ADIA - The Appliance for Digital Investigation and Analysis - Fedora 17 Version

Introduction

This DVD contains the files that constitute a virtual machine image for ADIA, the Appliance for Digital Investigation and Analysis. These virtual machines are based on Fedora 17.

This version of ADIA supports both VMware and Virtual Box. This version also support both the i386 (32 bit) and x86_64 (64 bit) host computer system architectures.

These versions will be the only release of ADIA for Fedora 17. You should routinely update ADIA to keep it current with package released by Red Hat (http://fedoraproject.org/) and packages released by CERT.

Installed Forensic Tools

This appliance contains the following tools as originally distributed:

Tool	Version	Description
2hash	0.2	Simultaneously perform an MD5 and SHA1 checksum on files
afflib	3.7.1	Library to support the Advanced Forensic Format
afftools	3.7.1	Utilities for afflib
aimage	3.2.5	Advanced Disk Imager
analysis-pipeline	3.0.0	Analysis Pipeline: automate common tasks when processing SiLK flow records
antiword	0.37	MS Word to ASCII/Postscript converter
ataraw	0.2.1	Linux user-level ATA raw command utility
autopsy	2.24	Autopsy Forensic Browser
bless	0.6.0	High quality, full featured hex editor
bless-doc	0.6.0	Bless user manual
bloom	1.4.6	NPS Bloom filter package (includes frag_find)
bulk_extractor	1.3.1	bulk_extractor is a C++ program that scans a disk image, a file, or a directory of files and extracts useful information
bulk_extractor-stoplist	1	Context stop list for bulk_extractor
catdoc	0.94.2	A program which converts Microsoft office files to plain text
cryptcat	1.2.1	Netcat with encryption
dc3dd	7.1.614	Patched version of GNU dd for use in computer forensics
dcfldd	1.3.4.1	Improved dd, useful for forensics and security
ddrescue	1.16	Data recovery tool trying hard to rescue data in case of read errors
dd_rescue	1.33	Fault tolerant "dd" utility for rescuing data from bad media
dff	1.3.0	dff - open source digital investigation framework
disktype	9	Detect the content format of a disk or disk image

Tool	Version	Description
distorm3	3	distorm3 - binary stream disassembler library
djvulibre	3.5.24	DjVu viewers, encoders, and utilities
DropboxReader	1	DropboxReader
eindeutig	20050628_1	Parse Outlook Express DBX files
epub	0.5.0	Extract thumbnails and associated metadata from the Thumbs.db files
etherape	0.9.12	Graphical network monitor for Unix
exfat-utils	1.0.1	Utilities for exFAT file system
ext3grep	0.10.2	Recovery tool for ext3 filesystems
fatback	1.3	Undelete files from FAT file systems
file	5.11	A utility for determining file types
fmem-kernel-objects	1.6	This package contains all of the kernel objects for all of the kernels for the currently supported versions of Fedora in the CERT Linux Repository.
foremost	1.5.7	Recover files by "carving" them from a raw disk
frag_find	1.0.0	NPS Bloom Filter Package
fred	0.1.0beta4	Microsoft registry hive editor
fundl	2	A File UNDeLetion program built on top of the Sleuthkit
fuse-exfat	1.0.1	Free exFAT file system implementation
galleta	20040505_1	Examine the contents of cookie files
GeoIP	1.4.8	C library for country/city/organization to IP address or hostname mapping
ghex	3.4.1	Binary editor for GNOME
ghostpdl	9.07	Artifex Software's implementation of the PCL-5 and PCL-XL family of page description languages
gpart	0.1h	A program for recovering corrupt partition tables
gparted	0.14.1	Gnome Partition Editor
grokevt	0.5.0	Read and process Windows Event Files
guymager	0.7.1	Imager for forensic media acquisition
hachoir-core	1.3.4	Library for carving binary files
hachoir-metadata	1.3.3	Extracts metadata from multimedia files
hachoir-parser	1.3.5	File format parser fo hachoir suite
hachoir-regex	1.0.5	A Python library for regular expression (regex or regexp) manupulation
hachoir-subfile	0.5.3	A tool based on hachoir-parser to find subfiles in any binary stream
hachoir-urwid	1.1	A binary file explorer based on Hachoir library to parse the files
hachoir-wx	0.3.1	A wxWidgets-based program that provides a user-friendly interface to hachoir-parser
hivex	1.3.5	Read and write Windows Registry binary hive files
ImageMagick	6.7.5.6	An X application for displaying and manipulating images
jafat	1.1.6	JAFAT is an assortment of tools to assist in the forensic investigation of computer systems.
KHracker	0.3	Known Hosts Entry Decrypter
libbfio	20110625	Library to support (abstracted) basic file IO
libewf	20130128	Library to support the Expert Witness Compression Format (EWF)
libguytools	2.0.2	A small programming toolbox

Tool	Version	Description
libpcap	1.2.1	A system-independent interface for user-level packet capture
libpff	20120802	libpff - Library to access the PFF and the OFF format
libpst	0.6.58	Utilities to convert Outlook .pst files to other formats
libvshadow-tools	20130501	Several tools for reading Windows NT Volume Shadow Snapshots (VSS)
libwpd-tools	0.9.7	Tools to transform WordPerfect Documents into other formats
libxslt	1.1.26	Library providing the Gnome XSLT engine
log2timeline	0.65	A framework for timeline creation and analysis
mac-robber	1.02	Tool to create a timeline of file activity for mounted file systems
md5deep	4.3	Programs to compute MD5, SHA-1, or SHA-256 message digests on files
mdbtools	0.6	Access data stored in Microsoft Access databases
missidentify	1	Find Win32 applications
mount_ewf	20090113	mount files in Expert Witness Format using loopback file system
nDPI	1.4.0	Open source deep packet inspection
nmap	6.01	Network exploration tool and security scanner
nmap-frontend	6.01	The GTK+ front end for nmap
partclone	0.2.48	File System Clone Utilities
parted	3	The GNU disk partition manipulation program
perl-Image-ExifTool	9.27	Utility for reading and writing image meta info
perl-Mac-PropertyList	1.33	Work with Mac plists at a low level
perl-NetPacket	1.3.1	Assemble/disassemble network packets at the protocol level
perl-Net-Pcap	0.17	Interface to pcap(3) LBL packet capture library
perl-Parse-Evtx	1.1.1	Windows Event Log Parser library and tools collection
perl-Parse-Win32Registry	0.51	Parse Windows Registry Files
poppler-utils	0.18.4	Command line utilities for converting PDF files
prism	1.2	Visualize flow data as a time-series broken down into several configurable bins
pstotext	1.9	PostScript to text converter
ptfinder	0.3.05	Find processes and threads in a Windows memory dump
ptk	1.0.5	An alternative advanced interface for the suite TSK (The SleuthKit)
python-netaddr	0.7.5	A pure Python network address representation and manipulation library
python-registry	0.2.3	Read access to Windows Registry Files
pytsk	20121113	pytsk - Python binding for The Sleuth Kit
rayon	1.3.3	Python library and set of tools for generating basic two-dimensional statistical visualizations
recode	3.6	Conversion between character sets and surfaces
recoll	1.18.1	Desktop full text search tool with Qt GUI
registrydecoder	20120816	registrydecoder - automates acquisition, analysis, and reporting of Microsoft Windows registry contents.
reglookup	1.0.1	Windows NT registry reader/lookup tool
regripper	28000000	A Windows Registry data extraction and correlation tool
regripper-plugins	20130429	Plugins for regripper

Tool	Version	Description
rifiuti	20040505_1	Examine the contents of INFO2 in the Windows Recycle bin
rifiuti2	0.5.1	Examine the contents of INFO2 in the Windows Recycle bin
safecopy	1.7	Safe copying of files and partitions
scalpel	2	Fast file carver working on disk images
scrounge-ntfs	0.9	Data recovery program for NTFS file systems
sfdumper	2.2	A Selective File Dumper program built on top of the Sleuthkit
shellbags	0.5.1	Cross-platform shellbag parser
silk-analysis	2.5.0	SiLK Toolset: The Analysis Suite
silk-common	2.5.0	SiLK Toolset: Common Libraries and Configuration Files
silk-devel	2.5.0	The SiLK Toolset development files
silk-flowcap	2.5.0	SiLK Toolset: Remote Flow Collection
silk-rwflowappend	2.5.0	SiLK Toolset: Remote Data Storage Appending Daemon
silk-rwflowpack	2.5.0	SiLK Toolset: The Packer
silk-rwpollexec	2.5.0	SiLK Toolset: Batch Command Executor
silk-rwreceiver	2.5.0	SiLK Toolset: File Transfer Receiver
silk-rwsender	2.5.0	SiLK Toolset: File Transfer Sender
sleuthkit	4.0.2	The Sleuth Kit (TSK)
snort	2.9.4.6	An open source Network Intrusion Detection System (NIDS)
snort-sample-rules	2.9.4.6	Sample rules for snort
socat	1.7.2.1	Bidirectional data relay between two data channels ('netcat++')
sox	14.3.2	A general purpose sound file conversion tool
splunk	4.0.11	Splunk
ssdeep	2.9	Computes a checksum based on context triggered piecewise hashes
ssldump	0.9	An SSLv3/TLS network protocol analyzer
stegdetect	0.6	Detect and extract steganography messages inside JPEG
tcpflow	1.3.0	Network traffic recorder
tcpxtract	1.0.1	Tool for extracting files from network traffic
testdisk	6.13	Tool to check and undelete partition, PhotoRec recovers lost files
tln_tools	20110729	Timeline tools - Open Source code for Windows Forensic Analysis and Incident Response
unrar	4.1.4	Utility for extracting, testing and viewing RAR archives
unrtf	0.21.1	RTF (Rich Text Format) to other formats converter
untex	1.3	Command to strip LaTeX commands from input
unzip	6	A utility for unpacking zip files
videosnarf	0.63	Output detected media sessions
vinetto	0.07beta	Extract thumbnails and associated metadata from the Thumbs.db files
Volatility	2.2	Tools for the extraction of digital artifacts from volatile memory (RAM) images
wireshark	1.6.14	Network traffic analyzer
wireshark-gnome	1.6.14	Gnome desktop integration for wireshark
xmount	0.5.0	A on-the-fly convert for multiple hard disk image types
xplico	1.0.1	Internet traffic decoder and network forensic analysis tool

Tool	Version	Description
yaf	2.4.0	Yet Another Flow sensor
yara-python	1.7	yara-python - Python extension that gives access to YARA from Python scripts

Most of these tools operate from the command line and as such, the default login contains a Terminal icon in the panel located at the bottom of the screen. Launch a Terminal by double clicking on that icon.

Installation

VMware

ADIA has been tested and works on VMware Workstation 9.0.2 under Windows 7 Professional and VMware Fusion 5.0.3 under Mac OS X 10.7.4 and 10.8.3. We expect that it will work in other configurations but they remain untested. When the virtual machine was packaged for distribution, it was converted to work with VMware Workstation 5 and later.

To install ADIA under VMware, do the following:

1. Start VMware
2. Select *File→Open*
3. Navigate to the opened ISO image
4. Select the OVA file image
5. Import the virtual machine
6. Once imported, select *VM→Settings*
7. Select the *Options* tab
8. Enable Shared Folders
9. Share a folder with the name *Forensics*
    a. (typically with the host path *C:\Forensics*, but any folder will do)
10. Optionally update the hardware version of the newly created virtual machine
11. Start the virtual machine
12. The virtual machine will boot and should automatically login as examiner (with password `forensics`)

Installing ADIA under VMware requires about 7Gb of disk space.

Virtual Box

ADIA has been tested and works on Virtual Box 4.2.12 under Windows 7 Professional and Mac OS X 10.7.4 and 10.8.3. We expect that it will work in other configurations but they remain untested. Note: you will need to also have the Virtual Box Extension Pack installed to run ADIA.

To install ADIA under Virtual Box, do the following:

1. Start Virtual Box
2. Select *File→Import Appliance...*
3. Select **Import Appliance**
4. Navigate to the opened ISO image
5. Select the OVA file image
6. Select **Next**
7. Select **Import**
8. When the virtual machine has been imported, double click on it to boot it
9. The virtual machine will been and should automatically login as examiner (with password `forensics`)

Installing ADIA under Virtual Box requires about 7Gb of disk space.

Network Assumptions - DHCP

ADIA assumes that it is connected to a network that provides configuration information through DHCP. Whether that connection is NATed or bridged is a configuration choice, but as long as DHCP service is provided, the appliance will use it to configure its network connection. You can reconfigure ADIA to use a static address through the Network Manager icon on the desktop. See http://projects.gnome.org/NetworkManager/ for more information.

Network Assumptions - Proxy Server

This appliance also assumes that it is directly connected to the Internet without a proxy server. If that does not match the configuration of your network, then you must configure a proxy server as needed.

For example, if you use a browser, you will need to configure your network's proxy server into that browser. If you wish to load or update the packages installed on this appliance, you will need to configure your network's proxy server in */etc/yum.conf*. Other applications will also need to be configured to use your network's proxy server so consult your organization's documentation to determine how to do this.

Sharing Files with the Host Computer System

ADIA is configured to use file systems shared to it by the host. There is an icon on the **examiner** login desktop named *Shared Folders* that when double clicked starts a file browser that initially contains the names of all of the directories shared to it.

To share folders from the host to this appliance, consult the documentation for your version of VMware or Virtual Box.

By default, ADIA assumes that there is a share named Forensics (typically the folder *C:\Forensics*) that is shared from the host. Further, if you intend to use the **Autopsy** tool, create a directory named *morgue* in this shared folder.

Default Login Session

As distributed, this appliance automatically logs into the examiner account when it is booted. However, should the screen lock or in some other way prompt for the examiner password, it is the string `forensics`. The password for the root account is also `forensics`.

The Gnome Window system is used for the examiner login. The use of other window systems is untested and may result in unexpected results.

Routine Maintenance

It is recommended that you routinely update packages using:

```
sudo yum update
```

This will update all packages except the kernel-based packages. To update them where possible, use the following:

```
sudo yum update --disableexcludes=all
```

Note that if you update the kernel for Virtual Box, you will also need to install the Guest Additions and then reboot. See this web page for the procedure to do that:

http://www.virtualbox.org/manual/ch04.html

From time to time, the packages used to build the examiner login account will be updated, most often when new tool documents are distributed. To update the examiner login with these new files, do the following:

```
        sudo manage-examiner-login -S -v
```

This will update the examiner login and retain any conflicts as described in the manage-examiner-login man page.

Miscellaneous Comments

1. The packages for all installed applications reside on a repository located at CERT at http://www.cert.org/forensics/repository.
2. Automatically mounting file systems such as those on an external USB device is enabled but file systems are mounted read-only by default. If you need read-write access to an external file system, you will need to remount it using the mount command and a terminal window.

Updates and New Versions of this Appliance

For updates and new versions of this appliance, visit the http://www.cert.org/forensics/repository/#ADIA web site.

Questions and Bug Reports

Send mail to forensics-linux-repository@cert.org with any questions and bug reports that you may have. We will answer questions as we are able.

SHA256 File Checksums

Here are the checksums for the four ISO Fedora 17-based ADIA images:

ADIA Version	Virtualization Application	Checksum
ADIA-FC17-i386	VMware	346d55192c4e2576746734e249ff7ee3ff05c2b988e75601d8cca4549211ee5a
ADIA-FC17-x86_64	VMware	f630f39efa52f4fa322551815fb25e9ba729952b5d3c73faf646bda3a9d41466
ADIA-FC17-i386	Virtual Box	4a10f30d8f654a7982499202951b47e41e5c4fa5c57fd18bf5c68b38d23c9685
ADIA-FC17-x86_64	Virtual Box	483818ec3399250ce46265f79f4b2a853fa264929dbcad78d693e61b7ff30c8e

May, 2013