HBGary
DETECT. DIAGNOSE. RESPOND.

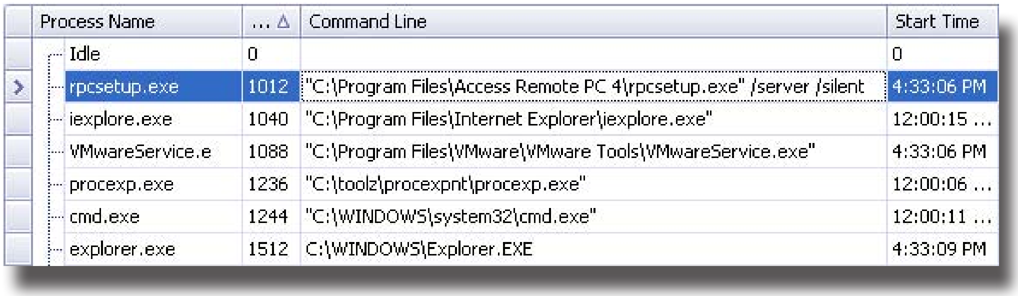
Responder™ *Field Edition*

Complete Windows Memory Investigation Suite

HBGary Responder™ Field Edition is used by computer forensic investigators, law enforcement and information security professionals to quickly capture and identify critical information found in memory. Cyber investigations are incomplete if volatile memory is not preserved and analyzed for potential evidentiary artifacts. Responder Field Edition includes memory preservation, memory analysis, rootkit behavior detection, basic malware analysis and reporting.

Preservation of Windows Physical Memory and Pagefile

FastDump Pro enables investigators and security analysts to easily "freeze the live memory" on workstations and servers. FastDump Pro preserves physical memory and the pagefile. It supports both 32– and 64-bit systems, process probing, compression, and works on systems with more than 4 gigabytes of RAM.



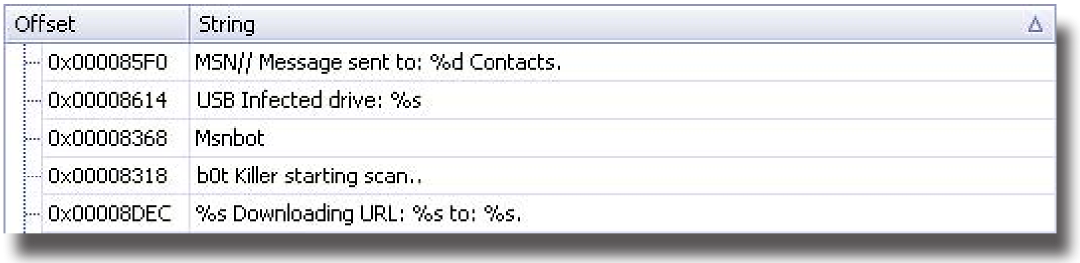
Process Name	... △	Command Line	Start Time
Idle	0		0
rpcsetup.exe	1012	"C:\Program Files\Access Remote PC 4\rpcsetup.exe" /server /silent	4:33:06 PM
iexplore.exe	1040	"C:\Program Files\Internet Explorer\iexplore.exe"	12:00:15 ...
VMwareService.e	1088	"C:\Program Files\VMware\VMware Tools\VMwareService.exe"	4:33:06 PM
procexp.exe	1236	"C:\toolz\procexpnt\procexp.exe"	12:00:06 ...
cmd.exe	1244	"C:\WINDOWS\system32\cmd.exe"	12:00:11 ...
explorer.exe	1512	C:\WINDOWS\Explorer.EXE	4:33:09 PM

Powerful Memory Searching

The system has full ASCII and Unicode searching to help indentify keys and passwords in clear text, unencrypted data, web pages, graphics, instant messenger chat sessions, document data, web based email and Outlook or Firefox email. Search the VAD tree, memory heaps and stacks per process.

Automated Memory Analytics

Responder Field Edition is the easiest to use and can analyze more types of Windows physical memory than any software in the industry. Responder automatically rebuilds all the underlying data structures in RAM for you and presents the data in a graphical user interface for rapid access to information. This includes all physical-to-virtual address mappings, recreates the object manager, exposes all objects, and enables investigators to perform a complete and comprehensive computer investigation.



Offset	String △
0x000085F0	MSN// Message sent to: %d Contacts.
0x00008614	USB Infected drive: %s
0x00008368	Msnbot
0x00008318	b0t Killer starting scan..
0x00008DEC	%s Downloading URL: %s to: %s.

Automated Malware Analysis

The new face of malware is designed to never touch the disk and reside only in memory. Responder provides you with easy to use "runtime information" to identify rootkits and malware not detected by anti-virus.

User Interface and Reporting

Responder has a friendly user interface to support investigator workflow. A flexible reporting module allows quick delivery of information to attorneys, management or clients. Reports can be exported out to CVS, PDF, RTF and other reporting standards.

Extending Digital Investigations into Live Memory

HBGary
DETECT. DIAGNOSE. RESPOND.

Supported Platforms

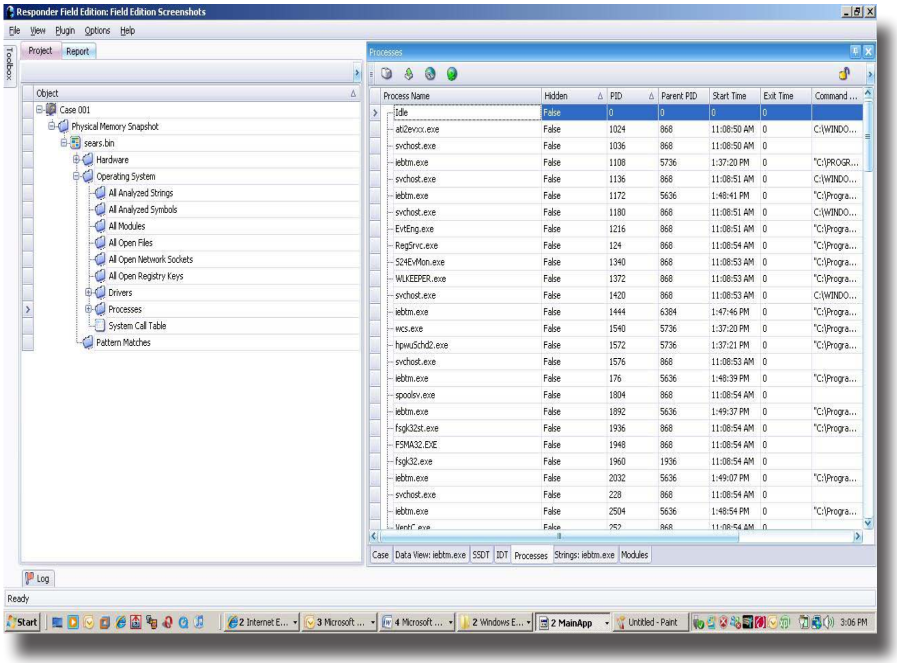
- Full support of Windows versions and service packs for Windows 2008, Vista, 2003, XP and 2000
- 32–bit and 64-bit systems
- All RAM sizes, even larger than 4 GB

FastDump Pro for RAM Preservation

- Physical memory imaging tool
- Pagefile.sys acquisition
- Process probe
- Small footprint in memory
- Works with external media
- 1 license with Responder Field Edition

Automated Memory Analysis

- Reconstruct digital objects in memory
- Processes, Drivers, and Modules
- Memory map (VAD Tree)
- Strings and Symbols
- Open network sockets
- Established network connections
- Listening ports
- Open files
- Open registry keys per process
- Interrupt Descriptor Table
- System Service Descriptor Table
- Recover keys, passwords and internet history
- Recover documents and messages
- Complete analysis of RAM and pagefile
- Full ASCII and Unicode searching



Process Name	Hidden	PID	Parent PID	Start Time	Exit Time	Command ...
Idle	False	0	0	0	0	
ati2evxx.exe	False	1024	868	11:08:50 AM	0	C:\WINDO...
svchost.exe	False	1036	868	11:08:50 AM	0	
iebtm.exe	False	1108	5736	1:37:20 PM	0	"C:\PROGR...
svchost.exe	False	1136	868	11:08:51 AM	0	C:\WINDO...
iebtm.exe	False	1172	5636	1:48:41 PM	0	"C:\Progra...
svchost.exe	False	1180	868	11:08:51 AM	0	C:\WINDO...
EvtEng.exe	False	1216	868	11:08:51 AM	0	"C:\Progra...
RegSrvc.exe	False	124	868	11:08:54 AM	0	"C:\Progra...
S24EvMon.exe	False	1340	868	11:08:53 AM	0	"C:\Progra...
WLKEEPER.exe	False	1372	868	11:08:53 AM	0	"C:\Progra...
svchost.exe	False	1420	868	11:08:53 AM	0	C:\WINDO...
iebtm.exe	False	1444	6384	1:47:46 PM	0	"C:\Progra...
wcs.exe	False	1540	5736	1:37:20 PM	0	"C:\Progra...
hpwuSchd2.exe	False	1572	5736	1:37:21 PM	0	"C:\Progra...
svchost.exe	False	1576	868	11:08:53 AM	0	
iebtm.exe	False	176	5636	1:48:39 PM	0	"C:\Progra...
spoolsv.exe	False	1804	868	11:08:54 AM	0	
iebtm.exe	False	1892	5636	1:49:37 PM	0	"C:\Progra...
fsgk32st.exe	False	1936	868	11:08:54 AM	0	"C:\Progra...
FSMA32.EXE	False	1948	868	11:08:54 AM	0	
fsgk32.exe	False	1960	1936	11:08:54 AM	0	
iebtm.exe	False	2032	5636	1:49:07 PM	0	"C:\Progra...
svchost.exe	False	228	868	11:08:54 AM	0	
iebtm.exe	False	2504	5636	1:48:54 PM	0	"C:\Progra...
VentC.exe	False	252	868	11:08:54 AM	0	

Automated Malware Analysis

- Extract binaries from memory
- Defeat packers & software protections
- Integrated x86 disassembler
- Code view (deadlisting)
- Rootkit detection—SSDT hooks, IDT hooks, driver hooks, DKOM detection
- Report suspicious binaries
- Malware behavior report

Price: $979.00 U.S.