Awesome Memory Forensics

A curated list of awesome Memory Forensics for DFIR.

Memory Forensics is forensic analysis of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Consequently, the memory (RAM) must be analyzed for forensic information.

If you want to contribute, please read the contribution guidelines.

Contents

Tool

Memory Acquisition

Introduce commercial and open source tools for memory acquisition.

Software

- Surge - Volexity's Surge Collect offers flexible storage options and an intuitive interface that any responder can run to eliminate the issues associated with the corrupt data samples, crashed target computers, and ultimately, unusable data that commonly results from using other tools.
- MAGNET RAM - MAGNET RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory.

- FTK Imager - FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted.
- Winpmem - WinPmem has been the default open source memory acquisition driver for windows for a long time.
- Ram Capturer - Belkasoft Live RAM Capturer is a tiny free forensic tool that allows to reliably extract the entire contents of computer's volatile memory—even if protected by an active anti-debugging or anti-dumping system.
- LiME - A Loadable Kernel Module (LKM) which allows for volatile memory acquisition from Linux and Linux-based devices, such as Android.
- AVML - AVML is an X86_64 userland volatile memory acquisition tool written in Rust, intended to be deployed as a static binary.
- fmem - This module creates /dev/fmem device, that can be used for dumping physical memory, without limits of /dev/mem (1MB/1GB, depending on distribution).
- FEX Memory Imager - FEX Memory Imager (FEX Memory) is a free imaging tool designed to capture the physical Random Access Memory (RAM) of a suspect's running computer. This allows investigators to recover and analyze valuable artifacts found only in memory.
- MacQuisition
- Digital Collector - A powerful forensic imaging software solution to perform triage, live data acquisition and targeted data collection for Windows and Mac computers.
- varc - Volatile Artifact Collector gathers a snapshot of volatile data from a system.

Hardware

- PCILeech - PCILeech uses PCIe hardware devices to read and write target system memory. This is achieved by using DMA over PCIe. No drivers are needed on the target system.

Misc

- EVTXtract - EVTXtract recovers and reconstructs fragments of EVTX log files from raw binary data, including unallocated space and memory images.
- Volatility3 Inodes Plugin - The plugin is a pushed verion of the lsof plugin extracting inode metadata information from each files.
- Volatility3 Prefetch Plugin - The plugin is scanning, extracting and parsing Windows Prefetch files from Windows XP to Windows 11.

Memory Analysis

Introduce commercial and open source tools for memory analysis.

- Volcano - A comprehensive, cross-platform, next- generation memory analysis solution, Volexity Volcano Professional's powerful core extracts, indexes, and correlates artifacts to provide unprecedented visibility into systems' runtime state and trustworthiness.
- Volatility3 - Volatility is the world's most widely used framework for extracting digital artifacts from volatile memory (RAM) samples.
- MemProcFS - The Memory Process File System (MemProcFS) is an easy and convenient way of viewing physical memory as files in a virtual file system.
- WinDbg - The Windows Debugger (WinDbg) can be used to debug kernel-mode and user-mode code, analyze crash dumps, and examine the CPU registers while the code executes.
- Volatility - The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples.
- Volafox - macOS Memory Analysis Toolkit' is developed on Python 2.x (***Deprecated***)
- Rekall - A new branch within the Volatility project was created to explore how to make the code base more modular, improve performance, and increase usability. (***Deprecated***)
- Redline - Redline®, FireEye's premier free endpoint security tool, 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.
- Memoryze - Mandiant's Memoryze™ is 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.
- dwarf2json - Go utility that processes files containing symbol and type information to generate Volatilty3 Intermediate Symbol File (ISF) JSON output suitable for Linux and macOS analysis.

Books

- The Art of Memory Forensics - Detecting Malware and Threats in Windows, Linux, and Mac Memory.
- Practical Memory Forensics - Jumpstart effective forensic analysis of volatile memory.

Course

- Malware and Memory Forensics Training
- A Complete Practical Approach To Malware Analysis And Memory Forensics - 2022 Edition

Videos

13 Cubed

- Introduction to Memory Forensics
- Windows Memory Analysis
- Windows Process Genealogy
- Windows Process Genealogy (Update)
- Memory Forensics Baselines
- Extracting Prefetch from Memory
- Detecting Persistence in Memory
- Introduction to Redline
- Introduction to Redline (Update)
- Profiling Network Activity with Volatility 3 - GeoIP from Memory
- Volatility Profiles and Windows 10
- Dumping Processes with Volatility 3
- First Look at Volatility 3 Public Beta
- Volatility 3 and WSL 2 - Linux DFIR Tools in Windows?
- MemProcFS - This Changes Everything

DFIR Science

- Introduction to Memory Forensics with Volatility 3
- Amazon AWS EC2 Forensic Memory Acquisition - LiME
- Forensic Memory Acquisition in Linux - LiME
- Forensic Memory Acquisition in Windows - FTK Imager
- Fast password cracking - Hashcat wordlists from RAM
- What is Random Access Memory?
- Forensics: What data can you find in RAM?

Black Hat 2022

- New Memory Forensics Techniques to Defeat Device Monitoring Malware

Black Hat 2019

- Investigating Malware Using Memory Forensics - A Practical Approach

Black Hat 2012

- One-byte Modification for Breaking Memory Forensic Analysis

SANS Digital Forensics and Incident Response

- SANS DFIR Webcast - Memory Forensics for Incident Response

ETC

- Memory Forensics with Jupyter Notebooks

Articles

JPCERT

- How to Use Volatility 3 Offline
- Migrate Volatility Plugins 2 to 3
- MalConfScan with Cuckoo: Plugin to Automatically Extract Malware Configuration
- Volatility Plugin for Detecting RedLeaves Malware
- A New Tool to Detect Known Malware from Memory Images – impfuzzy for Volatility –
- A Volatility Plugin Created for Detecting Malware Used in Targeted Attacks
- Volatility Plugin for Detecting Cobalt Strike Beacon

Blogs

- Volatility3 Windows Plugin : Prefetch
- Volatility3 Linux Plugin : Inodes
- Memory analysis using volatility3 (1) - Windows 11
- Memory analysis using volatility3 (2) - Ubuntu Linux
- Memory analysis using volatility3 (3) - macOS
- Realizing Windows Memory Forensics with Volatility and Gimp

CheastSheet

- Volatility3 CheatSheet

WriteUps

Papers

Digital Investigation

- The evidence beyond the wall: Memory forensics in SGX environments

DFRWS USA 2022

- Memory Analysis of .NET and .Net Core Applications
- Juicing V8: A Primary Account for the Memory Forensics of the V8 JavaScript Engine

DFRWS EU 2022

- Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application
- Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing
- Memory forensic analysis of a programmable logic controller in industrial control systems

DFRWS USA 2021

- Duck Hunt: Memory Forensics of USB Attack Platforms
- Seance: Divination of Tool-Breaking Changes in Forensically Important Binaries
- Leveraging Intel DCI for Memory Forensics

DFRWS EU 2021

- One key to rule them all: Recovering the master key from RAM to break Android's file-based encryption

DFRWS USA 2020

- Hiding Process Memory via Anti-Forensic Techniques
- Memory Analysis of macOS Page Queues
- Memory FORESHADOW: Memory FOREnSics of HArDware cryptOcurrency Wallets – A Tool and Visualization Framework

DFRWS EU 2020

- BMCLeech: Introducing Stealthy Memory Forensics to BMC Tobias Latzo
- Tampering Digital Evidence is Hard: The Case of Main Memory Images
- On Challenges in Verifying Trusted Executable Files in Memory Forensics

Datasets

- Digital Corpora
- NIST
- The Art of Memory Forensics
- MemLabs
- Windows XP

Challenges

- 2022 Volatility Plugin Contest
- 2021 Volatility Plugin Contest
- 2020 Volatility Plugin Contest
- 2019 Volatility Plugin & Analysis Contests
- 2018 Volatility Plugin & Analysis Contests
- 2017 Volatility Plugin Contest
- 2016 Volatility Plugin Contest
- 2015 Volatility Plugin Contest
- 2014 Volatility Plugin Contest
- 2013 Volatility Plugin Contest
- 2005 DFRWS Forensic Challenge

Contributors

Thank you for your contribution!

We welcome any contribution to the extent that Code of Conduct and the License comply.