cugu / **awesome-forensics**

Watch 58 Star 386 Fork 109

A curated list of awesome forensic analysis tools and resources

computer-forensics digital-forensics forensic-analysis dfir open-source free

76 commits **1** branch **0** releases **9** contributors CC0-1.0

Branch: **master** New pull request Find file Clone or download

hslatman and **cugu** Add Disk Arbitrator (#15) Latest commit `9bdb21e` 4 days ago

.travis.yml	Create .travis.yml	2 years ago

CONTRIBUTING.md	Update CONTRIBUTING.md	7 months ago
LICENSE	Initial commit	2 years ago
README.md	Add Disk Arbitrator (#15)	4 days ago

README.md

Awesome Forensics build failing

Curated list of awesome **free** (mostly open source) forensic analysis tools and resources.

Collections

- DFIR – The definitive compendium project - Collection of forensic resources for learning and research. Offers lists of certifications, books, blogs, challenges and more
- dfir.training - Database of forensic resources focused on events, tools and more
- ForensicArtifacts.com Artifact Repository - Machine-readable knowledge base of forensic artifacts

Tools

- Forensics tools on Wikipedia
- Free computer forensic tools - Comprehensive list of free computer forensic tools

Distributions

- bitscout - LiveCD/LiveUSB for remote forensic acquisition and analysis
- deft - Linux distribution for forensic analysis
- SANS Investigative Forensics Toolkit (sift) - Linux distribution for forensic analysis

Frameworks

- dff - Forensic framework
- IntelMQ - IntelMQ collects and processes security feeds
- Laika BOSS - Laika is an object scanner and intrusion detection system
- PowerForensics - PowerForensics is a framework for live disk forensic analysis
- 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

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

Imageing

- 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
- Guymager - Open source version for disk imageing on linux systems

Carving

more at Malware Analysis List

- bstrings - Improved strings utility
- bulk_extractor - Extracts informations like email adresses, creditscard numbers and histrograms of disk images
- floss - Static analysis tool to automatically deobfuscate strings from malware binaries
- photorec - File carving tool

Memory Forensics

more at Malware Analysis List

- 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
- Rekall - Memory Forensic Framework
- volatility - The memory forensic framework
- VolUtility - Web App for Volatility framework

Network Forensics

more at Malware Analysis List, Forensicswiki's Tool List, awesome-pcaptools and Wireshark Tool and Script List

- SiLK Tools - SiLK is a suite of network traffic collection and analysis tools

- Wireshark - The network traffic analysis tool
- NetLytics - Analytics platform to process network data on Spark.

Windows Artifacts

more at Malware Analysis List

- ArtifactExtractor - Extract common Windows artifacts from source images and VSCs
- FastIR Collector - Collect artifacts on windows
- FRED - Cross-platform microsoft registry hive editor
- LogonTracer - Investigate malicious Windows logon by visualizing and analyzing Windows event log
- 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

- OSXAuditor

Internet Artifacts

- chrome-url-dumper - Dump all local stored infromation collected by Chrome
- hindsight - Internet history forensics for Google Chrome/Chromium

Timeline Analysis

- DFTimewolf - Framework for orchestrating forensic collection, processing and data export using GRR and Rekall
- plaso - Extract timestamps from various files and aggregate them
- timesketch - Collaborative forensic timeline analysis

Disk image handling

- aff4 - AFF4 is an alternative, fast file format
- 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)
- xmount - Convert between different disk image formats

Decryption

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

Learn forensics

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

CTFs

- Forensics CTFs
- Precision Widgets of North Dakota Intrusion

Resources

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

File System Corpora

- Digital Forensic Challenge Images - Two DFIR challanges 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
- @4n6k
- @aheadless

- @AppleExaminer - Apple OS X & iOS Digital Forensics
- @blackbagtech
- @carrier4n6 - Brian Carrier, author of Autopsy and the Sleuth Kit
- @CindyMurph - Detective & Digital Forensic Examiner
- @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

Blogs

- thisweekin4n6.wordpress.com - Weekly updates for forensics

Other

- /r/computerforensics/ - Subreddit for computer forensics
- ForensicPosters - Posters of file system structures

Related Awesome Lists

- Android Security
- AppSec
- Binary
- CTFs
- Hacking
- Honeypots
- Incident-Response
- Infosec
- Malware Analysis
- Pentesting
- Security
- YARA

Contributing

Pull requests and issues with suggestions are welcome!