Installing and Operating the CERT Forensic Appliance
DRAFT

February 2011
CERT® Program
Guided Tour

The CERT Forensic Appliance

Overview: This guided tour shows how to download, start, and operate the CERT Forensic Appliance, hereafter referred to as the “appliance”. It is assumed that one or more of VMware Player, VMware Workstation, or VMware Fusion have been installed on the host computer where the appliance will run. The screen captures shown here have been taken from the CERT Forensics Appliance running under:

- VMware Fusion 3.1.2 under Mac OS X 10.6.6,
- VMware Workstation 7.1.3 under Windows 7 Professional, and
- VMware Workstation 7.1.3 under Fedora 14.

It is assumed that users of the appliance will have some knowledge of Linux, the shell, and running program and commands.

Tasks Shown in this Guided Tour

Task 1 – Download, Install, and Start the Appliance .................................................................1
Task 2 – Configure and Add Shared Folders to the Appliance ....................................................10
Task 3 – Get Help ..........................................................................................................................15
Task 4 – Update the Appliance and Install Additional Packages ................................................18
Task 5 – Attach An External Disk to the Appliance ...................................................................22

Figures Shown in this Guided Tour

Figure 1 - Appliance on CERT Forensics Repository Web Page..................................................1
Figure 2 - Check ISO Image Signature – Fedora ............................................................................1
Figure 3 - Appliance ISO Image as Mounted – Mac OS .................................................................2
Figure 4 - Appliance ISO Image as Mounted – Windows ..............................................................2
Figure 5 - Appliance ISO Image as Mounted – Fedora .................................................................2
Figure 6 - Verify ISO Image Contents – Fedora .............................................................................3
Figure 7 - Verify Checksums in ZIP Archive in ISO Image – Fedora .............................................4
Figure 8 - VMware Moved or Copied Window – Mac OS .............................................................4
Figure 9 - VMware Moved or Copied Window – Windows ............................................................4
Figure 10 - VMware Moved or Copied Window – Fedora ............................................................5
Figure 11 - Appliance Login Window – Mac OS ..........................................................................5
Figure 12 - Appliance – Automatic Login Window .....................................................................6
Figure 13 - Appliance Booted – Mac OS .......................................................................................6
Figure 14 - Appliance with Dockbarx Applet – MacOS ...............................................................7
Figure 15 - VMware Fusion Shared Folder Settings Window – Mac OS ..........................................10
Figure 16 - VMware Fusion Shared Folder Settings Window as Configured – Mac OS ................10
Figure 17 - Shared Folders ............................................................................................................11
Figure 18 - VMware Workstation Shared Folder Settings Window – Windows ............................11
Figure 19 - VMware Workstation Shared Folder Settings Window as Configured – Windows ....12
Figure 20 - Shared Folders ...........................................................................................................12
Figure 21 - VMware Workstation Shared Folder Settings Window – Fedora ..............................13
Figure 22 - VMware Workstation Shared Folder Settings Window as Configured – Fedora .......13
Figure 23 - Shared Folders ...........................................................................................................14
Figure 24 - Main Pages Main Page ................................................................................................15
Figure 25 - Tool Documentation Folder.......................................................................................16
Figure 26 - Man Page for Windows ➔ Registry ➔ reglookup ..........................................................17
Figure 27 - Software Updates Showing Applicable Updates ..........................................................18
Figure 28 - Add/Remove Software Main Window .........................................................................19
Figure 29 - Installing Additional Software – Results of hex editor Search ..................................19
Figure 30 - Installing Additional Software – Details of the Bless Package ....................................20
Figure 31 - Installing Additional Software – Files in the Bless Package .......................................20
Figure 32 - Installing Additional Software – Dependencies Window ..........................................21
Figure 33 - Installing Additional Software – Authenticate Window ............................................21
Figure 34 - Run Newly Installed Application ..............................................................................21
Figure 35 - VMware Fusion External Disk Connection Window ....................................................22
Figure 36 - External Disk Contents Window ................................................................................22
Figure 37 - External Disk Mounted Read-Only ............................................................................23
Figure 38 - VMware Workstation USB Warning Message Window .............................................23
Task 1 – Download, Install, and Start the Appliance

The first task is to retrieve the latest version of the appliance from the CERT Forensics Repository, [http://www.cert.org/forensics/repository](http://www.cert.org/forensics/repository). You will need approximately 10Gb of local disk storage for the image. See Figure 1 for the portion of this web page where the appliance can be found.

Note: while several versions of the appliance are available, this document describes the latest that is based on Fedora 14. Note also that the checksums shown here are examples; those on the website are the values which should be used to determine the veracity of a downloaded image.

![Figure 1 – The Appliance on CERT Forensics Repository Web Page](image)

1. Visit the [http://www.cert.org/forensics/repository](http://www.cert.org/forensics/repository) web page using your browser and download the version of the appliance that you require. This file is formatted as an ISO image, a zip file, or a zip of an ISO image.

2. We recommend that you also download the associated GPG signature file so that you can verify that the image download was successful. Figure 2 shows this procedure on a Fedora system. It is assumed that both the downloaded image and the related signature file have been downloaded to the 

   ![Figure 2 - Check ISO Image Signature - Fedora](image)

Note also the use of the MD5 checksum as posted on the web page.

---

3. To check the MD5 or SHA1 checksums in the README.txt file on a Mac OS X system, you can install Mac Ports (see [http://guide.macports.org/](http://guide.macports.org/)) for more information), install the coreutils package, and then use the command `gmd5sum` and `gsha1sum` instead of `md5sum` and `sha1sum` respectively.
3. Once you’ve downloaded the ISO image of the appliance, burn it to a DVD or mount it. Figure 3 shows the image mounted on a Mac OS X system (achieved by double clicking on the ISO image file), Figure 4 under Windows (mounted using the PowerISO utility\(^2\)), and Figure 5 under Fedora (through nautilus, the file and Internet browser).

4. Use the README.txt.asc file along with the CERT Forensics PGP Key, available at http://www.cert.org/forensics/tools/forensics.asc, to verify the README.txt file. This file also contains the MD5 and SHA1 checksums for all of the files in the ISO image. Figure 6 shows how to do this on a Fedora system\(^3\). Note that the files that comprise the zip archive are not available to be checked at this point.

![Figure 6 - Verify ISO Image Contents – Fedora](image)

5. Next, unzip the appliance to the folder where your version of VMware normally installs client images. Again, you can use the contents of the README.txt file to verify the unzipped files. Those places are:
   a. Mac OS - $HOME/Documents/Virtual Machines.localized
   b. Windows - %HOMEPATH%\Documents\Virtual Machines
   c. Fedora - $HOME/vmware

\(^3\) To check the MD5 or SHA1 checksums in the README.txt file on a Mac OS X system, you can install MacPorts (see http://guide.macports.org/ for more information), install the coreutils package, and then use the command `gmd5sum` and `gsha1sum` instead of `md5sum` and `sha1sum`. Under a Windows system, one solution is to use the CYGWIN package (see http://www.cygwin.com/ for more information) and then follow the example shown here.
6. Go to that folder and check the checksums of those files. See Figure 7. Again, notice that some of the files are again missing which cause errors to be produced.

```
[llr@nauer ~]$ ls -l SHONE/vmware
.
[llr@nauer vmware]$ dos2unix /tmp/appliance/README.txt | md5sum -c - 2> /dev/null
autorun.bat: FAILED open or read
FC14-foren-2011-01-i386.zip: FAILED open or read
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s083.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s082.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s083.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s084.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s085.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s086.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s087.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s088.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s089.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s090.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s091.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s092.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s093.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s094.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s095.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s096.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s097.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s098.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s099.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s100.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s101.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s102.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s103.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s104.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s105.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s106.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s107.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s108.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s109.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s110.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s111.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s112.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s113.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s114.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s115.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s116.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s117.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s118.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s119.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s120.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s121.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s122.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s123.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s124.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s125.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s126.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s127.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s128.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s129.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s130.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-s131.vmdk: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-vmutil: OK
FC14-foren-2011-01-i386/FC14-foren-2011-01-i386-vmware.log: OK
FC14-foren-2011-01-i386/vmware.log: OK

Figure 7 - Verify Checksums in ZIP Archive in ISO Image – Fedora

7. Since the veracity of the files in the appliance folder – FC14-foren-2011-01-i386 in this case – could be verified, it is safe to now start VMware Workstation (Windows or Fedora) or Fusion (Mac OS). Select the File ➔ Open menu option, browse to the folder where the appliance has been installed, and then double click on the file with the .vmx extension.

8. You may have to manually power on the appliance to start it.

9. Once the booting process starts, VMware presents a window similar to that shown in Figure 8 (Mac OS), Figure 9 (Windows), and Figure 10 (Fedora). Select the (Mac OS), (Windows), or (Fedora) button and then on Windows select the button to continue.
10. VMware may display a message about shared folders being disabled. They need to be re-enabled and configured as described in Task 2 – Configure and Add Shared Folders to the Appliance which begins on page 10.

11. When the appliance has completely booted, you should see a window similar to that shown in Figure 13 (Mac OS). Windows and Fedora are similar.
12. You can select the login and then select the button as shown in Figure 12 or you can wait until the automatic login period expires and the login process completes (about 10 seconds).

![Figure 12 - Appliance – Automatic Login Window](image)

13. Note: while the password is not needed for login, it will be needed if you lock the screen or if it locks automatically (this is the default). The password for the default examiner account is forensics. The password for the root account – the Linux equivalent of the Windows administrator account – is also forensics. This password is also documented on the background of the examiner’s login workspace.

14. Figure 13 shows the initial window in the booted appliance in Mac OS (Windows and Fedora are similar). Beginning with Fedora 14, the Appliance uses a Windows 7 theme. Note the Error window. Select the button in all of these windows that appear at login. We regret this error window and are working to rectify it.

![Figure 13 - Appliance Booted – Mac OS](image)
15. Figure 14 shows what the appliance should look like once booting and the automatic login process completes. The difference between Figure 13 and Figure 14 is that the Dockbarx applet has been added to the panel at the bottom of the window. The Dockbarx applet is an integral part of the Windows 7 look and feel of the appliance.

![Figure 14 - Appliance with Dockbarx Applet – MacOS](image)

16. Notice that there are two open windows. They are:

   a. A terminal window – this is the equivalent of the `cmd.exe` command prompt in Windows. It is located in the lower left of the appliance window.

   b. The Tool Documentation File Browser window – this is a file browser that contains references to the help files for the forensics tools installed in the appliance. It is located in the upper right of the appliance window.

---

4 To add the Dockbarx applet to the panel, right click in the panel at the bottom of the window, select the “Add to Panel…” menu item, and then select the Dockbarx Applet. Note that this applet, while helpful in mimicking the Windows 7 interface, seems to have some bug that produces the error message shown in Figure 13.
17. Also on the desktop are these icons. Double click on an icon to activate it.

- Launch a browser showing all of the mounted files systems in the appliance.
- Launch a browser that gives a brief explanation of the appliance.
- Launch a browser showing the home file system of the examiner that is the default account on the appliance.
- Launch a browser showing any shares on the network to which the appliance is connected.
- Launch a browser that is connected to the Autopsy web-based front end to The Sleuth Kit public domain forensic analysis tools.
- This icon should be edited to connect to an SMB-based file server available to the appliance.
- Open a folder listing the analysis tools presently installed. Example analysis tools are Autopsy and PTK.
- Open a folder listing the networking tools presently installed. Example networking tools are Wireshark and Xplico.
- Open a folder listing the system administration tools presently installed. Example system administration tools are Webmin and phpMyAdmin.
- Open a folder listing the indexing tools presently installed. Example indexing tools are Splunk.
- Open a folder listing the miscellaneous tools presently installed. Example miscellaneous tools are Adobe Reader and a Hex editor.
- Open a folder listing the documentation and help tools presently installed. Example documentation and help tools are the Tool Documentation folder opened by default on the desktop, the Forensics System Guide which is shown elsewhere on the desktop, and the system manual pages.
- Launch a file browser that shows the files moved to the trashcan.
18. Across the bottom of the appliance window are several more icons. Their means are the following:

- The standard main menu icon.
- Start a new terminal window.
- Starts the Firefox web browser.
- Locks the current session.
- Logs the examiner off of the appliance.
- Restarts or shuts down the appliance.
- This shows which of the four available desktops are currently displayed. By default the initial windows appear in the first workspace.
- The volume control icon.
- The network control icon.
- The current time and date.
- Minimizes all open windows. It is located at the lower right hand side of the screen.
Task 2 – Configure and Add Shared Folders to the Appliance

As mentioned previously, the appliance uses VMware’s shared folder mechanism to share files between the host and the appliance. Folders shared to the appliance are accessible in the /mnt/hgfs directory and by selecting the icon on the desktop.

By default, the appliance assumes that shared folders are enabled and that there is at least one share with the name Forensics. As mentioned previously, shared folders are disabled when the appliance is first installed. To re-enable and configure shared folders for the appliance, do one of the following, based on the host operating system. Note that this step can be performed with the appliance halted or running. If the appliance is running, changes in shared folders are immediately reflected in the appliance.

1. For Mac OS, follow these steps:
   a. Select Virtual Machine ➔ Shared Folders ➔ Open Shared Folder Settings… . This opens a window similar to that shown in Figure 15.

   ![Figure 15 - VMware Fusion Shared Folder Settings Window – Mac OS](image1)

   b. Check the Share folders on your Mac box.

   c. Select the button and add a folder. This opens a file browser which that you can use to navigate to and select the folders to be shared with the appliance. Folders can be anywhere on the system.

   d. Add as many shared folders as you need, but at last one of them should have the name Forensics that should be writable by you. Figure 16 shows one such folder added to the appliance.

   ![Figure 16 - VMware Fusion Shared Folder Settings Window as Configured – Mac OS](image2)
e. Once these settings are saved, all of the shares are mounted. By double clicking on the icon on the desktop, a browser window similar to that shown in Figure 17 opens.

![Figure 17 - Shared Folders](image)

f. Shared folders have now been enabled and configured for the appliance running under Mac OS.

2. For Windows, follow these steps:

a. Select VM → Settings… → Select the Options tab and then the Shared Folders line. This opens the window shown in Figure 18.

![Figure 18 - VMware Workstation Shared Folder Settings Window – Windows](image)

b. Select the **Always enabled** radio button in Figure 18.

c. Select the **Add...** button also in Figure 18 and add a folder. This opens a file browser which that you can use to navigate to and select the folders to be shared with the appliance. Folders can be anywhere on the system.
d. Add as many shared folders as you need, but at last one of them should have the name Forensics that should be writable by you. Select the button to continue. Figure 19 shows one such folder added to the appliance.

![Figure 19 - VMware Workstation Shared Folder Settings Window as Configured – Windows](image19)

e. Once these settings are saved, all of the shares are mounted. By double clicking on the icon on the desktop, a browser window similar to that shown in Figure 20 opens.

![Figure 20 - Shared Folders](image20)

f. Shared folders have now been enabled and configured for the appliance running under Windows.
3. For Fedora, follow these steps:
   a. Select VM→Settings. Select the Options tab and then the Shared Folders line. This opens the window shown in Figure 21.

![VMware Workstation Shared Folder Settings Window – Fedora](image1)

   Figure 21 - VMware Workstation Shared Folder Settings Window – Fedora

   b. Select the Always enabled radio button in Figure 22.

   c. Select the Add... button also in Figure 22 and add a folder. This opens a file browser which that you can use to navigate to and select the folders to be shared with the appliance. Folders can be anywhere on the system.

   d. Add as many shared folders as you need, but at last one of them should have the name Forensics that should be writable by you. Select the Save button to continue. Figure 22 shows one such folder added to the appliance.

![VMware Workstation Shared Folder Settings Window as Configured – Fedora](image2)

   Figure 22 - VMware Workstation Shared Folder Settings Window as Configured – Fedora
e. Once these settings are saved, all of the shares are mounted. By double clicking on the icon on the desktop, a browser window similar to that shown in Figure 23 opens.

![Figure 23 - Shared Folders](image)

f. Shared folders have now been enabled and configured for the appliance running under Fedora.
This completes the demonstration of enabling and configuring shared folders on the Appliance.
Task 3 – Get Help

Most programs installed on a Linux system in general and specifically the appliance are documented through manual pages, or man pages, for short. On most systems, the man program displays this documentation. You can use this program on most any Linux system that you encounter.

In addition, if you are not sure the name of a program, you can search by keyword. The way to do this from the command line is with the command:

```
man -k keyword
```

where `keyword` is the word you are using to narrow your search (e.g., compiler).

The man command run this way produces a list of man pages where the synopsis of that command contains that keyword.

On the appliance, an improved and web-based help system has been installed. It is available through two different interfaces that are described next.

1. On the desktop is the folder that contains the icon. If you first open the folder and then double click on this icon, a web browser is started that creates the web page shown in Figure 24.

   ![Man Pages Main Page](image)

   **Figure 24 - Man Pages Main Page**
You can search by keyword (the red arrow – this is the equivalent of `man –k keyword`), by name and description (the yellow arrow), by man page name (the green arrow), and finally by a full index search using all of the text in every man page (the blue arrow).

2. On the desktop in the `Documentation and Help` folder is the `Tool Documentation` icon. This folder browser is already open by default when the examiner logs into the appliance. This lists the tools that have special significance to the forensics examination process. Figure 25 shows high-level list of topics for which there are tools available for analysis. By navigating through this folder hierarchy, you can display the documentation provided for a specific tool.

In addition, if you know the name of the tool, but not how it may be classified, you can use the `000 By Name` folder that lists all tools in alphabetical order.

![Figure 25 - Tool Documentation Folder](image-url)
3. For example, Figure 26 shows the man page when you select `Windows → Registry → reglookup`.

```
reglookup
Section: User Commands (1)
Updated: File Conversion Utilities
Index Return to Main Contents

NAME
reglookup - windows nt+ registry reader/lookup tool

SYNOPSIS
reglookup [options] registry-file

DESCRIPTION
reglookup is designed to read windows registry elements and print them out to stdout in a CSV-like format. It has filtering options to narrow the focus of the output. This tool is designed to work with on windows NT/2K/XP/2K3 registries, though your mileage may vary.

OPTIONS
reglookup accepts the following parameters:
-p <prefix-filter>
   Specify a path prefix filter. Only keys/values under this registry path will be output.
-t <type-filter>
   Specify a type filter. Only elements which match this registry data type will be printed. Acceptable values are: NONE, SZ, EXPAND_SZ, BINARY, DWORD, DWORD_BE, LINK, MULTI_SZ, RSRC_LIST, RSRC_DESC, RSRC_REQ_LIST, QUADWORD and KEY
-h
   Enables the printing of a column header row. (default)
-H
   Disables the printing of a column header row.
-s
   Adds four additional columns to output containing information from key security descriptors. The columns are: owner, group, secl, dacl. (This feature's output probably contains bugs right now.)
-S
   Disables the printing of security descriptor information. (default)
-v
   Verbose output. (Currently does little to nothing.)
registry-file
   Required argument. Specifies the location of the registry file to read. Typically, these files will be found on a NTFS partition under %SystemRoot%\system32\config.
```

**Figure 26 - Man Page for Windows → Registry → reglookup**

This concludes the Get Help task.
Task 4 – Update the Appliance and Install Additional Packages

Keeping your copy of the appliance up to date is an important task that you should perform regularly. You may also find additional tools that help you to do the forensics analysis job and so you may want to install them in your copy of the appliance. This section describes how to do these tasks.

Note: This task requires Internet connectivity. If you do not have that connectivity, you cannot perform this task.

1. If you need to specify a proxy server to connect to the Internet, do the following:
   a. Start the System→Preferences→Network Proxy configuration tool.
   b. Select the required options, for example: http://proxy.foo.com:port.
   c. Select the Close button to save these preferences.

2. To update the appliance, start the System→Administration→Software Update application.

3. Once the software update application has been able to connect to the various repositories that contain updates, you will see the updates presently available to you. Figure 27 shows an example:

   ![Software Updates](image)

   **Figure 27 - Software Updates Showing Applicable Updates**

4. Note: the Appliance has been configured to update all packages except the kernel or any open-vm-tools packages. If you must update these packages, they must be updated together. To do this, use the following command in a terminal window:

   ```
   sudo yum update -disableexcludes=all
   ```
5. Deselect the updates that you do not want installed, and then select the "Install Updates" button to start the update. Certain updates may require that the system be rebooted. The software update application will advise you if this action is necessary.

6. To add a package, start the ➔ System ➔ Administration ➔ Add/Remove Software application. Figure 28 shows this application’s main window.

![Figure 28 - Add/Remove Software Main Window](image)

7. Imagine that you wanted to install the Bless Hex Editor to the system. Enter the term `bless` in the upper left input line and the click the `Find` button. Figure 29 shows the results of this search.

![Figure 29 - Installing Additional Software – Results of hex editor Search](image)
8. Double click on your choices. The panel at the bottom of Figure 30 displays the information about this package. In this case, the panel also displays a URL that points to the home page that describes the tool in more detail.

![Figure 30 - Installing Additional Software – Details of the Bless Package](image)

9. Select Selection ➔ Get File List to see the files that would be installed if this package were to be installed. Figure 31 shows this list.

![Figure 31 - Installing Additional Software – Files in the Bless Package](image)

10. The Selection menu shows other attributions of the package, including what other packages this package depend upon, if any (these will be installed if bless is installed), and what other packages depend on bless, if any.

11. To install the Bless Hex Editor, select it in the main window and then select the button.
12. The dependencies are computed and the window similar to that shown in Figure 32 appears. Select the Continue button to continue.

![Figure 32 - Installing Additional Software – Dependencies Window](image)

13. The application prompts you for the root password as shown in Figure 33. Supply it and select the button to continue. On the appliance, the root password is forensics.

![Figure 33 - Installing Additional Software – Authenticate Window](image)

14. Once the package is installed the application opens the window shown in Figure 34. You can now run your newly installed tool by selecting the Run button, or end the installation process by selecting the Close button.

![Figure 34 - Run Newly Installed Application](image)

15. End the Add/Remove Software application by selecting System → Quit.

This ends the Update and Install Software Task.
Task 5 – Attach An External Disk to the Appliance

The next task is to attach an external disk to the appliance. This is a common task when performing a forensic analysis.

By default, all external disks automatically mounted by the appliance are read-only. In addition, using write blockers or other write inhibiting technology is highly recommended.

This section explains how to add an external disk for Mac OS, Windows, and Fedora. For all systems, attaching an external disk formatted as NTFS and labeled LRR-001 is described. Note: Attach external disks only after the appliance has booted and the login process has completed.

1. If you are running VMware Fusion, do the following:
   a. Select the VMware application by clicking somewhere in the appliance.
   b. For some versions of VMware Fusion, you must first select Virtual Machine → USB → Connect The Vendor Name Of Your Disk. Note that if this drive is connected to some other virtual machine, it may have to be disconnected from that machine first. For other versions of VMware Fusion, when the disk is plugged into your host computer, a window will open asking where the disk is to be connected. See Figure 35.
   c. In either case, once the disk has been connected to the appliance, an icon similar to the
      icon is automatically created on the desktop and the window comparable to that shown in Figure 36 opens to show the drive’s contents.

![Figure 35 - VMware Fusion External Disk Connection Window](image)

![Figure 36 - External Disk Contents Window](image)
d. Use the open terminal window to verify that the mounted file system is read-only. See Figure 37.

![Terminal window showing file system permissions](image)

**Figure 37 - External Disk Mounted Read-Only**

e. To umount the disk:

   i. right click on the icon and select the menu item, then
   ii. select `Virtual Machine → USB → Disconnect The Vendor Name Of Your Disk` from the menu.

f. The drive will then be reconnected to the host. It can then be ejected by either:

   i. right clicking on the icon on the desktop and selecting from the menu, or
   ii. dragging the desktop icon to the Trash Can.

2. If you are running VMware Workstation – either Windows or Fedora – do the following:
   a. Select the VMware application by clicking somewhere in the appliance.
   b. Select `VM → Removable Devices → The Name Of Your Disk → Connect (Disconnect from host)`.
   c. If the warning shown in Figure 38 appears, select the button to continue.

![VMware Workstation USB Warning Message Window](image)

**Figure 38 - VMware Workstation USB Warning Message Window**

d. Once connected, the icon is automatically created on the desktop and the window shown in Figure 36 opens to show the drive’s contents.
e. The files on the external disk are now available at /media/The Name Of Your Disk from the command line or at the icon on the desktop.

f. To umount the disk:

   i. right click on the icon and select the menu item, then
   ii. select VM ➔ Removable Devices ➔ The Name Of Your Disk ➔ Disconnect (Connect to host) from the menu.

g. The drive will then be reconnected to the host. Remove it as appropriate for Windows or Fedora.

This completes the task of attaching an external disk to the appliance.