

Knoppix

Live Linux Filesystem

First Responder Guide for Law Enforcement and Corrections Officers



**THE GREAT POWER OF LINUX
ON A SMALL DISC**



07/01/2003

BASED ON DEBIAN GNU/LINUX

Preface

The purpose of this guide is to provide some basic guidance in using Knoppix as a “first responder” tool to determine whether a computer should be examined in more detail. Here are some examples of how Knoppix might be used:

Law enforcement officers have received information of a crime that may not be enough to support a warrant. They decide to conduct a “knock and talk” with the individual. During the contact they obtain consent to look at the individual’s computer for evidence. Knoppix provides a method of looking at the computer, without altering the evidence. Evidence found using Knoppix can be used as a justification to either seize the computer (where clear contraband is found, such as child porn) or establish probable cause to obtain a search warrant.

Corrections personnel (Probation, Parole, and/or Pretrial Services Officers) are responsible for supervising defendants and/or offenders for Courts and/or parole authorities. Frequently, this responsibility requires the ability to monitor an offender’s or defendant’s computer use. Knoppix provides a method to take a quick look at the computer, without altering evidence. Again, evidence found using Knoppix can be used for a violation hearing. Additionally, this evidence can be provided to law enforcement for their use in pursuing new criminal charges, i.e., to establish probable cause for a search warrant.

Officers are faced with numerous computers for processing. Imaging all of these computers for forensic processing is a timely process. Knoppix can be a method for quickly determining which computers should be imaged immediately.

This guide is not meant to describe procedures for forensic processing of a computer. This manual is limited to providing information on detecting files that have not been deleted. Individuals that are seeking to use Knoppix or other Linux tools as a forensic tool to uncover deleted files are encouraged to obtain additional training. Here are a few sites to obtain training and/or tools:

<http://www.linux-forensics.com/>

<http://ohiohtcia.org/linuxintro-1.8.1.pdf>

http://groups.yahoo.com/group/linux_forensics/

<http://www.accessdata.com/>

<http://www.asrdata.com/>

<http://crazytrain.com/content.html>

http://www.dmares.com/maresware/linux_forensics.htm

<http://biatchux.dmzs.com/>

KNOPPIX FIRST RESPONDER GUIDE

What is it?

Knoppix was created by Klaus Knopper. It is a GNU/Linux distribution that boots and runs completely from a CD. It runs a complete Linux distribution based on Debian, of recent Linux software and Desktop environments, with programs such as OpenOffice.org, Abiword, The Gimp, Konqueror, Mozilla, and hundreds more of quality open source programs, compressed from 1.7 GB to fit on a 700 MB CD. Its default windowing environment is KDE, but comes with Gnome, windowmaker, blackbox, enlightenment and many more.

Information about Knoppix such as, configuration issues, updates, etc. can be obtained at Knoppix.net.

Ernest Baca, Special Agent with Bureau of Immigration and Customs Enforcement, has modified Knoppix into package called the Penguin Sleuth Kit (PSK). Briefly, his changes to the structure are:

1. Changed KNOPPIX so it wouldn't automatically mount swap partitions.
2. Removed most language modules to make space for new security auditing tools and forensic tools software.
3. Cosmetic changes to add his feel to the Distro.

Ernest describes PSK as “no more than KNOPPIX on steroids” and notes it is just another alternative not a replacement. Individuals are encouraged to use PSK due to the modification that it will not automatically mount swap partitions. Additionally, Ernest has done a validation study of its effects on various operating systems. His modified version can be obtained at:

<http://www.linux-forensics.com/>

What is Linux?

Linux is a free Unix-type operating system originally created by Linus Torvalds with the assistance of developers around the world. It is developed under the GNU General Public License. The source code for Linux is freely available to everyone. The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

If you think of operating systems (OS) as being like cars, there are many different makes, such as Windows, DOS, Unix, and Linux. All of these OS do the same thing, i.e., run a computer. Within these OS, there are different models, such as Windows 95, Windows 98, Windows XP, etc.

KNOPPIX FIRST RESPONDER GUIDE

Linux has its own “models” or versions such as Red Hat, Mandrake, etc. These different versions have a different look or feel about them. If one general statement can be made about Linux models that sets them apart from the other OS, it is that they are FREE. Linux is like having a “free” car.¹

Do not be put off by Linux because it is free. Many argue that is much more stable and functional than other OS “makes” on which you might spend hundreds of dollars on. For more information on Linux go to linux.org.

Why should we use Knoppix?

It allows officers to examine an offender’s computer **without** altering evidence, i.e, data on the hard drive.

It allows officers to view multiple operating systems without difficulty.

It is FREE.

Steps Prior to Using Knoppix

You must make sure the subject’s computer boots to the CD drive for Knoppix to work. If the subject’s computer boots into Windows you have altered data, i.e., evidence. Here are suggested steps for making sure the computer boots to the CD:

1. Place non system, 3.5 disk in computer.
2. Access BIOS settings² (For a listing of the keys to access BIOS settings do a Google search for BIOS or check out the listing in the Appendix).
3. Note: Time and Date.
4. Check and change if there are appropriate BIOS settings to boot to CD-Rom first.
5. Place Knoppix CD in drive.
6. Save BIOS settings and exit.
7. Reboot machine.

¹Andy Rosen of ASR Data gave this analogy during a training session on SMART.

²Many computers display BIOS access instructions while the computer boots. Pressing a key or a combination of keys before the Operating System begins to load will access the BIOS. Some common keys are ESC, F1, F2, F10, Ctrl-Del or Del. Source: <http://www.iomega.com/support/documents/2157.html>, accessed 06/30/2003.

KNOPPIX FIRST RESPONDER GUIDE

Changing BIOS settings should be less and less of an issue as 3.5 drives are being phased out.

What if the subject's computer does not have a CD or DVD drive?

At present Knoppix works on approximately 75% of the machines. This amount will probably increase as new versions are released. If the subject's computer does not have a CD or DVD drive, you can not use Knoppix as described in this manual. It is strongly encouraged that you seek guidance from someone who can do an exam of the system without altering data, such as your local or state computer crime lab, Computer Analysis and Recovery Team (CART) member from the FBI or a computer team member from the U.S. Secret Service or Bureau of Immigration and Customs Enforcement Customs Investigations.

Other Issues of Concern

I. Older Systems

- A. On older systems, those without enough RAM, Knoppix will ask the user if they want to create a swap partition on the hard drive during the boot process. The no swap option should always be used. Penguin Sleuth, a modified forensic version of Knoppix has taken care of this problem and will not create a swap partition on the hard drive. Ernest Baca suggests the following procedure for previewing older computers:
1. Upon booting into Knoppix and getting the message not enough memory turn the computer off and put a USB hard drive formatted FAT32 or 256mb thumb drive in to the USB port.
 2. Then reboot with KNOPPIX. Use the 2 switch to boot to the command line.
 3. Use the command, fdisk -l to determine which drive is your thumb drive. It is always seen as a scsi device and sometimes with a FAT6 partition. If you have existing scsi drives it is always the last one on the list.
 4. If at any point it asks do you want to create a SWAP say no. Once at the command line use the mkmsdosswap command. It will then prompt you to make it on every drive. Say no until you see your thumb drive come up (ex:/dev/sda*) then click on Yes.
 5. Allocate the full thumb drive as a swap file. Then type startx from the command line.

KNOPPIX FIRST RESPONDER GUIDE

Ernest notes it works most of the time. You should be comfortable in doing the above procedure. I am reminded of a line in a Dirty Harry movie. Specifically, “A man has got to know his limitations.” This is particularly the case in computer forensics. You may wish to seek guidance from an expert prior to examining an older computer.

II. Linux Systems

- A. Care should also be made when Linux is the OS. If the suspect computer has Linux installed on it Knoppix will try to use the swap space and will alter possible evidence. Ernest Baca has noted that using Knoppix to do a live preview on computers with EXT3 or reiserfs partitions installed resulted in changes to the MD5 hash values for the partition.

Validation

Testing was done to insure that Knoppix did not write to a drive.

Ernest Baca has completed a validation study of Knoppix. He notes the following:

“In a nutshell I can reliably say that Knoppix is validated for live preview of EXT2³, FAT 32, and NTFS partitions.⁴” . I can not validate the use of Knoppix for live preview of EXT3 or reiserfs partitions until more research is done to either explain why or a solution is found to mount drives read-only without changing the state of the drive. Remember that this is a validation study for Knoppix and Knoppix derivatives and not other Linux systems.”

As new versions of Knoppix are released additional testing is required to insure that no writing to a hard drive is occurring. Officers are strongly encouraged to do their own practicing and testing of Knoppix prior to first using it on a suspect’s computer.

³EXT2 stands for Extended File System and is used by some versions of Linux. See <http://e2fsprogs.sourceforge.net/ext2intro.html#section:ext2fs>. EXT3 and reiserfs also are used by some verisons of Linux.

⁴For those unfamiliar with FAT 32 partitions they relate to Windows 95 OSR2, Windows 98, Windows 2000, and Windows Me. The original version of Windows 95, and Windows NT 4.0 do not recognize FAT32 partitions, and are unable to boot from a FAT32 volume. Windows XP uses NTFS. See <http://support.microsoft.com>, accessed 06/30/2003.

KNOPPIX FIRST RESPONDER GUIDE

Standard Review Procedures

Once Knoppix finishes loading, you will see what is very similar to a “Windows” Desktop. The media you want to look at will appear as an icon that reflects “Hard Disk Partition [hda1]” Multiple partitions or hard drives will be numbered hda2, hda3, etc.

I. Saving Files of Interest to USB Devices and 3.5 disks

- A. If you attach a USB device to the computer while in Knoppix, it will auto detect the device. You can then save files of interest to this device.
 - 1. Any USB device will be seen as “Hard Disk Partition [sdb*].” Click on it. This will bring up Konqueror.
 - 2. Check the contents to make sure it is your USB device, specifically, are the folders named the same (As preparation you may wish to create folders on the USB device prior to using it with Knoppix). Figure 1 on the next page contains a view of what Konqueror looks like for a hard drive.
 - 3. After you have confirmed which icon pertains to your USB device, exit and right click on the same icon. This will bring up a menu. Select, “Change read/write mode.” The question will appear, “Do you really want to change partition /dev/sdb* (vfat) to writeable? Click “Yes.” This will allow you to save files from the offender’s computer to your USB device.
- B. You can also save files of interest to a 3.5 disk using the same procedures.

KNOPPIX FIRST RESPONDER GUIDE

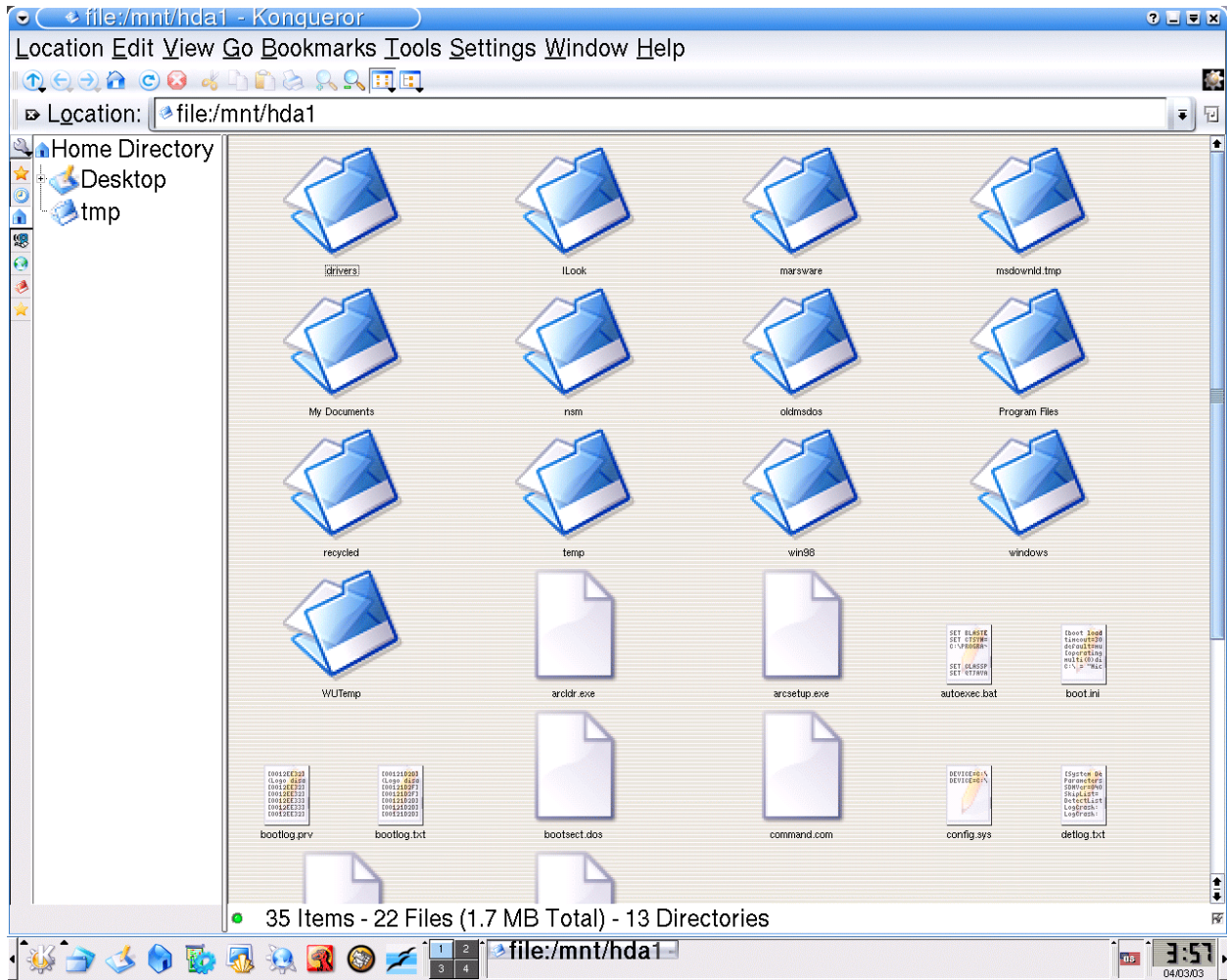


Figure 1

KNOPPIX FIRST RESPONDER GUIDE

II. Use of Konqueror

- A. Konqueror can be used to search a system for specific files of interest. It operates very similar to the Windows Find/Search functions.
1. Click on Hard Disk Partition hda. This will bring up Konqueror.
 2. On the pull down menu select “Tools.”
 3. After selecting Tools you will have several options. Select “Find.” In the example in Figure 2 we are using “*.jpg” to look for all jpg graphics files on the subject hard drive. This search will find all files with the jpg extensions on the subject’s hard drive. This same search can be used to find gif, bmp, or any other extensions. Make sure that the block “Include subdirectories” is checked and “Case sensitive search” is NOT checked (See Figure 2).
 4. Figure 3 is the result of this search. If the Thumbnails do not appear, pull down the “View” menu and change the Icon settings. Note: Dragging the mouse over the file will provide you a larger view of the file. If you click on a file to view it, the file will open. However, you will not be able to return to your search results.
 5. As you review the results you can copy and paste files of interest to your Desktop for later transfer to a USB device. You may of course also copy and paste them directly to your USB device (NOTE: If you do not transfer the files from the Desktop to the USB device they will be lost when you exit Knoppix). You can select individual files or numerous files. You can pull down the Edit on the Menu bar and select all or individual files. The copy and paste function is very similar to a Windows environment.

KNOPPIX FIRST RESPONDER GUIDE

Start of Search

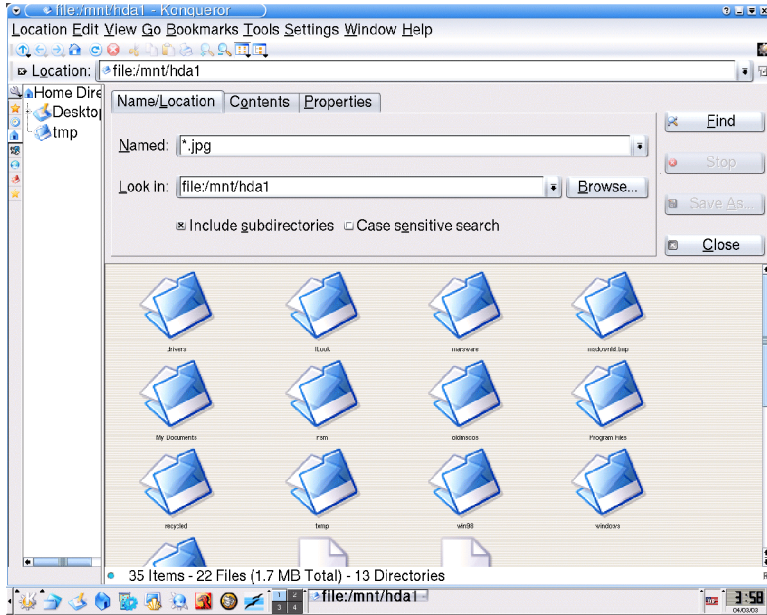


Figure 2

Results of Search

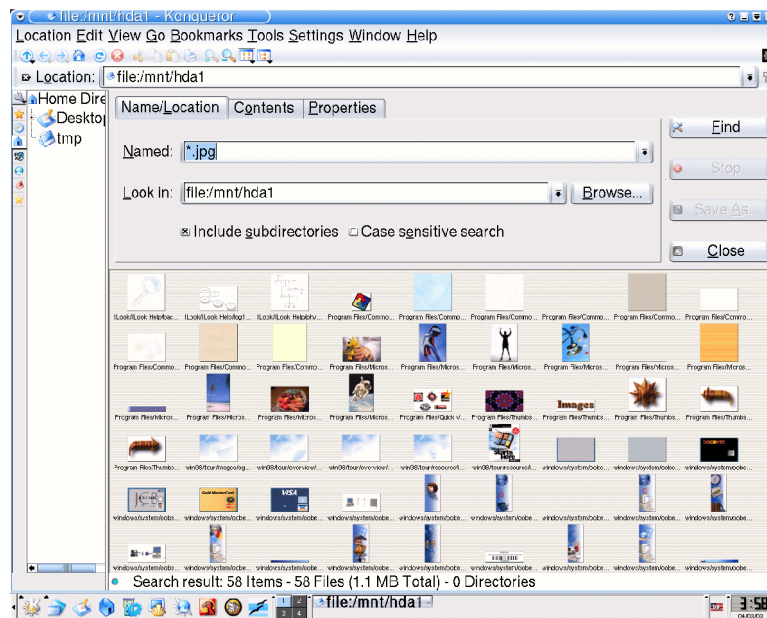


Figure 3

KNOPPIX FIRST RESPONDER GUIDE

Some specific file extensions of interest are as follows:

Nature of Offense	General Types	File Extensions
Sex	Still Images	BMP, GIF, JPG, JPEG, PNG
	Movies	AVI, MPEG, MPG, MOV, QT
Sex , Financial	Documents	DOC, PDF, PWD, TXT, WKS, WP(4,5, or 6), WPS
Financial	Worksheets	PXL, WB(1 or2) XLS, WK(1,3,4,or S)
All	Compressed	ZIP, TAR

You can also search for files that have specific text in their names. For instance, by typing in *girl* all files with girl in the name will be displayed. Such as younggirl.jpg, 14yrgirl.gif, etc.

One particular file that you might search for is “Index.dat.” These files contain Internet browsing history. Do the search, and copy all Index.dat files to your USB device for later analysis.

Directories of Interest

You may wish to search for the following directories and examine their contents:

Temp
Recycle
My Documents/My Pictures
My Received Files
Windows/cookies (Note: Index.dat file)
Windows/Favorites (Look for type of links)
Windows/History (Note. Index.dat file)
Windows/Temporary Internet Files (Look at Images)

Also be aware of directories that the offender created, such as My Child Porn or Young Kids, etc. You are going to want to look at these directories.

KNOPPIX FIRST RESPONDER GUIDE

III. Creating an Image Gallery

- A. This function will copy all thumbnails of all image files in a directory and create a HTML file.
 1. Using Konqueror, view the directory in which you are interested. Figure 4 is a view of a directory containing several different types of files.
 2. From the pull down Menu select “Tools.” Now select “Create Image Gallery.” Figure 5 is an example of what you view at the start upon clicking on Create Image Gallery. Look refers to your current directory. Directories is where you are going to save to.
 3. Change the directory to which you are going to save to the Desktop by clicking on directories (Figure 6).
 4. Click on the folder Icon at the end of the entry. Go to Desktop. You will see all devices listed (Figure 7). In location, type name of the file you are creating, such as subject’s name, Jones1, Jones2, etc. In the example we used Test.
 5. After naming the file, click okay. A new file will be created with all image files form the directory. A view of the file is contained in Figure 8. Note that non-image files are not included in this file.
 6. After creating the file on your Desktop move it to the USB device.

KNOPPIX FIRST RESPONDER GUIDE

Creating an Image Gallery

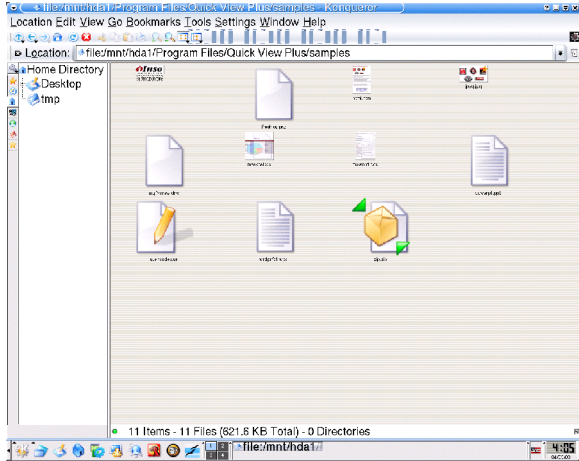


Figure 4

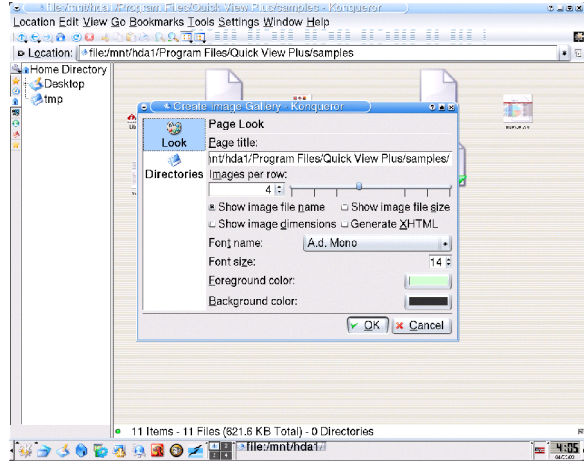


Figure 5

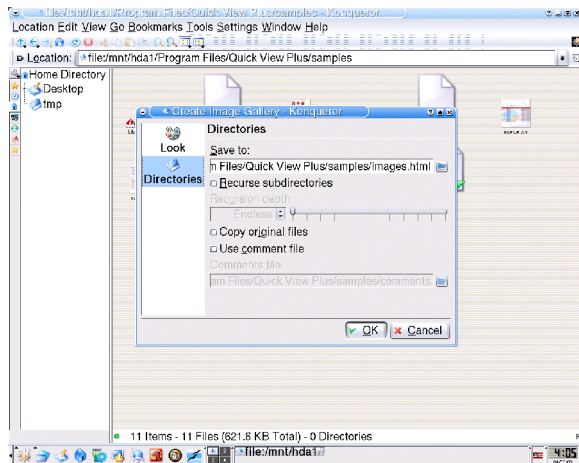


Figure 6

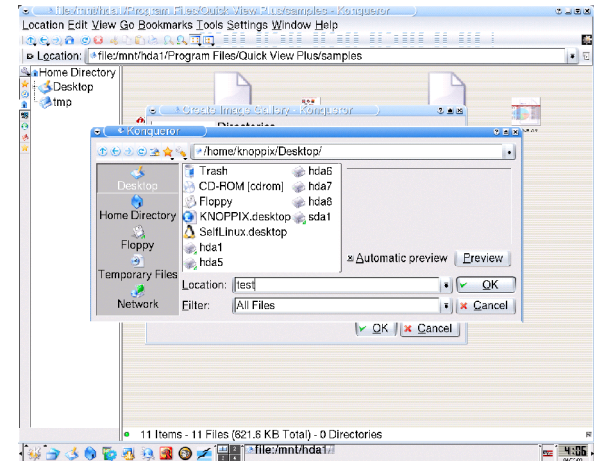


Figure 7

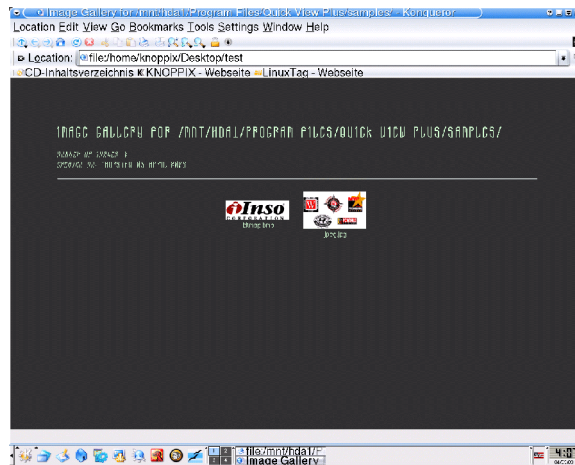


Figure 8

KNOPPIX FIRST RESPONDER GUIDE

IV. Recycle Bin

- A. As you know, files that are deleted in Windows are frequently not deleted but placed in the Recycle Bin. These files that are in the Recycle Bin can be viewed. However, even after files are actually removed from the Recycle Bin, you may be able to find information about these files by viewing a file called info2.
 1. Using the Search Tool that you used to find specific file extensions and Index.dat files, look for the info2 file. Figure 9 reflects the results of your search.
 2. Clicking on the info2 file brings up a menu that asks you with what do you wish to view the file. Select under Editors, Kedit.
 3. Figure 10 reflects the view of the info2 file. In scrolling through this file you will see original file and directory information that reference files that were sent to the Recycle Bin.

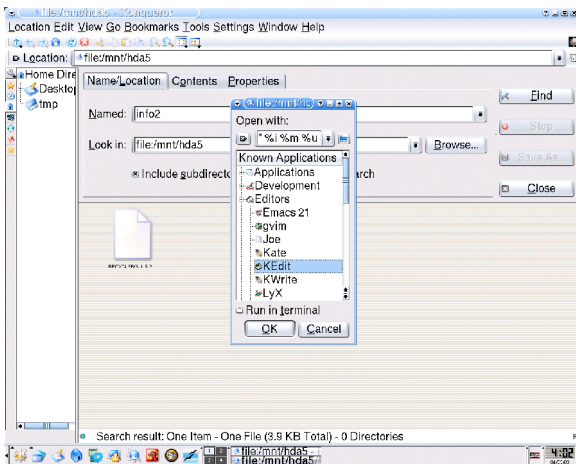


Figure 9

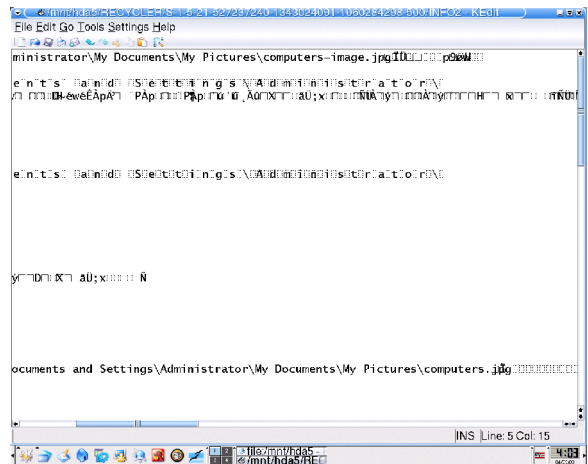


Figure 10

KNOPPIX FIRST RESPONDER GUIDE

Shutting Down Knoppix

To shutdown Knoppix click on the KDE sign located where the “Start” button is normally found on a Windows system, i.e. the lower right hand corner. Select “Log Off.”

Special Note

Knoppix is a useful tool for law enforcement and corrections officers. However, it can also be used by offenders to keep evidence of their activity, such as Internet browsing, from being saved on the hard drive of their system. Knoppix has been known to auto detect cable and DSL Internet connections with ease and to allow immediate access without difficulty.

Additional Information

This is a work in progress. If you have comments, corrections, and/or suggestions please forward them to me.

Art Bowker, Computer Crime Specialist
U.S. Probation Office, Ohio Northern
801 West Superior Avenue, Suite 300
Cleveland, Ohio 44113-1850
arthur_bowker@ohnp.uscourts.gov
Phone: 216-357-7303
Fax: 216-357-7350

KNOPPIX FIRST RESPONDER GUIDE

APPENDIX

KNOPPIX FIRST RESPONDER GUIDE

Access to BIOS Settings

Source: <http://www.iomega.com/support/documents/2157.html>, accessed 06/30/2003

Bios Manufacturer	Key Command(s)
ALR Advanced Logic Research, Inc. ® PC / PCI	F2
ALR PC non / PCI	CTRL+ALT+ESC
AMD® (Advanced Micro Devices, Inc.) BIOS	F1
AMI (American Megatrends, Inc.) BIOS	DEL
Award™ BIOS	CTRL+ALT+ESC
Award BIOS	DEL
DTK® (Datatech Enterprises Co.) BIOS	ESC
Phoenix™ BIOS	CTRL+ALT+ESC
Phoenix BIOS	CTRL+ALT+S
Phoenix BIOS	CTRL+ALT+INS
Acer®	F1, F2, CTRL+ALT+ESC
AST®	CTRL+ALT+ESC, CTRL+ALT+DEL
Compaq® 8700	F10
CompUSA®	DEL
Cybermax®	ESC
Dell® 400	F3
Dell 400	F1
Dell Dimension®	F2 or DEL
Dell Inspiron®	F2
Dell Latitude	Fn+F1 (while booted)
Dell Latitude	F2 (on boot)
Dell Optiplex	DEL
Dell Optiplex	F2
Dell Precision™	F2

KNOPPIX FIRST RESPONDER GUIDE

eMachine™	DEL
Gateway® 2000 1440	F1
Gateway 2000 Solo™	F2
HP® (Hewlett-Packard)	F1, F2
IBM®	F1
IBM E-pro Laptop	F2
IBM PS/2®	CTRL+ALT+INS after CTRL+ALT+DEL
IBM Thinkpad® (newer)	Windows: Programs-Thinkpad CFG.
Intel® Tangent	DEL
Micron™	F1, F2, or DEL
Packard Bell®	F1, F2, Del
Sony® VIAO	F2
Sony VIAO	F3
Tiger	DEL
Toshiba® 335 CDS	ESC
Toshiba Protege	ESC
Toshiba Satellite 205 CDS	F1
Toshiba Tecra	F1 or ESC

KNOPPIX EVIDENCE INVENTORY WORKSHEET
Original Media Access Worksheet

TO DOCUMENT EACH ACCESS TO ORIGINAL MEDIA	Date:	Time:	
	Accessed by:		
	Computer ID:		
Location of Computer:			
BIOS SETTINGS			
Access Date:	System Date:		
Access Time:	System Time:		
BIOS Set to Boot to CD ROM	YES	NO	
BIOS Settings Modified to Boot to CD ROM	YES	NO	
SEARCH			
Following files extensions were searched for:			
JPG	JPEG	GIF	OTHER:
PNG	AVI	MPEG	
Following text and/or file names were searched for:			
During search the following directories were examined:			
Search revealed following:			
Results documented to media	YES	NO	
Computer Seized	YES	NO	
Special Notes:	Time Ended		