIt -
- FastIR Collector - Collect artifacts on windows
- FireEye Memoryze
- LiME - Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices, formerly called DMD
- Magnet RAM Capture - is a free imaging tool designed to capture the physical memory
- :star:RAM Capturer - by Belkasoft is a free tool to dump the data from a computer's volatile memory. It's compatible with Windows OS.
- Velociraptor - Velociraptor is a tool for collecting host based state information using Velocidex Query Language (VQL) queries

Imageing

- :star:Belkalmager - by Belkasoft allows you to create images of hard and removable disks, Android and iOS devices and download data from the cloud.
- dc3dd - Improved version of dd
- dcfldd - Different improved version of dd (this version has some bugs!, another version is on [github adulau/dcfldd](#))
- FTK Imager - Free imageing tool for windows
- :star:Guymager - Open source version for disk imageing on linux systems

Carving

- bstrings - Improved strings utility
- bulk_extractor - Extracts informations like email adresses, creditcard numbers and histograms of disk images

-
- floss - Static analysis tool to automatically deobfuscate strings from malware binaries
 - :star: photorec - File carving tool
 - swap_digger - A bash script used to automate Linux swap analysis, automating swap extraction and searches for Linux user credentials, Web form credentials, Web form emails, etc.

Memory Forensics

- FireEye RedLine - provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.
- inVtero.net - High speed memory analysis framework developed in .NET supports all Windows x64, includes code integrity and write support
- KeeFarce - Extract KeePass passwords from memory
- MemProcFS - An easy and convenient way of accessing physical memory as files a virtual file system.
- Rekall - Memory Forensic Framework
- :star:volatility - The memory forensic framework
- VolUtility - Web App for Volatility framework

Network Forensics

- NetworkMiner
- Xplico
- :star:WireShark

Windows Artifacts

- Beagle - Transform data sources and logs into graphs
- CrowdResponse - by CrowdStrike is a static host data collection tool
- FRED - Cross-platform microsoft registry hive editor
- LastActivityView - LastActivityView by Nirsoft is a tool for Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer.
- LogonTracer - Investigate malicious Windows logon by visualizing and analyzing Windows event log
- python-evt - Pure Python parser for classic Windows Event Log files (.evt)
- RegRipper3.0 - RegRipper is an open source Perl tool for parsing the Registry and presenting it for analysis.

NTFS/MFT Processing

- MFT-Parsers - Comparison of MFT-Parsers
- MFTExtractor - MFT-Parser
- NTFS journal parser
- NTFS USN Journal parser
- RecuperaBit - Reconstruct and recover NTFS data
- python-ntfs - NTFS analysis

OS X Forensics

- APFS Fuse - is a read-only FUSE driver for the new Apple File System
- APOLLO
- Disk-Arbitrator - is a Mac OS X forensic utility designed to help the user ensure correct forensic procedures are followed during imaging of a disk device
- MAC OSX Artifacts - locations artifacts by mac4n6 group
- mac_apt (macOS Artifact Parsing Tool) - Extracts forensic artifacts from disk images or live machines
- MacLocationsScraper - Dump the contents of the location database files on iOS and macOS.
- macMRUParser - Python script to parse the Most Recently Used (MRU) plist files on macOS into a more human friendly format.
- OSXAuditor
- OSX Collect

Mobile Forensics

- Andriller - is software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices
- ALEAPP - An Android Logs Events and Protobuf Parser
- iOS Frequent Locations Dumper - Dump the contents of the StateModel#.archive files located in /private/var/mobile/Library/Caches/com.apple.routined/
- MEAT - Perform different kinds of acquisitions on iOS devices
- MobSF - is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.
- OpenBackupExtractor - is an app for extracting data from iPhone and iPad backups.

Docker Forensics

- dof (Docker Forensics Toolkit) - Extracts and interprets forensic artifacts from disk images of Docker Host systems
- Docker Explorer Extracts and interprets forensic artifacts from disk images of Docker Host systems

Browser Artifacts

- ChromeCacheView - by Nirsoft is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache
- chrome-url-dumper - Dump all local stored information collected by Chrome
- Dumpzilla - extract all forensic interesting information of Firefox, Iceweasel and Seamonkey browsers
- hindsight - Internet history forensics for Google Chrome/Chromium
- unfurl - Extract and visualize data from URLs

Timeline Analysis

- DFTimewolf - Framework for orchestrating forensic collection, processing and data export using GRR and Rekal
- :star: plaso - Extract timestamps from various files and aggregate them
- timeliner - A rewrite of mactime, a bodyfile reader
- timesketch - Collaborative forensic timeline analysis

Disk image handling

- Disk Arbitrator - A Mac OS X forensic utility designed to help the user ensure correct forensic procedures are followed during imaging of a disk device
- imagemounter - Command line utility and Python package to ease the (un)mounting of forensic disk images
- libewf - Libewf is a library and some tools to access the Expert Witness Compression Format (EWF, E01)
- OSFMount - allows you to mount local disk image files (bit-for-bit copies of an entire disk or disk partition) in Windows as a physical disk or a logical drive
- PancakeViewer - Disk image viewer based in dfvfs, similar to the FTK Imager viewer.
- xmount - Convert between different disk image formats

Decryption

- hashcat - Fast password cracker with GPU support
- John the Ripper - Password cracker

Management

- dfirtrack - Digital Forensics and Incident Response Tracking application, track systems
- Incidents - Web application for organizing non-trivial security investigations. Built on the idea that incidents are trees of tickets, where some tickets are leads

Picture Analysis

- Ghir0 - is a fully automated tool designed to run forensics analysis over a massive amount of images
- sherloq - An open-source digital photographic image forensic toolset

Steganography

- Binwalk - Binwalk is a fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
- Foremost - is a program to recover files based on their headers and footers
- Sonicvisualizer
- Steghide - is a steganography program that hides data in various kinds of image and audio files
- Stegsolve - analyze images in different planes by taking off bits of the image
- Wavsteg - is a steganography program that hides data in various kinds of image and audio files
- Zsteg - A steganographic coder for WAV files
- Audacity - an easy-to-use, multi-track audio editor and recorder

Metadata Forensics

- ExifTool by Phil Harvey
- Exiv2 - Exiv2 is a Cross-platform C++ library and a command line utility to manage image meta-data
- FOCA - FOCA is a tool used mainly to find metadata and hidden information in the documents

Website Forensics

Learn forensics

- Forensic challenges - Mindmap of forensic challenges
- OpenLearn - Digital forensic course
- Training material - Online training material by European Union Agency for Network and Information Security for different topics (e.g. Digital forensics, Network forensics)

Challenges

- AnalystUnknown Cyber Range
- Champlain College DFIR CTF
- Corelight CTF
- CyberDefenders
- DefCon CTFs - archive of DEF CON CTF challenges.
- Forensics CTFs
- IncidentResponse Challenge
- MagnetForensics CTF Challenge
- MalwareTech Challenges
- MalwareTraffic Analysis
- MemLabs
- NW3C Challenges
- PivotProject
- Precision Widgets of North Dakota Intrusion
- ReverseEngineering Challenges
- SANS Forensics Challenges

Resources

Webs

- ForensicsFocus
- InsecInstitute Resources
- SANS Digital Forensics

Blogs

- Cyberforensics
- Cyberforensicator
- DigitalForensicsMagazine
- FlashbackData
- Netresec
- roDigitalForensics
- SANS Forensics Blog
- SecurityAffairs - blog by Pierluigi Paganini
- thisweekin4n6.wordpress.com - Weekly updates for forensics
- Zena Forensics

Books

more at Recommended Readings by Andrew Case

- Network Forensics: Tracking Hackers through Cyberspace - Learn to recognize hackers' tracks and uncover network-based evidence
- The Art of Memory Forensics - Detecting Malware and Threats in Windows, Linux, and Mac Memory
- The Practice of Network Security Monitoring - Understanding Incident Detection and Response
- Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery - Cell Phone Investigations is the most comprehensive book written on cell phones, cell sites, and cell related data.

File System Corpora

- Digital Forensic Challenge Images - Two DFIR challenges with images
- Digital Forensics Tool Testing Images
- FAU Open Research Challenge Digital Forensics
- The CFReDS Project
 - Hacking Case (4.5 GB NTFS Image)

Twitter

- @4n6ist

-
- @aheadless
 - @AppleExaminer - Apple OS X & iOS Digital Forensics
 - @blackbagtech
 - @carrier4n6 - Brian Carrier, author of Autopsy and the Sleuth Kit
 - @CindyMurph - Detective & Digital Forensic Examiner
 - @EricRZimmerman - Certified SANS Instructor
 - @forensikblog - Computer forensic geek
 - @HECFBlog - SANS Certified Instructor
 - @Hexacorn - DFIR+Malware
 - @hiddenillusion
 - @iamevltwin - Mac Nerd, Forensic Analyst, Author & Instructor of SANS FOR518
 - @jaredcatkinson - PowerShell Forensics
 - @maridegrazia - Computer Forensics Examiner
 - @sleuthkit
 - @williballenthin
 - @XWaysGuide

Other

- /r/computerforensics/ - Subreddit for computer forensics
- ForensicControl -
- ForensicPosters - Posters of file system structures
- HFS+ Resources
- mac4n6 Presentations - Presentation Archives for OS X and iOS Related Research
- SANS Forensics CheatSheets - Different CheatSheets from SANS
- SANS Digital Forensics Posters - Digital Forensics Posters from SANS
- SANS WhitePapers - White Papers written by forensic practitioners seeking GCFA, GCFE, and GREM Gold

Related Awesome Lists

- Android Security
- AppSec
- Awesome Forensics
- CTFs
- Hacking
- Honey pots

-
- Incident-Response
 - Infosec
 - Malware Analysis
 - Pentesting
 - Security
 - Social Engineering
 - YARA