6

iDefense Special File Investigation Tools

NAME	DESCRIPTION	LOCATION
PDF Toolkit (PDFTK)	Toolkit for PDF investigations	http://www.accesspdf.com/pdftk
CHM Decompiler	Investigate compiled Windows Help files (*.chm)	http://www.zipghost.com/chmdecompiler.html
Jad	Decompile Java class files (*.class)	http://www.kpdus.com/jad.html
Windows script decoder	Decoder for obfuscated active server pages (ASPs)	http://www.virtualconspiracy.com/?page=/scrdec/intro
GetType	Determine file type	http://philip.helger.com/gt/index.php
TrID	Determine file type	http://mark0.net/soft-trid-e.html
OffViz	Object linking and embedding (OLE) document parser	http://blogs.technet.com/srd/archive/2009/07/31/announcing-offvis.aspx
OfficeMalScanner	Find malicious Office documents	http://www.reconstructer.org/code/OfficeMalScanner.zip
Swftools	Toolkit for Flash investigations	http://www.swftools.org
Spidermonkey	JavaScript interpreter	http://www.mozilla.org/js/spidermonkey
Pdftools	Tools by Didier Stevens	http://blog.didierstevens.com/programs/pdf-tools
Flare	Flash decompiler	http://www.nowrap.de/flare.html
Nemo	Flash decompiler	http://www.docsultant.com/nemo440
Dump flash decompiler	Flash decompiler	http://www.softpedia.com/progDownload/Dump-Flash-decompiler-Download-39174.html
File Insight	Edit files in various formats	http://www.webwasher.de/download/fileinsight
Malzilla	Malware-hunting tool	http://malzilla.sourceforge.net
Dezend	Decrypt PHP files protected by Zend	http://blog.w2.ro/dezend
SYSTEM INFORMATION TOOLS		
Process Hacker	Powerful ProcExp alternative	http://processhacker.sourceforge.net
Sysinternals suite	Sysinternals suite	http://download.sysinternals.com/Files/SysinternalsSuite.zip

NAME	DESCRIPTION	LOCATION
InsideClipboard	Inspect clipboard contents	http://www.nirsoft.net/utils/inside_clipboard.html
Winlister	Inspect Windows	http://www.nirsoft.net/utils/winlister.html
DeviceTree	Investigate drivers and devices	http://www.osronline.com
Spy++	Inspect Windows (requires Microsoft Development [MSDN] subscription)	http://msdn.microsoft.com/en-us/library/aa264396(VS.60).aspx
HONEYPOTS		
Nepenthes	Collects malware by emulating vulnerabilities	http://nepenthes.carnivore.it
Mwcollectd	Malware collection daemon	http://code.mwcollect.org/projects/show/mwcollectd
honeyd	Create virtual services and hosts	http://www.honeyd.org
BROWSER TOOLS		
Fiddler	Web-debugging proxy for Internet Explorer (IE)	http://www.fiddler2.com/fiddler2/
Firebug	Web development plug-in for Firefox	http://getfirebug.com
IEDeveloperToolbar	Toolbar for control of IE document object model (DOM)	http://www.microsoft.com/downloads/details.aspx
DHTMLSpy	Inspect dynamic HTML (DHTML) page elements	http://www.download.com/DHTMLSpy/3000-2068_4-10504833.html
NETWORK TOOLS		
Wireshark	Packer sniffer	http://www.wireshark.org
Snort	Packer sniffer and intrusion detection system (IDS)	http://www.snort.org
Tcpdump	Packer sniffer	http://www.tcpdump.org
Chaosreader	Report generator for pcaps	http://chaosreader.sourceforge.net
Scapy	Packet manipulation in Python	http://www.secdev.org/projects/scapy/
Pylibpcap	Python wrappers for libpcap	http://sourceforge.net/projects/pylibpcap/
SocksiPy	Python SOCKS client module	http://socksipy.sourceforge.net
Pehunter	Snort preprocessor for portable executable (PE) files	http://honeytrap.mwcollect.org/pehunter
oSpy	Log packets by application program interface (API) hooking	http://code.google.com/p/ospy/

NAME	DESCRIPTION	LOCATION
InetSim	Internet simulation in Perl	http://www.inetsim.org
Netcat for Windows	Netcat for Windows	http://www.securityfocus.com/tools/139
DISASSEMBLERS AND PLUG-INS		
IDA Pro	Interactive disassembler (commercial)	http://www.hex-rays.com/idapro/
IDA Pro	Free version of IDA with limitations	http://www.hex-rays.com/idapro/idadownfreeware.htm
BeaEngine	Disassembler (in C/Python/Asm)	http://beatrix2004.free.fr/BeaEngine/index1.php
Distorm64	Stream disassembler (in C/Python)	http://www.ragestorm.net/distorm
pydasm	Stream disassembler in Python	http://dkbza.org/pydasm.html
HexRays	Decompiler plug-in for IDA	http://www.hexrays.com
Coverit	Code coverage plug-in for IDA	http://www.hexblog.com/2006/03/coverage_analyzer.html
pe_scripts	PE tools International Data (IDC) scripts for IDA	http://www.hex-rays.com/idapro/freefiles/pe_scripts.zip
x86emu	x86 emulation plug-in for IDA	http://www.idabook.com/x86emu
IDA Python	Python interpreter and API plug-in (installed by default in IDA 5.6)	http://www.d-dome.net/idapython/
TurboDiff	Binary-diffing plug-in for IDA	http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=turbodiff
PatchDiff2	Binary-diffing plug-in for IDA	http://cgi.tenablesecurity.com/tenable/patchdiff.php
BinDiff	Binary-diffing plug-in for IDA (commercial)	http://www.zynamics.com/bindiff.html
Findcrypt	Locate cryptography constants in IDA	http://www.hexblog.com/2006/01/findcrypt.html
IDA Stealth	Hide debugger plug-in for IDA	http://newgre.net/idastealth
VIRTUALIZATION, EMU, AND LOCKDOWN		
VMware	Virtual machines application	http://www.vmware.com
VIX API	API for scripting VMware guests	http://www.vmware.com/support/developer/vix-api/
QEMU	Emulation application	http://bellard.org/qemu/index.html
Ether	Unpack using hardware extensions	http://ether.gtisc.gatech.edu/source.html
DeepFreeze	System lockdown (commercial)	http://www.faronics.com/html/deepfreeze.asp

NAME	DESCRIPTION	LOCATION
PIN	Instrumentation	http://rogue.colorado.edu/pin/
Virtual Box	Virtual machines application	http://www.virtualbox.org
PACKING AND UNPACKING TOOLS		
Saffron	Automated unpacker for personal identification numbers (PINs)	http://www.offensivecomputing.net/?q=node/492
Collaborative RCE Library	Collaborative regional coding enhancement (RCE) library	http://www.woodmann.com/collaborative/tools/index.php/Category:Unpacking_Tools
ImpREC	Imports reconstructor	http://www.woodmann.com/collaborative/tools/index.php/ImpREC
UIF	Universal imports fixer	http://www.woodmann.com/collaborative/tools/index.php/Universal_Import_Fixer
UPX	PE packer	http://upx.sourceforge.net
PEiD	Packer identification tool	http://peid.has.it
UserDB.TXT	PEiD signature database	http://www.peid.info/BobSoft/Downloads/UserDB.zip
	Online library of unpacking tutorials	http://www.tuts4you.com
LordPE	Process and dynamic link library (DLL) dumping tool	http://www.woodmann.com/collaborative/tools/index.php/LordPE
Procdump	Process and DLL dumping tool	http://www.fortunecity.com/millenium/firemansam/962/html/procdump.html
mkepe	PE fix-up tool	ftp://ftp.sac.sk/pub/sac/utilprog/mkpe130.zip
TOOLS FOR PE FILES		
Explorer Suite	Integrated development environment (IDE) for PE tool view and edit	http://ntcore.com/exsuite.php
Stud_PE	Inspect PE file headers	http://www.cgsoftlabs.ro/studpe.html
SADD	Section-adding tool	http://programmerstools.org/system/files?file=sadd1.0.zip
StripReloc	Strip relocations from PE files	http://www.jrsoftware.org/striprlc.php
PE Checksum	Update PE checksum values	http://www.codeproject.com/KB/cpp/PEChecksum.aspx
petools	Patch PE files and add new imports	http://comrade.ownz.com/projects/petools.html
Pefile	Library in Python to manipulate PEs	http://code.google.com/p/pefile/
Pelib	Library in C to manipulate PEs	http://www.pelib.com/download.php

NAME	DESCRIPTION	LOCATION
TOOL DEVELOPMENT		
Visual Studio C++ Express	Microsoft C/++ compiler IDE	http://www.microsoft.com/express/Downloads/#2008-Visual-CPP
WDK	Windows Driver Kit	http://www.microsoft.com/whdc/DevTools/WDK/WDKpkg.mspx
Netfilter	Transport driver interface (TDI) packet inspection framework	http://netfiltersdk.com
native-nt-toolkit	Header files for native API functions	http://code.google.com/p/native-nt-toolkit/
Nasm	Netwide assembler	http://nasm.sourceforge.net
Masm32	Microsoft assembler	http://www.masm32.com/masmdl.htm
kmdkit	Kernel mode driver development kit (DDK) for masm	http://www.freewebs.com/four-f/KmdKit/KmdKit.zip
Wine source code	Wine source code	http://www.codeweavers.com/support/docs/wine-user/getting-wine-source
Python	Python language	http://www.python.org
Perl	Perl for Windows	http://www.activestate.com/activeperl/
MinGW	GNU Compiler Collection (GCC) for Windows	http://www.mingw.org
PyScripter	Python IDE	http://www.mmm-experts.com/Products.aspx?ProductId=4
Pywin32	Python library for accessing Win32 functions	http://sourceforge.net/projects/pywin32/
py2exe	Convert Python to executable (EXE) files	http://www.py2exe.org
OpenSSL	Cryptography library in C	http://www.openssl.org
Yara	Malware classification library in Python	http://code.google.com/p/yara-project/
PyCrypto	Cryptography library in Python	http://www.dlitz.net/software/pycrypto/
PROXIES		
Paros	Proxy for HTTP and secure socket layer (SSL) traffic	http://www.parosproxy.org/download.shtml
Burp suite	Proxy with fuzzer tools	http://portswigger.net/suite/
COM TOOLS		
oleretools	Perl scripts for COM reversing	http://www.joestewart.org/tools/oleretools.zip
Frank Boldewin's tools	IDA Python scripts for COM reversing	http://www.reconstructer.org/code.html
Comtypes	COM in Python	http://sourceforge.net/projects/comtypes

NAME	DESCRIPTION	LOCATION
DEBUGGERS AND PLUG-INS		
Olly debugger	User mode debugger	http://www.ollydbg.de
PhantOm	Hide debugger plug-in for Olly	http://www.woodmann.com/collaborative/tools/index.php/PhantOm
OllyBonE	Break on execute plug-in for Olly	http://www.woodmann.com/collaborative/tools/index.php/OllyBonE
PE Dumper	Process and DLL dump plug-in for Olly	http://www.woodmann.com/collaborative/tools/index.php/PE_Dumper
OllyScript	Scripting language for Olly	https://sourceforge.net/project/showfiles.php?group_id=195914
Immunity debugger	Olly + Python API + Immunity	http://www.immunitysec.com/products-immdbg.shtml
OllyDbg plug-ins for ImmDbg	OllyDbg plug-ins for ImmDbg	http://www.tuts4you.com/download.php?list.74
Windbg	Debugging tools for Windows (included in Windows DDK)	http://www.microsoft.com/whdc/DevTools/Debugging/default.mspx
PowerDbg	Scriptable plug-ins for WinDbg	http://www.codeplex.com/powerdbg
Livekd	Local kernel mode debugger (included in Sysinternals Suite)	http://technet.microsoft.com/en-us/sysinternals/bb897415.aspx
WinAppDbg	Program instrumentation in Python	http://apps.sourceforge.net/trac/winappdbg/
API HOOKING		
Rohitab API Monitor	Log API calls and parameters	http://www.rohitab.com/apimonitor/index.html
Sysanalyzer	iDefense Malcode Analyst Pack	http://labs.idefense.com/software/malcode.php#more_sysanalyzer
Madshi	API hooking library (commercial)	http://forum.madshi.net
Mhook	API hooking library in C	http://codefromthe70s.org/mhook22.aspx
Detours	Microsoft's API-hooking library	http://research.microsoft.com/sn/detours
EasyHook	Library for API hooking (kernel support)	http://www.codeplex.com/easyhook
CaptureBat	Honeynet project API monitor	https://www.honeynet.org/node/315
MEMORY ANALYSIS		
win32dd	Dump physical memory	http://win32dd.msuiche.net
pmdump	Dump individual process memory	http://www.ntsecurity.nu/toolbox/pmdump/
F-Response	Remote read-only drive access	http://www.f-response.com

NAME	DESCRIPTION	LOCATION
HBGary Fastdump	Dump physical memory fast	http://www.hbgary.com/products-services/fastdump-pro/
HBGary Flypaper	Block memory-free functions	https://www.hbgary.com/products-services/flypaper/
Volatility	Memory forensics framework in Python	https://www.volatilesystems.com/default/volatility
Volatility plug-ins	Volatility plug-ins	http://www.forensicswiki.org/wiki/List_of_Volatility_Plugins
HBGary Responder	Memory forensics platform for Windows	http://www.hbgary.com/responder_pro.html
Memoyze	Memory forensics platform for Windows	http://www.mandiant.com/software/memoryze.htm
PTFinder	Memory forensic tools in Perl	http://computer.forensikblog.de/en/2007/11/ptfinder_0_3_05.html
Sandman	C library to analyze hibernation files	http://sandman.msuiche.net/index.php
ONLINE SERVICES		
VirusTotal	Online virus scanner	http://www.virustotal.com
CWSandbox	Online behavior monitor	http://www.cwsandbox.org
Team Cymru ASN	Internet Protocol (IP) to Autonomous System Number (ASN) lookup tool	http://asn.cymru.com
JoeBox	Online behavior monitor	http://www.joebox.org
MalwareDomainList	Tracking exploits site	http://www.malwaredomainlist.com
Anubis	Online behavior monitor	http://anubis.iseclab.org
Threat Expert	Online behavior monitor	http://www.threatexpert.com
Jsunpack	Unpack JavaScript	http://jsunpack.jeek.org/dec/go
Wepawet	Analyze PDF and Shockwave Flash (SWF) files online	http://wepawet.iseclab.org/index.php
ROOTKIT AND MALWARE SCANNERS		
GMER	Multifunction rootkit scanner	http://www.gmer.net
IceSword	Multifunction rootkit scanner	http://www.antirootkit.com/software/IceSword.htm
Rootkit Revealer	Cross-view rootkit detector	http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx
Rootkit Unhooker	Multifunction rootkit scanner	https://www.rootkit.com/newsread.php?newsid=902
Malware Bytes	Malware scanner	http://www.malwarebytes.org
HijackThis	Malware scanner	http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis
BOOTABLE OS		
Plain Sight	Live forensics	http://www.plainsight.info

NAME	DESCRIPTION	LOCATION
BartPE	Bootable Windows XP/2003	http://www.nu2.nu/pebuilder
Helix3	Live forensics (commercial)	http://www.e-fense.com/products.php
CAINE	Live forensics (free)	http://www.caine-live.net/index.html
Knoppix	Live Linux environment	http://www.knoppix.net
FORENSIC TOOLS		
RegRipper	Forensic registry parser	http://www.regripper.net
Windows Registry Recovery	Graphic user interface (GUI) for browsing hive files	http://www.mitec.cz/wrr.html
Index Analyzer	IE history file viewer	http://www.systenance.com/indexdat.php
Scalpel	File-carving utility	http://www.digitalforensicssolutions.com/Scalpel/
Jafat LNK Parser	Windows shortcut and .lnk file parser	http://jafat.sourceforge.net/files.html
Forensic Acquisition Utilities (FAU)	Forensic acquisition utilities	http://www.gmgsystemsinc.com/fau
FTK Imager (Lite)	Capture disk and random access memory (RAM)	http://www.accessdata.com/downloads.html
Live View	Create vmdk from dd disc copies	http://liveview.sourceforge.net
Fatkit	Forensic analysis toolkit	http://www.4tphi.net/fatkit/
FTimes	Baseline and evidence collection	http://ftimes.sourceforge.net/FTimes/index.shtml
AIDE	Advanced intrusion detection environment	http://www.cs.tut.fi/~rammer/aide.html
FoxAnalysis	Firefox history analyzer	http://forensic-software.co.uk/foxanalysis.aspx
Pasco	index.dat parsing tool	http://odessa.sourceforge.net
R-Studio	File recovery software (commercial)	http://www.data-recovery-software.net
Mount Image Pro	Mount forensic images (commercial)	http://www.mountimage.com/?file=MIP-Setup.exe
ssdeep	Fuzzy hashing utility	http://ssdeep.sourceforge.net/usage.html
DBAN	Forensic disk-wiping CD	http://www.dban.org
sqlitebrowser	Sqlite3 GUI database browser	http://sqlitebrowser.sourceforge.net
REPORT GENERATION		
Snippy	Tiny screen capture program	http://www.bhelpuri.net/Snippy/SnippyDownload.htm
Camtasia Studio	Screen-recording suite	http://www.techsmith.com/camtasia.asp
Snapz Pro	Screen shot and recording for OS X (commercial)	http://www.ambrosiasw.com/utilities/snapzprox/
Graphviz	Graph visualization software	http://www.graphviz.org

NAME	DESCRIPTION	LOCATION
MISCELLANEOUS TOOLS		
HashCalc	Compute hashes in various algorithms	http://www.slavasoft.com/hashcalc
RemoteDll	Inject DLLs into processes	http://securityxploded.com/remotedll.php
Shellcode 2 Exe	Create EXE wrappers for shell code	http://sandsprite.com/shellcode_2_exe.php
Notepad++	Source code editor	http://notepad-plus.sourceforge.net/uk/site.htm
VB Decompiler	VB Decompiler	http://www.vb-decompiler.org
IrpTracker	Observe IOCTLs sent to device drivers	http://www.osronline.com/article.cfm?id=199
OpenVPN	SSL virtual private network (VPN) software	http://openvpn.net/index.php/open-source/downloads.html
Tor	Anonymity online	http://www.torproject.org
winexe	Exec commands on Win from Linux	http://eol.ovh.org/winexe/
Regshot	Detect changes to the registry and file system	https://sourceforge.net/projects/regshot
Win32kdiag	Detect hidden mountpoints	http://forums.majorgeeks.com/showthread.php?t=198257
Metasploit	Exploit and shellcode builder	http://www.metasploit.com
s2b	Shellcode-to-binary converter	http://www.honeynor.no/tools/s2b.py
7zip	Manipulate archives on Windows	http://www.7-zip.org
Bintext	Extract strings from binaries	http://www.foundstone.com/us/resources/proddesc/bintext.htm
Winhex	Hex viewer	http://www.x-ways.net/winhex.zip
Secunia PSI	Up-to-date software scanner	http://secunia.com/vulnerability_scanning/personal/
Cygwin	Linux environment for Windows	http://www.cygwin.com
eEye BDS	Binary-diffing suite	http://research.eeye.com/html/tools/RT20060801-1.html
DOCUMENTATION AND INFORMATION		
Woodman RCE Forums	Reverse engineering forums	http://www.woodmann.com
Offensive Computing	Malware information	http://www.offensivecomputing.net
OpenRCE	Reverse engineering information	https://www.openrce.org