



Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

meirwah / awesome-incident-response

Watch

269

★ Star

1,908

🍴 Fork

500

<> Code

! Issues 0

🔗 Pull requests 2

📁 Projects 0

📊 Insights

## Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

### A curated list of tools for incident response

incident-response

security

cybersecurity

dfir

awesome-list

awesome

list

📄 273 commits

🔗 1 branch

📦 0 releases

👤 31 contributors

📄 Apache-2.0

Branch: master ▾

New pull request

Find file

Clone or download ▾






meirwah Merge pull request #110 from megan201296/master ...

Latest commit 7d2d156 14 days ago

📄 LICENSE

Initial commit

3 years ago

 <a href="#">README.md</a>	Update README.md	15 days ago
 <a href="#">README_ch.md</a>	Update as per the lastest EN version	2 months ago
 <a href="#">contributing.md</a>	add contrib guide	3 years ago

## README.md

# awesome-incident-response

---

A curated list of tools and resources for security incident response, aimed to help security analysts and [DFIR](#) teams.



## Contents

---

- [All in one tools](#)
- [Books](#)
- [Communities](#)
- [Disk Image Creation Tools](#)
- [Evidence Collection](#)
- [Incident Management](#)
- [Linux Distributions](#)
- [Linux Evidence Collection](#)
- [Log Analysis Tools](#)
- [Memory Analysis Tools](#)

- [Memory Imaging Tools](#)
- [OSX Evidence Collection](#)
- [Other lists](#)
- [Other tools](#)
- [Playbooks](#)
- [Process Dump Tools](#)
- [Sandboxing/reversing tools](#)
- [Timeline tools](#)
- [Videos](#)
- [Windows Evidence Collection](#)

## IR tools Collection

---

### All in one Tools

- [Belkasoft Evidence Center](#) - The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps
- [CimSweep](#) - CimSweep is a suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows
- [CIRTKit](#) - CIRTKit is not just a collection of tools, but also a framework to aid in the ongoing unification of Incident Response and Forensics investigation processes
- [Cyber Triage](#) - Cyber Triage remotely collects and analyzes endpoint data to help determine if it is compromised. It's agentless approach and focus on ease of use and automation allows companies to respond without major infrastructure changes and without a team of forensics experts. Its results are used to decide if the system should be erased or investigated further.

- [Digital Forensics Framework](#) - DFF is an Open Source computer forensics platform built on top of a dedicated Application Programming Interface (API). DFF proposes an alternative to the aging digital forensics solutions used today. Designed for simple use and automation, the DFF interface guides the user through the main steps of a digital investigation so it can be used by both professional and non-expert to quickly and easily conduct a digital investigations and perform incident response
- [Doorman](#) - Doorman is an osquery fleet manager that allows remote management of osquery configurations retrieved by nodes. It takes advantage of osquery's TLS configuration, logger, and distributed read/write endpoints, to give administrators visibility across a fleet of devices with minimal overhead and intrusiveness
- [Envdb](#) - Envdb turns your production, dev, cloud, etc environments into a database cluster you can search using osquery as the foundation. It wraps the osquery process with a (cluster) node agent that can communicate back to a central location
- [Falcon Orchestrator](#) - Falcon Orchestrator by CrowdStrike is an extendable Windows-based application that provides workflow automation, case management and security response functionality.
- [GRR Rapid Response](#) - GRR Rapid Response is an incident response framework focused on remote live forensics. It consists of a python agent (client) that is installed on target systems, and a python server infrastructure that can manage and talk to the agent
- [Kolide Fleet](#) - Kolide Fleet is a state of the art host monitoring platform tailored for security experts. Leveraging Facebook's battle-tested osquery project, Kolide delivers fast answers to big questions.
- [Limacharlie](#) - an endpoint security platform. It is itself a collection of small projects all working together, and gives you a cross-platform (Windows, OSX, Linux, Android and iOS) low-level environment allowing you to manage and push additional modules into memory to extend its functionality
- [MIG](#) - Mozilla Investigator (MIG) is a platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security
- [MozDef](#) - The Mozilla Defense Platform (MozDef) seeks to automate the security incident handling process and facilitate the real-time activities of incident handlers

- [nightHawk](#) - the nightHawk Response Platform is an application built for asynchronous forensic data presentation using ElasticSearch as the backend. It's designed to ingest Redline collections.
- [Open Computer Forensics Architecture](#) - Open Computer Forensics Architecture (OCFA) is another popular distributed open-source computer forensics framework. This framework was built on Linux platform and uses PostgreSQL database for storing data
- [Osquery](#) - with osquery you can easily ask questions about your Linux and OSX infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company. Queries in the *incident-response pack* help you detect and respond to breaches
- [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
- [The Sleuth Kit & Autopsy](#) - The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things
- [TheHive](#) - TheHive is a scalable 3-in-1 open source and free solution designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.
- [X-Ways Forensics](#) - X-Ways is a forensics tool for Disk cloning and imaging. It can be used to find deleted files and disk analysis
- [Zentral](#) - combines osquery's powerful endpoint inventory features with a flexible notification and action framework. This enables one to identify and react to changes on OS X and Linux clients.

## Books

- [Dfir intro](#) - By Scott J. Roberts
- [The Practice of Network Security Monitoring: Understanding Incident Detection and Response](#) - Richard Bejtlich's book on IR

## Communities

- [augmentd](#) - Community driven site providing a list of searches that can be implemented in and executed with a variety of common security tools.
- [Sans DFIR mailing list](#) - Mailing list by SANS for DFIR
- [Slack DFIR channel](#) - Slack DFIR Community channel - [Signup here](#)

## Disk Image Creation Tools

- [AccessData FTK Imager](#) - AccessData FTK Imager is a forensics tool whose main purpose is to preview recoverable data from a disk of any kind. FTK Imager can also acquire live memory and paging file on 32bit and 64bit systems
- [Bitscout](#) - Bitscout by Vitaly Kamluk helps you build your fully-trusted customizable LiveCD/LiveUSB image to be used for remote digital forensics (or perhaps any other task of your choice). It is meant to be transparent and monitorable by the owner of the system, forensically sound, customizable and compact.
- [GetData Forensic Imager](#) - GetData Forensic Imager is a Windows based program that will acquire, convert, or verify a forensic image in one of the following common forensic file formats
- [Guymager](#) - Guymager is a free forensic imager for media acquisition on Linux
- [Magnet ACQUIRE](#) - ACQUIRE by Magnet Forensics allows various types of disk acquisitions to be performed on Windows, Linux, and OS X as well as mobile operating systems.

## Evidence Collection

- [bulk\\_extractor](#) - bulk\_extractor is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Because of ignoring the file system structure, the program distinguishes itself in terms of speed and thoroughness
- [Cold Disk Quick Response](#) - uses a streamlined list of parsers to quickly analyze a forensic image file (dd, E01, .vmdk, etc) and output nine reports

- [ir-rescue](#) - *ir-rescue* is a Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.
- [Live Response Collection](#) - The Live Response collection by BriMor Labs is an automated tool that collects volatile data from Windows, OSX, and \*nix based operating systems

## Incident Management

- [CyberCPR](#) - A community and commercial incident management tool with Need-to-Know built in to support GDPR compliance while handling sensitive incidents
- [Cyphon](#) - Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.
- [Demisto](#) - Demisto community edition(free) offers full Incident lifecycle management, Incident Closure Reports, team assignments and collaboration, and many integrations to enhance automations (like Active Directory, PagerDuty, Jira and much more...)
- [FIR](#) - Fast Incident Response (FIR) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike
- [RTIR](#) - Request Tracker for Incident Response (RTIR) is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker
- [SCOT](#) - Sandia Cyber Omni Tracker (SCOT) is an Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user
- [threat\\_note](#) - A lightweight investigation notebook that allows security researchers the ability to register and retrieve indicators related to their research

## Linux Distributions

- [ADIA](#) - The Appliance for Digital Investigation and Analysis (ADIA) is a VMware-based appliance used for digital investigation and acquisition and is built entirely from public domain software. Among the tools contained in ADIA are Autopsy, the Sleuth Kit, the Digital Forensics Framework, log2timeline, Xplico, and Wireshark. Most of the system maintenance uses Webmin. It is designed for small-to-medium sized digital investigations and acquisitions. The appliance runs under Linux, Windows, and Mac OS. Both i386 (32-bit) and x86\_64 (64-bit) versions are available.
- [CAINE](#) - The Computer Aided Investigative Environment (CAINE) contains numerous tools that help investigators during their analysis, including forensic evidence collection
- [CCF-VM](#) - CyLR CDQR Forensics Virtual Machine (CCF-VM): An all-in-one solution to parsing collected data, making it easily searchable with built-in common searches, enable searching of single and multiple hosts simultaneously
- [DEFT](#) - The Digital Evidence & Forensics Toolkit (DEFT) is a Linux distribution made for computer forensic evidence collection. It comes bundled with the Digital Advanced Response Toolkit (DART) for Windows. A light version of DEFT, called DEFT Zero, is also available, which is focused primarily on forensically sound evidence collection
- [NST - Network Security Toolkit](#) - Linux distribution that includes a vast collection of best-of-breed open source network security applications useful to the network security professional
- [PALADIN](#) - PALADIN is a modified Linux distribution to perform various forensics task in a forensically sound manner. It comes with many open source forensics tools included
- [Security Onion](#) - Security Onion is a special Linux distro aimed at network security monitoring featuring advanced analysis tools
- [SIFT Workstation](#) - The SANS Investigative Forensic Toolkit (SIFT) Workstation demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated

## Linux Evidence Collection

- [FastIR Collector Linux](#) - FastIR for Linux collects different artefacts on live Linux and records the results in csv files



## Log Analysis Tools

- [Lorg](#) - a tool for advanced HTTPD logfile security analysis and forensics
- [Logdissect](#) - A CLI utility and Python API for analyzing log files and other data.

## Memory Analysis Tools

- [Evolve](#) - Web interface for the Volatility Memory Forensics Framework
- [inVtero.net](#) - Advanced memory analysis for Windows x64 with nested hypervisor support
- [KnTList](#) - Computer memory analysis tools
- [LiME](#) - LiME (formerly DMD) is a Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices
- [Memoryze](#) - Memoryze by Mandiant is a free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images, and on live systems, can include the paging file in its analysis
- [Memoryze for Mac](#) - Memoryze for Mac is Memoryze but then for Macs. A lower number of features, however
- [Rekall](#) - Open source tool (and library) for the extraction of digital artifacts from volatile memory (RAM) samples
- [Responder PRO](#) - Responder PRO is the industry standard physical memory and automated malware analysis solution
- [Volatility](#) - An advanced memory forensics framework
- [VolatilityBot](#) - VolatilityBot is an automation tool for researchers cuts all the guesswork and manual tasks out of the binary extraction phase, or to help the investigator in the first steps of performing a memory analysis investigation
- [VolDiff](#) - Malware Memory Footprint Analysis based on Volatility
- [WindowsSCOPE](#) - another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory

## Memory Imaging Tools

- [Belkasoft Live RAM Capturer](#) - A tiny free forensic tool to reliably extract the entire content of the computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system
- [Linux Memory Grabber](#) - A script for dumping Linux memory and creating Volatility profiles.
- [Magnet RAM Capture](#) - Magnet RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer. Supports recent versions of Windows
- [OSForensics](#) - OSForensics can acquire live memory on 32bit and 64bit systems. A dump of an individual process's memory space or physical memory dump can be done

## OSX Evidence Collection

- [Knockknock](#) - Displays persistent items(scripts, commands, binaries, etc.) that are set to execute automatically on OSX
- [mac\\_apl - macOS Artifact Parsing Tool](#) - Plugin based forensics framework for quick mac triage that works on live machines, disk images or individual artifact files
- [OSX Auditor](#) - OSX Auditor is a free Mac OS X computer forensics tool
- [OSX Collector](#) - An OSX Auditor offshoot for live response

## Other Lists

- [List of various Security APIs](#) - A collective list of public JSON APIs for use in security.

## Other Tools

- [Cortex](#) - Cortex allows you to analyze observables such as IP and email addresses, URLs, domain names, files or hashes one by one or in bulk mode using a Web interface. Analysts can also automate these operations using its REST API.
- [Crits](#) - a web-based tool which combines an analytic engine with a cyber threat database

- [domfind](#) - *domfind* is a Python DNS crawler for finding identical domain names under different TLDs.
- [DumpsterFire](#) - The DumpsterFire Toolset is a modular, menu-driven, cross-platform tool for building repeatable, time-delayed, distributed security events. Easily create custom event chains for Blue Team drills and sensor / alert mapping. Red Teams can create decoy incidents, distractions, and lures to support and scale their operations.
- [Fenrir](#) - Fenrir is a simple IOC scanner. It allows scanning any Linux/Unix/OSX system for IOCs in plain bash. Created by the creators of THOR and LOKI
- [Fileintel](#) - Pull intelligence per file hash
- [HELK](#) - Threat Hunting platform
- [Hindsight](#) - Internet history forensics for Google Chrome/Chromium
- [Hostintel](#) - Pull intelligence per host
- [imagemounter](#) - Command line utility and Python package to ease the (un)mounting of forensic disk images
- [Kansa](#) - Kansa is a modular incident response framework in Powershell
- [rastrea2r](#) - allows one to scan disks and memory for IOCs using YARA on Windows, Linux and OS X
- [RaQet](#) - RaQet is an unconventional remote acquisition and triaging tool that allows triage a disk of a remote computer (client) that is restarted with a purposely built forensic operating system
- [Stalk](#) - Collect forensic data about MySQL when problems occur
- [SearchGiant](#) - a commandline utility to acquire forensic data from cloud services
- [Stenographer](#) - Stenographer is a packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. It stores as much history as it possible, managing disk usage, and deleting when disk limits are hit. It's ideal for capturing the traffic just before and during an incident, without the need explicit need to store all of the network traffic
- [sqhunter](#) - a threat hunter based on osquery and Salt Open (SaltStack) that can issue ad-hoc or distributed queries without the need for osquery's tls plugin. sqhunter allows you to query open network sockets and check them against threat intelligence sources.

- [traceroute-circl](#) - traceroute-circl is an extended traceroute to support the activities of CSIRT (or CERT) operators. Usually CSIRT team have to handle incidents based on IP addresses received. Created by Computer Emergency Response Center Luxembourg
- [X-Ray 2.0](#) - A Windows utility (poorly maintained or no longer maintained) to submit virus samples to AV vendors

## Playbooks

- [Demisto Playbooks Collection](#) - Playbooks collection
- [IRM](#) - Incident Response Methodologies by CERT Societe Generale
- [IR Workflow Gallery](#) - Different generic incident response workflows, e.g. for malware outbreak, data theft, unauthorized access,... Every workflow consists of seven steps: prepare, detect, analyze, contain, eradicate, recover, post-incident handling. The workflows are online available or for download
- [PagerDuty Incident Response Documentation](#) - Documents that describe parts of the PagerDuty Incident Response process. It provides information not only on preparing for an incident, but also what to do during and after. Source is available on [GitHub](#).

## Process Dump Tools

- [Microsoft User Mode Process Dumper](#) - The User Mode Process Dumper (userdump) dumps any running Win32 processes memory image on the fly
- [PMDump](#) - PMDump is a tool that lets you dump the memory contents of a process to a file without stopping the process

## Sandboxing/reversing tools

- [Cuckoo](#) - Open Source Highly configurable sandboxing tool
- [Cuckoo-modified](#) - Heavily modified Cuckoo fork developed by community
- [Cuckoo-modified-api](#) - A Python library to control a cuckoo-modified sandbox

- [Hybrid-Analysis](#) - Hybrid-Analysis is a free powerful online sandbox by Payload Security
- [Malwr](#) - Malwr is a free online malware analysis service and community, which is powered by the Cuckoo Sandbox
- [Mastiff](#) - MASTIFF is a static analysis framework that automates the process of extracting key characteristics from a number of different file formats
- [Metadefender Cloud](#) - Metadefender is a free threat intelligence platform providing multiscanning, data sanitization and vulnerability assesment of files
- [Viper](#) - Viper is a python based binary analysis and management framework, that works well with Cuckoo and YARA
- [Virusotal](#) - Virustotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners
- [Visualize\\_Logs](#) - Open source visualization library and command line tools for logs. (Cuckoo, Procmon, more to come...)

## Timeline tools

- [Highlighter](#) - Free Tool available from Fire/Mandiant that will depict log/text file that can highlight areas on the graphic, that corresponded to a key word or phrase. Good for time lining an infection and what was done post compromise
- [Morgue](#) - A PHP Web app by Etsy for managing postmortems.
- [Plaso](#) - a Python-based backend engine for the tool log2timeline
- [Timesketch](#) - open source tool for collaborative forensic timeline analysis

## Videos

- [Demisto IR video resources](#) - Video Resources for Incident Response and Forensics Tools
- [The Future of Incident Response](#) - Presented by Bruce Schneier at OWASP AppSecUSA 2015

## Windows Evidence Collection

- [AChoir](#) - Achoir is a framework/scripting tool to standardize and simplify the process of scripting live acquisition utilities for Windows
- [Binaryforay](#) - list of free tools for win forensics (<http://binaryforay.blogspot.co.il/>)
- [Crowd Response](#) - Crowd Response by CrowdStrike is a lightweight Windows console application designed to aid in the gathering of system information for incident response and security engagements. It features numerous modules and output formats
- [FastIR Collector](#) - FastIR Collector is a tool that collects different artefacts on live Windows systems and records the results in csv files. With the analyses of these artefacts, an early compromise can be detected
- [FECT](#) - Fast Evidence Collector Toolkit (FECT) is a light incident response toolkit to collect evidences on a suspicious Windows computer. Basically it is intended to be used by non-tech savvy people working with a journeyman Incident Handler
- [Fibratus](#) - tool for exploration and tracing of the Windows kernel
- [IOC Finder](#) - IOC Finder is a free tool from Mandiant for collecting host system data and reporting the presence of Indicators of Compromise (IOCs). Support for Windows only
- [Fidelis ThreatScanner](#) - Fidelis ThreatScanner is a free tool from Fidelis Cybersecurity that uses OpenIOC and YARA rules to report on the state of an endpoint. The user provides OpenIOC and YARA rules and executes the tool. ThreatScanner measures the state of the system and, when the run is complete, a report for any matching rules is generated. Windows Only.
- [LOKI](#) - Loki is a free IR scanner for scanning endpoint with yara rules and other indicators(IOCs)
- [Panorama](#) - Fast incident overview on live Windows systems
- [PowerForensics](#) - Live disk forensics platform, using PowerShell
- [PSRecon](#) - PSRecon gathers data from a remote Windows host using PowerShell (v2 or later), organizes the data into folders, hashes all extracted data, hashes PowerShell and various system properties, and sends the data off to the security team. The data can be pushed to a share, sent over email, or retained locally
- [RegRipper](#) - Regripper is an open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis

- [TRIAGE-IR](#) - Triage-IR is a IR collector for Windows

