CounterTack®
Big Data Endpoint Detection and Response

Memory Analysis & Forensics

Competitive Comparison

	Responder	Freeware	Freeware II	Competitor "M"	Comments
	Behavior-based in-memory forensics for Windows and Linux physical memory images	Open source memory forensics tool with fairly limited functionality and bare UI	Open source memory tool designed for improved usability and integration than Freeware	Free private sector tool providing host investigative capabilities for malicious activity through memory and file analysis	
System Resources Analyzed	●	●	●	●	Includes running processes & modules, open files, registry keys, Interrupt Descriptor Table, System Service Descriptor Table, network sockets.
Rapid Analysis	◑	●	●	●	Time taken to do the analysis. Note: tools that perform a shallow version of analysis inherently do not take as long.
OS Coverage	◕	●	●	◑	Windows, Linux, OSX
Integrated Application	●	○	○	●	Distinguishes sets of tools (pieces of solution) which require complex setup versus fully-integrated solutions.
Intuitive GUI	●	○	●	○	Comprehensive view of all aspects of memory and malware.
Analysis Depth	●	○	○	○	Ability to provide thorough data and make conclusions enabling decision-making. This includes providing data structures, traits & severity (e.g. DDNA scores), disassembly (what is the code doing and what is it *intended* to do) and initial reverse engineering.
Software Maturity & Support	●	○	○	○	Level of testing including regression, compatibility, integration w/ other tools, support, etc.
Disassembly Step	●	○	○	○	Convert back from assembly language into algorithms to see what code is attempting to do.

Key: ● Best ◕ Good (75%) ◑ Average (50%) ◔ Poor (25%) ○ Uncompetitive

CounterTack Inc.
100 5th Ave, First Floor
Waltham, MA 02451
www.countertack.com

CounterTack®
Big Data Endpoint Detection and Response