



## PRODUCTS

MANDIANT Intelligent  
Response

MCIRT

[Free Software](#)

## Memoryze



MANDIANT 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.

MANDIANT Memoryze features:

- image the full range of system memory (not reliant on API calls).
- image a process' entire address space to disk. This includes a process' loaded DLLs, EXEs, heaps and stacks.
- image a specified driver or all drivers loaded in memory to disk.
- enumerate all running processes (including those hidden by rootkits). For each process, Memoryze can:
  - report all open handles in a process (for example, all files, registry keys, etc.).
  - list the virtual address space of a given process including:
    - displaying all loaded DLLs.
    - displaying all allocated portions of the heap and execution stack.
  - list all network sockets that the process has open, including any hidden by rootkits.
  - specify the functions imported by the EXE and DLLs.
  - specify the functions exported by the EXE and DLLs.
  - hash the EXE and DLLs in the process address space> (MD5, SHA1, SHA256. This is disk based.)
  - verify the digital signatures of the EXE and DLLs. (This is disk based.)
  - output all strings in memory on a per process basis.
- identify all drivers loaded in memory, including those hidden by rootkits. For each driver, Memoryze can:
  - specify the functions the driver imports.
  - specify the functions the driver exports.
  - hash the driver. (MD5, SHA1, SHA256. this is disk based.)
  - verify the digital signature of the driver (This is disk based.)
  - output all strings in memory on a per driver base.
- report device and driver layering, which can be used to intercept network packets, keystrokes and file activity.
- identify all loaded kernel modules by walking a linked list.
- identify hooks (often used by rootkits) in the System Call Table, the Interrupt Descriptor Tables (IDTs) and driver function tables (IRP tables).

**MANDIANT Memoryze can perform all these functions on live system memory or memory image files – whether they were acquired by Memoryze or other memory acquisition tools.**

Memoryze officially supports:

- Windows 2000 Service Pack 4 (32-bit)
- Windows XP Service Pack 2 and Service Pack 3 (32-bit)
- Windows Vista Service Pack 1 and Service Pack 2 (32-bit)
- Windows 2003 Service Pack 2 (32-bit)
- Windows 2003 Service Pack 2 (64-bit)
- Windows 7 Service Pack 0 (32-bit)
- Windows 7 Service Pack 0 (64-bit)
- \*Windows 2008 Service Pack 1 and Service Pack 2 (32-bit)
- Windows 2008 R2 Service Pack 0 (64-bit)

*\*Beta Support*

In order to visualize Memoryze's output, please download [Audit Viewer](#). Audit Viewer is an open source tool that allows users to examine the results of Memoryze's analysis. Audit Viewer allows the incident responder or forensic analyst to quickly view complex XML output in an easily readable format. Using familiar grouping of data and search capabilities, Audit Viewer makes memory analysis quicker and more intuitive.

[Check out the ways you can use Memoryze.](#)

### MANDIANT IOC FINDER BEST PRACTICES



The MANDIANT consultants have created this useful field guide to illustrate using MANDIANT IOC Finder in a responsible, risk-adverse way.

[Read it now.](#)

### IOC USEFUL LINKS

**Support/Forums:**

[OpenIOC](#)  
[MANDIANT IOC Finder](#)  
[MANDIANT IOC Editor](#)

**OpenIOC Website:**

[www.OpenIOC.org](http://www.OpenIOC.org)

**White Paper:**

[An Introduction to OpenIOC](#)

**OpenIOC Inquiries:**

[info@openioc.org](mailto:info@openioc.org)

**User Guide:**

[MANDIANT IOC Finder](#)

And, if you like Memoryze's standalone capabilities, check out [MANDIANT Intelligent Response](#). It's our enterprise-grade incident response accelerator. MIR has all the memory forensics of Memoryze, plus a lot more... making enterprise live response faster and easier, especially for teams of responders. Imagine Memoryze doing deep memory forensics on thousands of machines at a time, then having the results easily searchable to find where evil is hiding across your enterprise. Then add disk analysis and live response. That's Intelligent Response.

Learn more about Memoryze...check out the [MANDIANT forums](#).

Register for updates and sneak peeks to future projects or [download now](#).

First Name

Last Name

Email

Telephone

Company

Twitter Handle

Email Opt Out☐



[Home](#) > [Products](#) > [Free Software](#) > Memoryze

PRODUCTS

SERVICES

EDUCATION

NEWS & EVENTS

ABOUT US

- Careers
- Support
- User Forums
- Contact Us
- Blog
- Twitter
- Privacy Policy

Office Locations:

- Washington, DC
- New York
- Los Angeles
- San Francisco
- Reston, VA

Washington, DC Headquarters:

- Phone: +1.703.683.3141
- Toll free: 1.800.647.7020