

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To) -	
4. TITLE AND SUBTITLE Helix Tool Introduction Laboratories			5a. CONTRACT NUMBER W911NF-11-1-0174		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 206022		
6. AUTHORS Dr. Jeff Duffany (Advisor), Michelle Maldonado			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Polytechnic University of Puerto Rico 377 Ponce De Leon Hato Rey San Juan, PR 00918 -			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 58924-CS-REP.14		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly					
15. SUBJECT TERMS MD5 Generator; Rootkit Revealer; Cookie Viewer					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Alfredo Cruz
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 787-622-8000

## **Report Title**

Helix Tool Introduction Laboratories

### **ABSTRACT**

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification. For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge. Helix can be run as an operating system, it can be run from command line and it also has a windows GUI. Helix allows for the analysis of a live system. Many corporate systems use Windows and the Windows GUI is a perfect way to get started in practicing forensics. In this document you will find simple laboratories to follow so that you may familiarize yourself with the Helix tool using the Windows GUI and get started in the practice of computer forensics

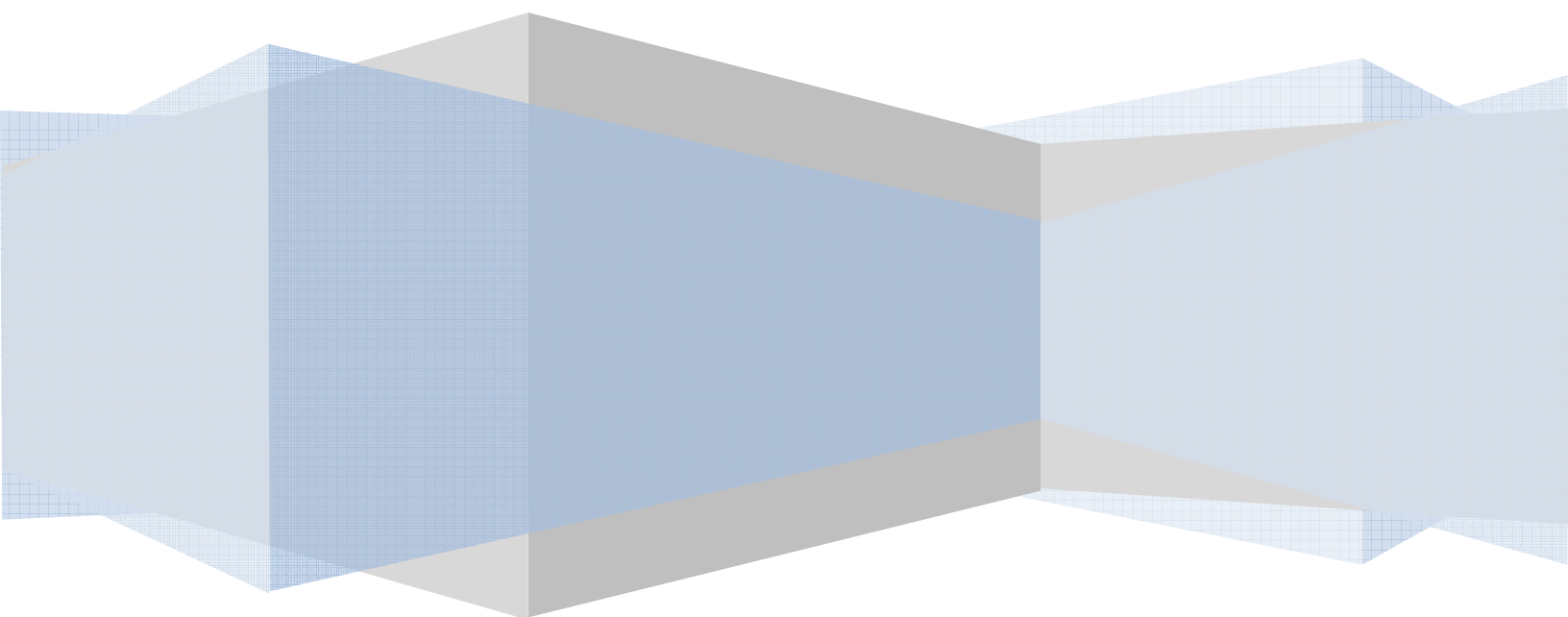
These laboratories were run on an XP-virtual machine. Helix is available as a free downloadable ISO image from <http://www.e-fense.com/helix/>.

# Helix Tool

Introduction Laboratories

Michelle Maldonado Rodríguez

2012



## Table of Contents

Introduction .....	3-4
Familiarizing ourselves with the Windows Side .....	5-8
Laboratory 1 - Preview System Information .....	9-11
Laboratory 2 - Acquire a “live” image of a Windows System using dd.....	12-19
Laboratory 3 - Incident Response tools for Windows Systems.....	20-28
Part A – MD5 Generator .....	22-23
Part B – Rootkit Revealer .....	23-25
Part C – Internet Explorer History Viewer .....	25-27
Part D – Internet Explorer Cookie Viewer .....	27-28
Laboratory 4 – Scan for pictures of a live system. ....	29-31
Laboratory 5 – Exiting Helix .....	32

## Introduction

Computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the computer in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the hard drive. Once the original hard drive has been copied, it is locked in a safe or other secure storage facility to maintain its pristine condition. All investigation is done on the digital copy. However there are some systems that cannot be taken offline and the investigation of a live running system may be required.

Investigators use a variety of techniques and proprietary forensic applications to examine the hard drive copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

For someone who would like to get started practicing computer forensics it might be a little overwhelming. There are many different tools, and techniques. Each tool will provide different capabilities and will affect the suspect system differently. Some tools can be very expensive, but there are many tools available which are free and fairly complete. The Helix tool is very robust and free of charge. Helix can be run as an operating system, it can be run from command line and it also has a windows GUI. Helix allows for the analysis of a live system. Many corporate systems use Windows and the Windows GUI is a perfect way to get started in practicing forensics. In this document you will find simple laboratories to follow so that you may familiarize yourself with the Helix tool using the Windows GUI and get started in the practice of computer forensics

These laboratories were run on an XP-virtual machine. Helix is available as a free downloadable ISO image from <http://www.e-fense.com/helix/>.

While it is possible to download the image file with your browser, it is recommended that you use a download accelerate such as Download Express (<http://www.metaproducts.com/DE.html>), Download Accelerator Plus (<http://www.speedbit.com/>), or Get Right (<http://www.getright.com/>) to ensure that the large file, which is about 700MBs, downloads properly. These utilities can resume

downloads that are interrupted, and can segment large files and simultaneously download the different segments for faster transfers.

## Helix User Manual

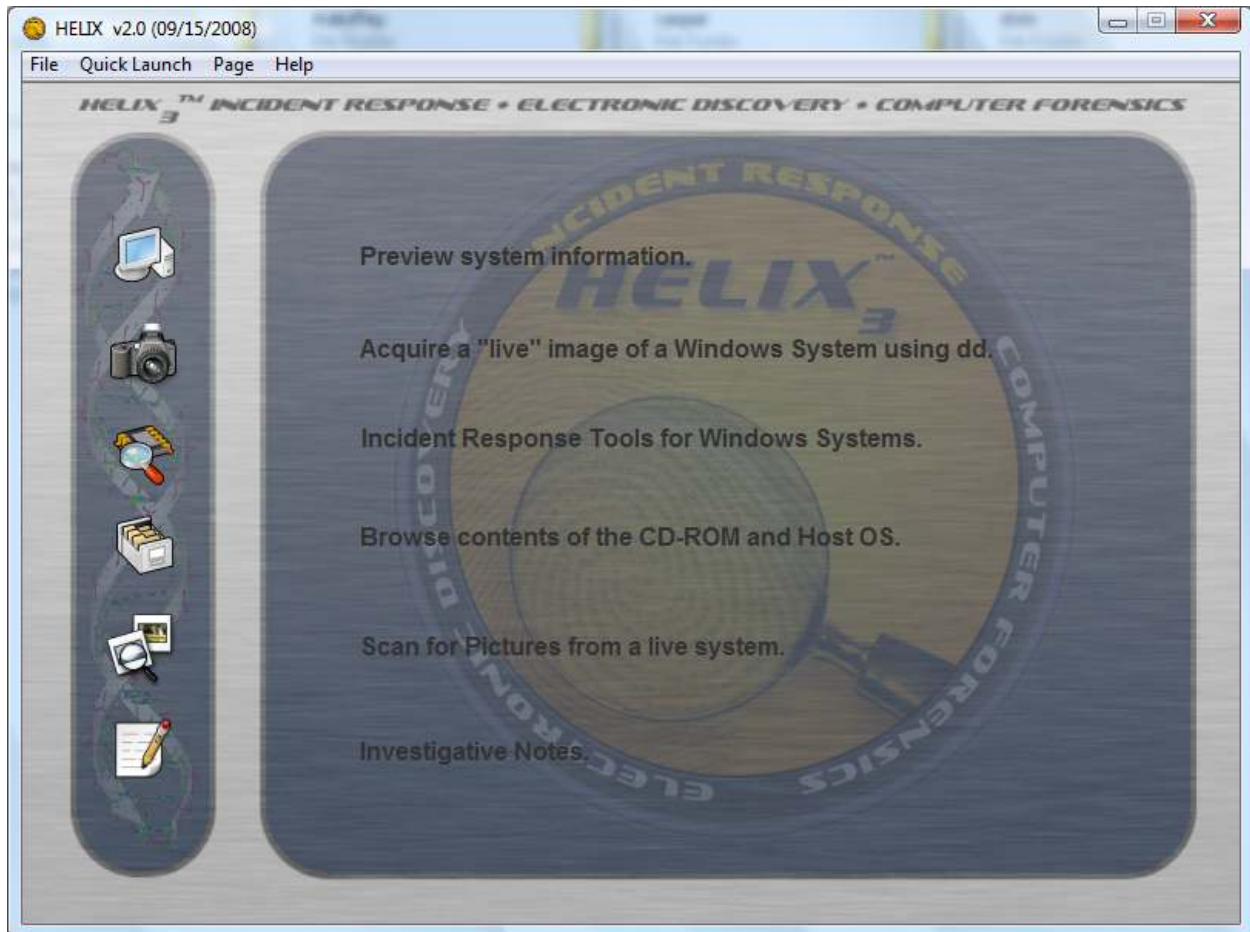
### I. Familiarizing ourselves with the Windows Side

*Note: When performing a live preview of a system, many of the actions taken can and will modify information on the suspect machine. This method should only be used when the system cannot be taken offline.*

1. Insert the Helix CD in the computers CD drive. If the CD auto-run features is enabled (which is the Windows default), a Helix warning window should appear. If auto-run is disabled, you can run Helix by double clicking on the helix.exe file on the CD.



2. Select the language you prefer and click on the Accept button. Then the main window will be opened.









3. This Main screen doesn't behave as a standard window. It doesn't show up in the taskbar, and you cannot switch to it via the <ALT><TAB> key sequence. Helix does place an icon in the system tray which can be used to access the program. To bring the Helix main screen to the front, you can double-click on the icon, or right-click, and select Restore. Other options on the right-click menu include Minimize and Exit.



4. Main Options:



- a.  **Preview System Information**  
This choice will provide you with the basic information of the system. It includes Operating system version, network information, owner information, and a summary of the drives on the system. In addition, there is a second page that will show a list of running processes.
- b.  **Acquire a “live” image of a Windows System using dd**  
This option will allow the investigator to make copies of hard drives, floppy disks, or memory, and store them on local removable media, or over a network.
- c.  **Incident Response tools for Windows Systems**  
This option provides access to 20 tools, all of which can be run directly from the CDROM. Once you click the icon, a small triangle will appear, next to the icon. Clicking on this small triangle will provide access to the others pages of tools.
- d.  **Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime**  
The option provides the user with access to some common reference documents in PDF format. The documents include a chain of custody form, preservation of digital evidence information, Linux forensics Guide for beginners, and forensic examination for digital evidence guide. These documents are highly recommended, and the investigator should review them before attempting any forensic examination.
- e.  **Browse contents of the CD-ROM and Host OS**  
This is a simple file browser that will provide the investigator with information about the selected file. It will display the filename, created, accessed and modified dates, Attributes, CRC, MD5 and the file size. Due to the nature of the windows operating system, the first time you select a file; it will display the access date of the last access. If you select the same file again, it will display the date and time of the previous access. This is a feature of the windows operating system, and cannot be prevented. This is one of the problems with examining a live system – the investigator’s actions may modify the system.
- f.  **Scan for Pictures from a live system**

This tool will allow the investigator to quickly scan the system to see if there are any suspect graphic images on the suspect system. Many different graphic formats are recognized, and displayed as thumbnails.

## 5. Menu Bar



In addition to the icons, all the features are directly accessible via the Helix menu bar.

File – Allows the user to exit the Helix application

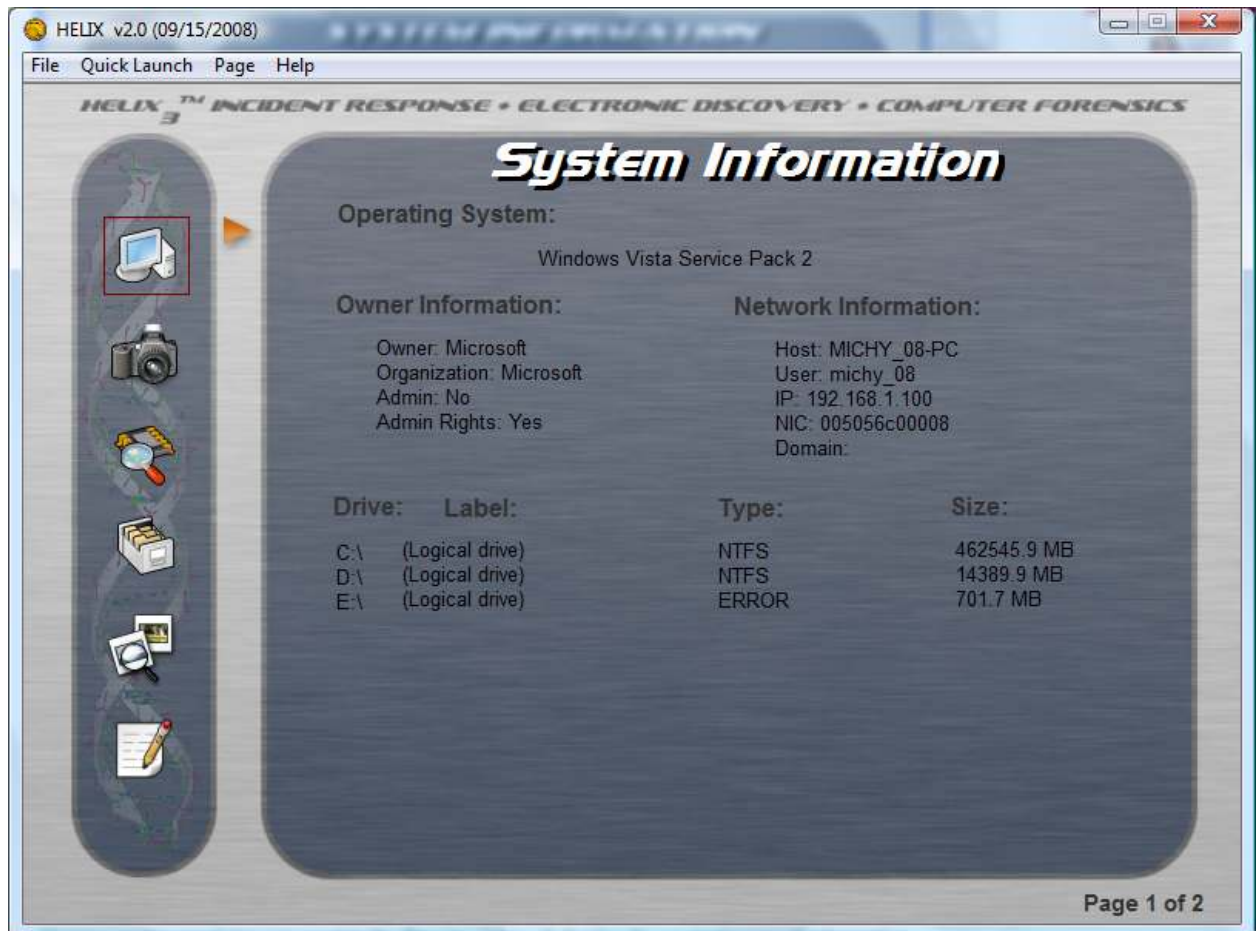
Quick Launch – Allows the user to launch a command tool or the FTK Imager software

Page – Allows the user to jump directly to any of the utility screens

Help – Displays information about the program, and the license agreement

## Laboratory 1 - Preview System Information

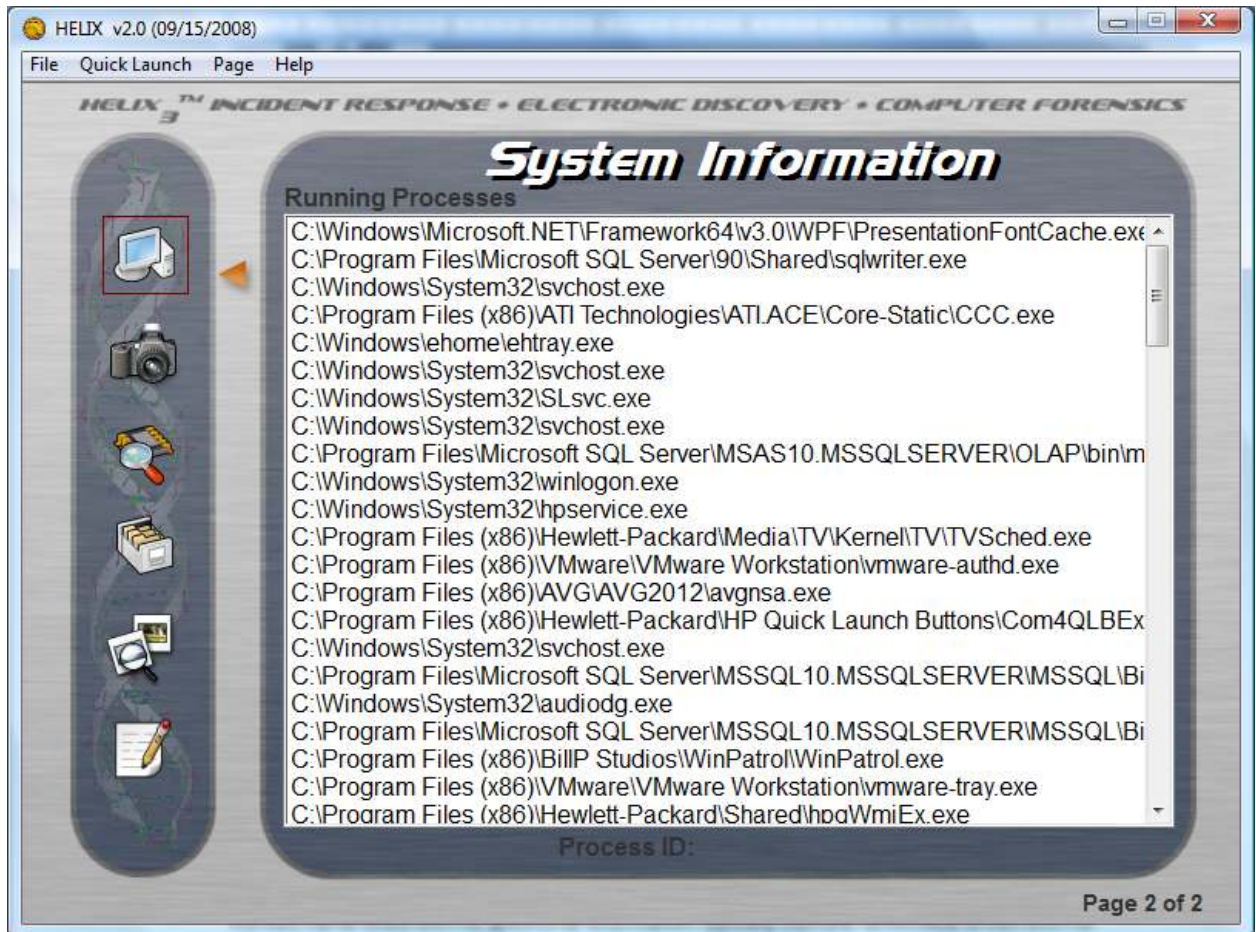
1. Select the Preview System Information option from the menu.



This screen displays some general information about the system being investigated. Some points of interest:

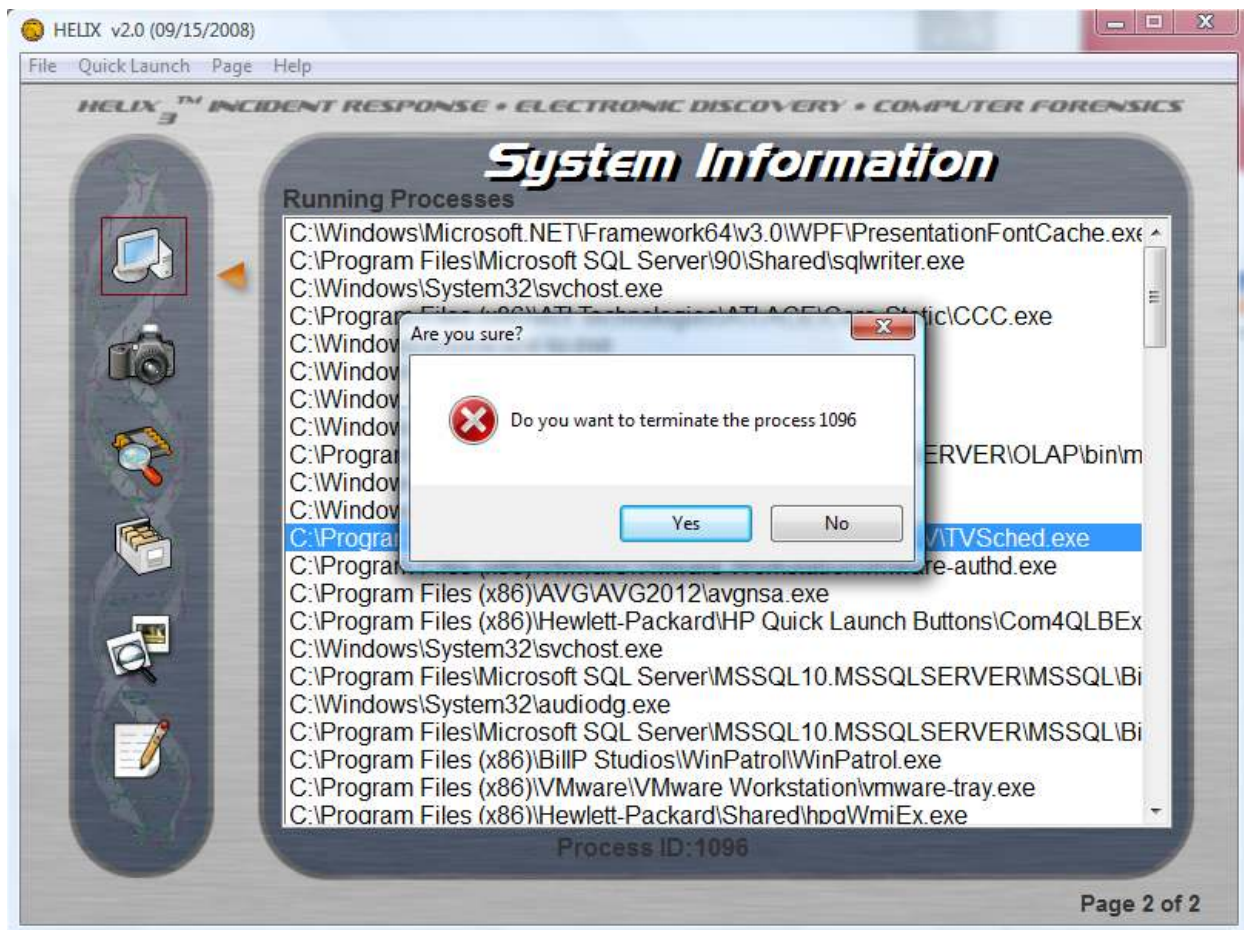
- “Admin:” tells us if the current user is the administrator (good security practice to change the name of the administrator account)
- “Admin Rights” tell us of the current user has administrator privileges.
- “NIC:” is the MAC address of the network card. If this value is “000000000000” it indicates that the network card is in promiscuous mode, and could be capturing all the network traffic on the system.
- “IP:” is the current IP address – this could change if the system is set up for DHCP.
- Drives name listed with no additional information typically indicate removable drives with no media inserted.

2. Click on the small triangle next to the Preview Icon. This will display the second page of information, which lists the running processes. Clicking the triangle will flip the between the two pages of information.



In addition to displaying all the running processes in memory, double-clicking on any process will provide the user the option to terminate the selected application. Care should be taken, and the investigator should be sure they are terminating the proper process. Terminating the wrong process could result in system damage and loss of forensic evidence.

3. Select a process and double click on it.



NOTE: Why don't we just use the built in "task manager" to display this information? If they system has been hijacked by a root kit, or some other malicious program, it is possible that the Windows Task Manager has been modified to not display the malicious code. Since Helix is running from the CD, it cannot be modified, and should be able to display all the programs currently running on the system.

Now you have some knowledge about the system that you're analyzing and the processes that are being run on it. And if there are hidden processes that are running which the owner of the system was unaware of you have been able to identify those as well.

## Laboratory 2 - Acquire a “live” image of a Windows System using dd

Select the acquisition option in the menu. There are two tools provided to acquire images of physical memory or disk drives. On the first page, there is a graphical front-end to the command line version of dd, a common disk duplication utility. The dd utility can capture physical memory and drives. Also, dd can image over a network.



### Part A - Using dd

The source field includes a drop-down box for the investigator to select any drive in the system. The destination can be a local removable drive, network drive or a net-cat listener. The image name is the user chosen name, and the standard extension is “.dd”.

The Options include:

- Attached/Shared: check this option to save the image to a local drive, or a network share.
- Net-Cat: check this option to transfer the image to a net-cat server located on the network. With this option you will need to specify the IP address and port number of the net-cat server.

- Split Image: Allows you to split the image into multiple files if the image will exceed the capacity of the storage medium. For example, if you are imaging a 10 gig hard drive, you can split the image so that it will fit on a CDROM, DVD, or FAT 32 file system, which has a 4 gig file size limitation.

Select the desired source and destination files. Once you enter all the parameters, and press the “Acquire” button, a forensic command shell window will open up. This command shell uses trusted binaries to prevent root kits from tampering with the image being created. You can now paste the dd command line into the shell by right clicking and selecting “paste” from the context menu. Press enter to execute the command.

Once the command is finished, there will be 3 files in the destination directory:

- Filename.dd – the image of the source disk
- filename.dd.md5 – a file containing the MD5 of the image file.
- Audit.log – a file containing the command and the output of the program.

You should examine the Audit.log file. If all went well you should see that all the MD5 Hashes match and you will see the message “The checksums do match”. If they match, that means you have an accurate copy of the evidence. Here is an example of the file.

```

image.dd_audit - Notepad
File Edit Format View Help
Forensic Acquisition utilities, 1, 0, 0, 1035
dd, 3, 16, 2, 1035
Copyright (C) 2002-2004 George N. Garner Jr.

Command Line: dd.exe if=\\.\PhysicalMemory of="C:\Documents and Settings\Administrator\Desktop\image\image.dd"
conv=noerror --md5sum --verify=md5 --md5out="C:\documents and settings\Administrator\Desktop\image\image.dd.md5"
--log="C:\Documents and Settings\Administrator\Desktop\image\image.dd_audit.log"

Based on original version developed by Paul Rubin, David Mackenzie, and Stuart Kemp
Microsoft Windows: version 5.1 (Build 2600.Professional Service Pack 2)

26/04/2012 00:37:37 (utc)
Current User: VICTIMA-01\Administrator

Total physical memory reported: 523760 KB
Copying physical memory...
D:\JRF\FAU\dd.exe:
stopped reading physical memory:

The parameter is incorrect.
\6843dc92866da9c6f0e41ef9957b8b [\\.\PhysicalMemory] C:\Documents and Settings\Administrator\Desktop\image\image.dd

Verifying output file...
\6843dc92866da9c6f0e41ef9957b8b [C:\documents and settings\Administrator\Desktop\image\image.dd] C:\documents and settings\Administrator\pa
The checksums do match.
The operation completed successfully.

Output C:\documents and settings\Administrator\Desktop\image\image.dd 526866816/526866816 bytes (compressed/uncompressed)
131071+0 records in
131071+0 records out

```

And that’s it. You now have an accurate copy of the suspect’s chosen drive. Print out the Audit.log file, put it in the evidence envelope along with the original floppy, update the chain-of-custody form, and return the evidence to the evidence locker.

## Part B - Using FTK Imager

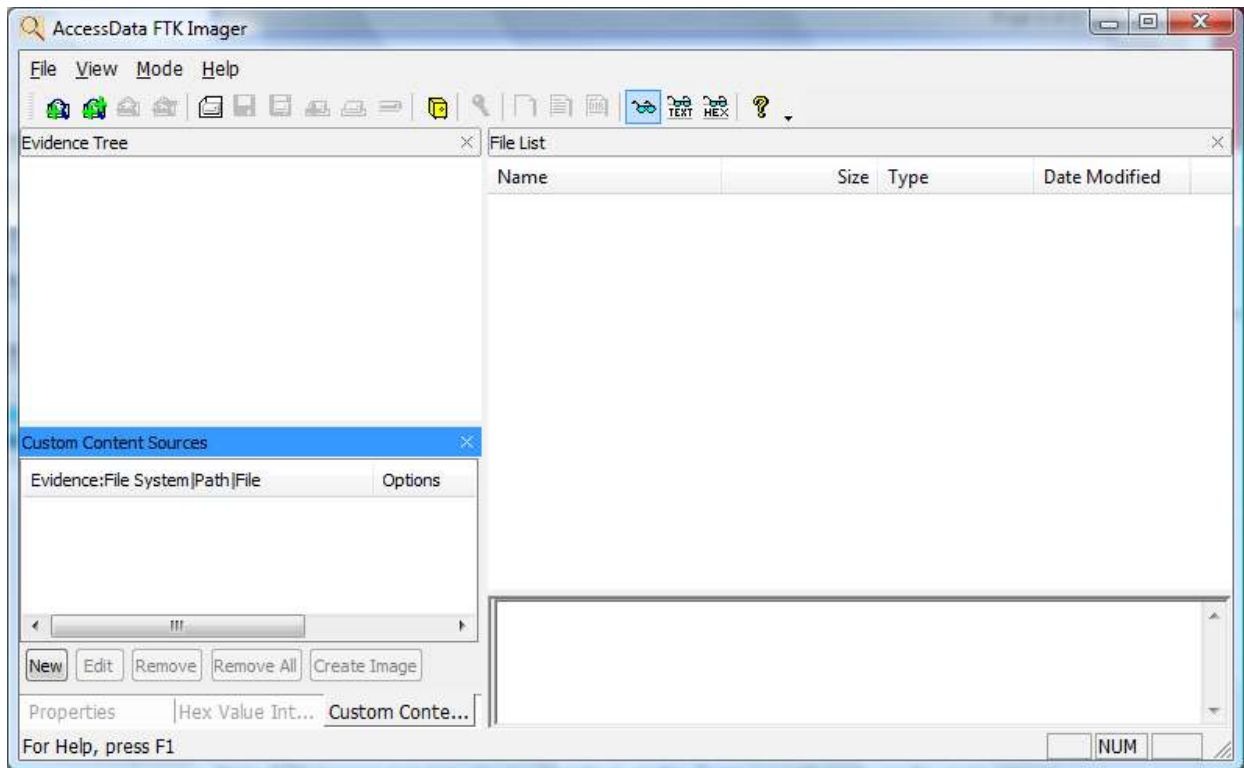
“FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with Access Data® Forensic Toolkit® (FTK™) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence.” (Access Data, 2005) According to the FTK Image Help File (Access Data, 2005), you can:

- Preview files and folders on local hard drives, floppy diskettes, Zip disks, CDs, and DVDs.
- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs.
- Preview the contents of forensic images stored on the local machine or on a network drive.
- Export files and folders.
- Generate hash reports for regular files and disk images (including files inside disk images). To access the FTK Imager, select the second page of the Image Acquisition page. This page will display the release notes for the current version of the tool. Click on the “Imager” to launch the actual application.

To access the FTK Imager, select the second page of the Image Acquisition page. This page will display the release notes for the current version of the tool. Click on the “Imager” to launch the actual application.





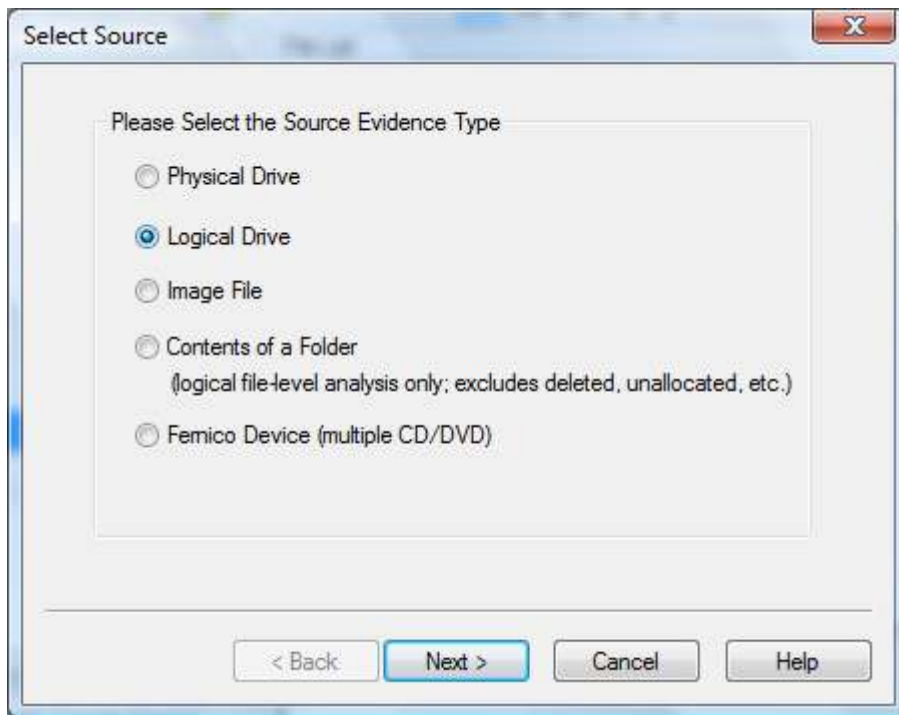


*Note: FTK Imager can now also be launched via the Quick Launch menu on the main screen.*

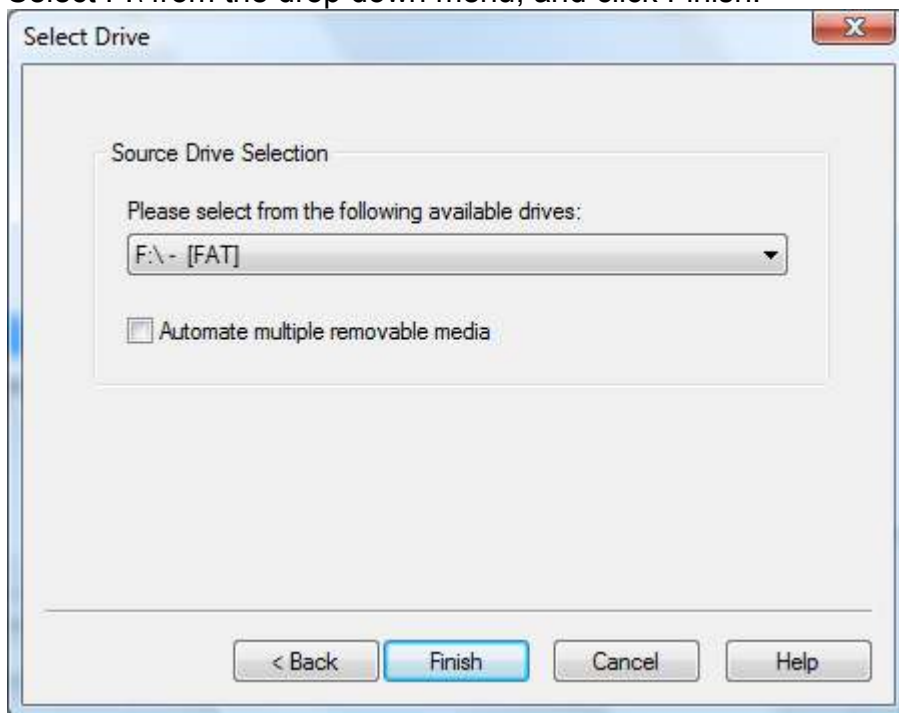
The FTK imager is a powerful and flexible tool. It can be used to examine media and images, and extracted deleted files. It has extensive information available via the Help menu or the question mark icon on the toolbar.

Once you have an image of a disk it might be a good idea to have additional copies, just in case. Let's use the FTK Imager to create the image and the necessary copies. For this test let's say that we have received a flash drive belonging to a suspect. It could be a different source, like a floppy disk for example.

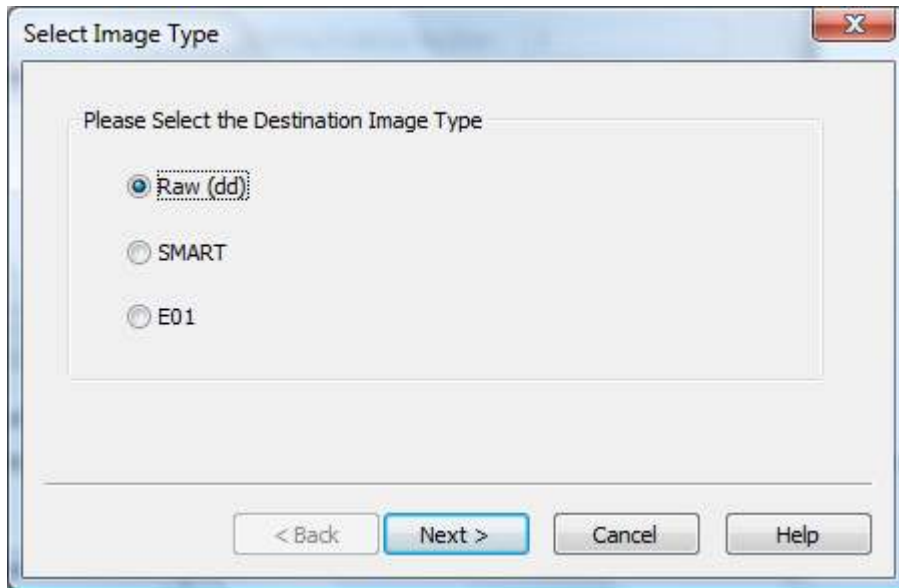
First From the menu, select File / Create Disk Image. Select Logical Drive, and click Next.



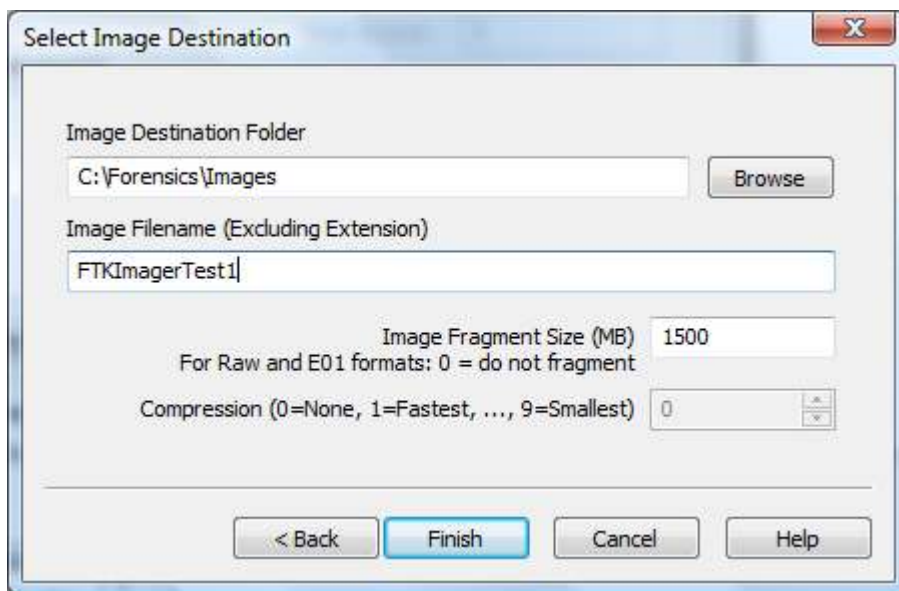
Select F:\ from the drop down menu, and click Finish.



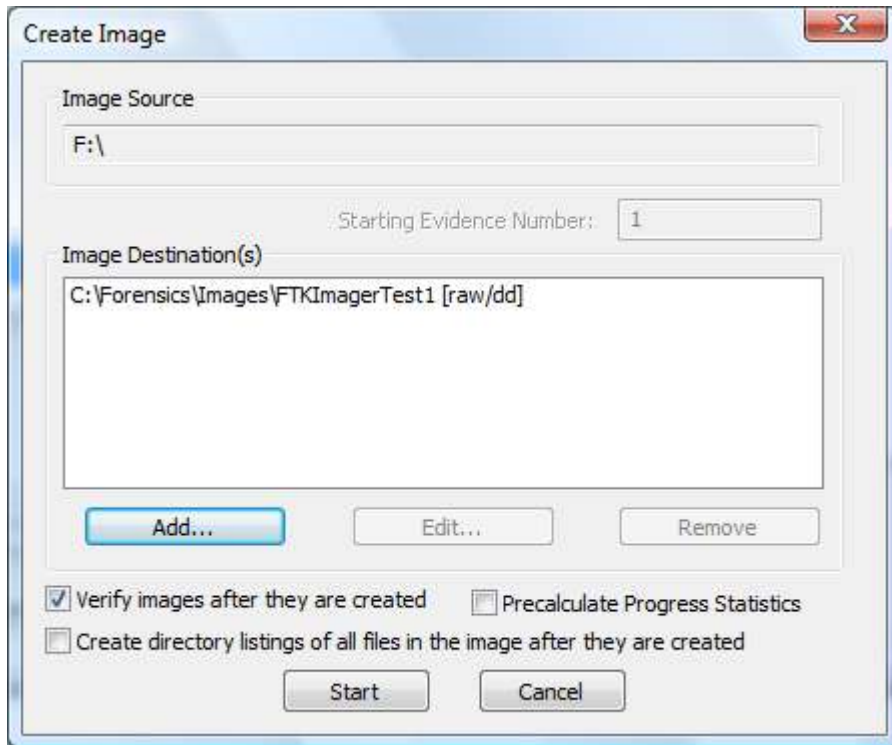
Now you are to select the destination drive. Click "Add...". You can choose from three Image Types. Raw (dd) is the same format as created by dd command, and is the most universal format. Smart is for the SMART forensic tool from ASR Data, and E01 is the format used by EnCase. Be sure that the "Raw (dd)" option is selected and click Next.



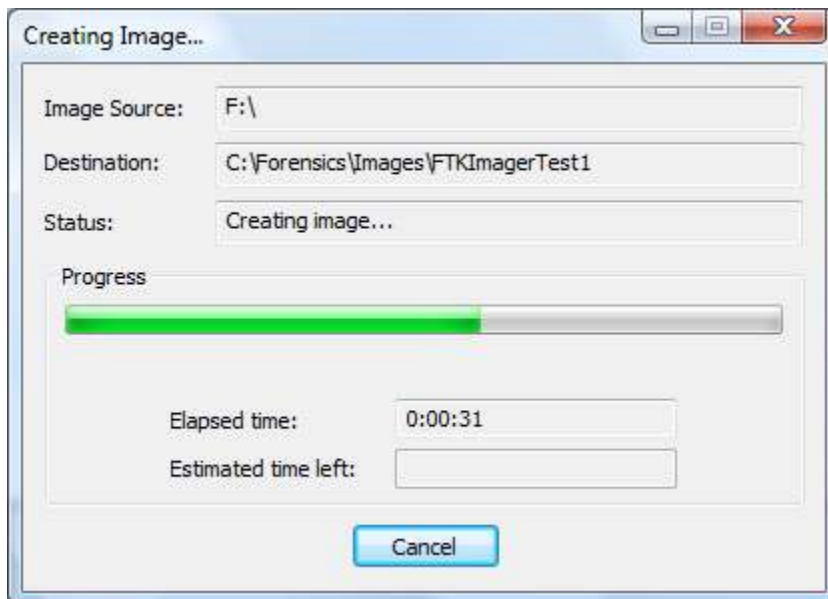
Select the folder you wish to create the image in. Include the image file name, but not the extension, it will be added automatically. The image fragment size is used to split large images into chunks that can fit into removable media. In this case we will be saving into a local folder that we will create in the C:\ drive. (C:\Forensics\Images). Click Finish.



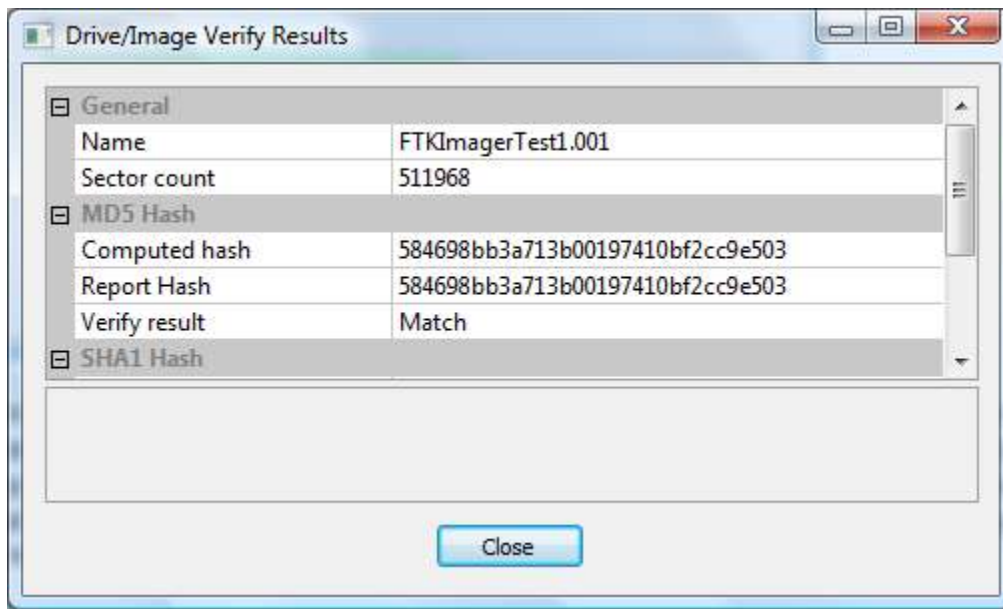
You are returned back to this screen. Click Start.



The time it takes to perform the image will vary on the size of the image we are creating.



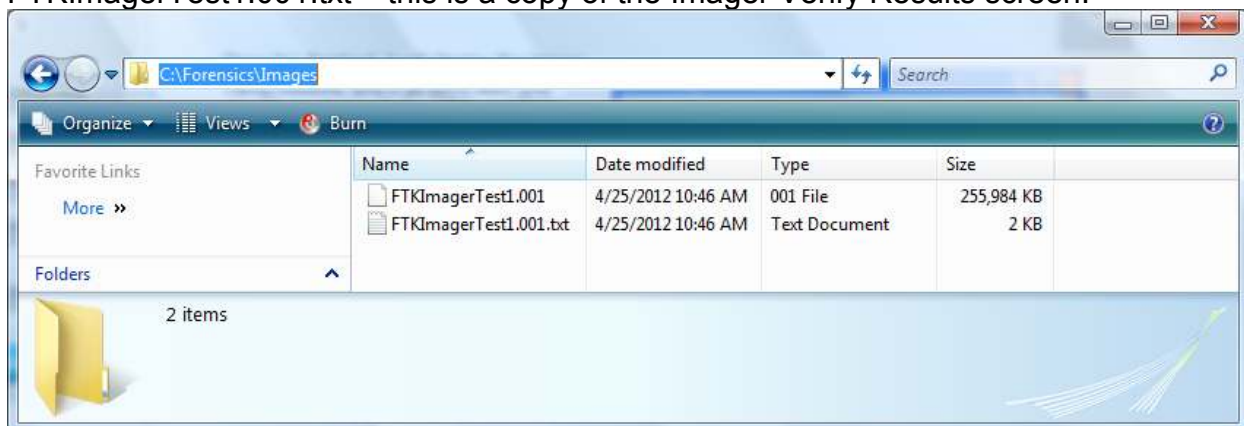
Once it is finished, it will display the Image. Verify Results, and if all went well, you should see that both the MD5 and SHA1 hashes displayed match. If they match, that means you have an accurate copy of the evidence. If they don't match, that typically means you have a bad disk, and the drive had a problem reading the source. Click Close You can click Close again on the Creating Image screen.



You should have two files in your destination folder:

FTKImagerTest1.001 – this is the image of the source disk.

FTKImagerTest1.001.txt – this is a copy of the Imager Verify Results screen.

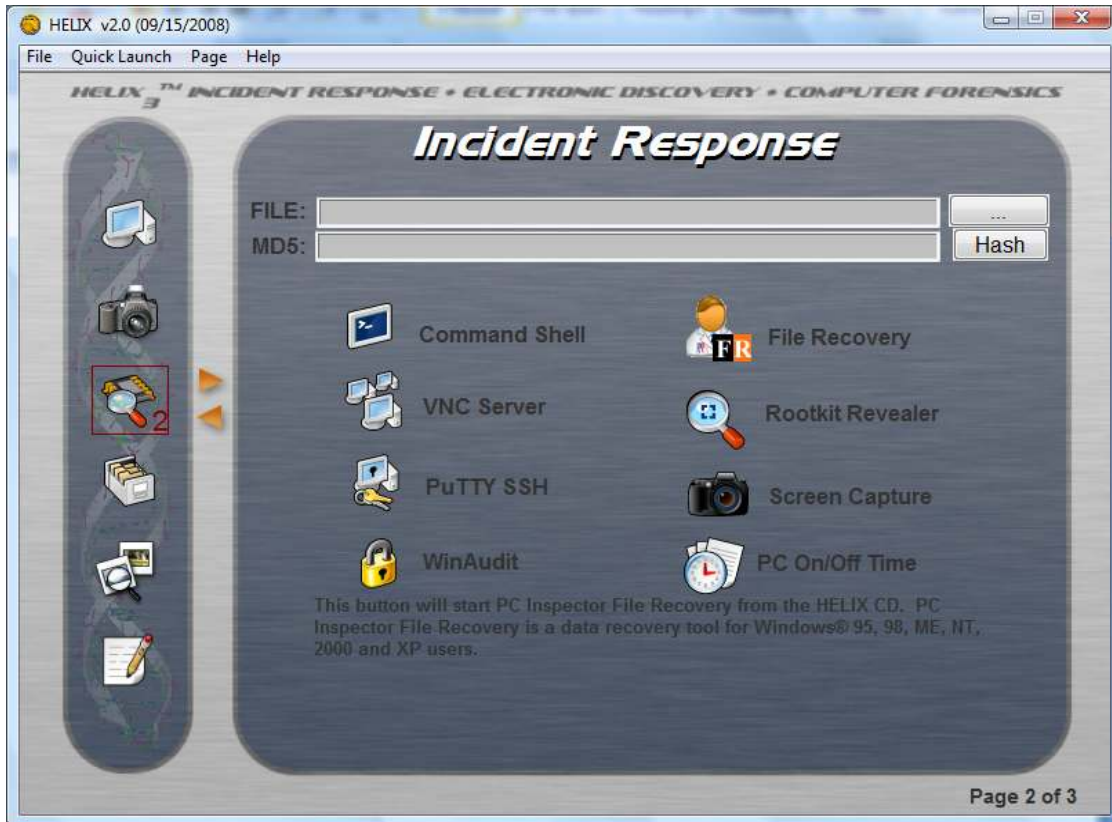


Congratulations! You now have an accurate copy of the suspect's disk. Print out the FTKImagerTest1.001.txt file, put it in the evidence envelope along with the original disk (in our case flash drive), update the chain-of-custody form, and return the evidence to the evidence locker. In order to create a copy you will repeat the previous steps but you will then save the image onto the appropriate removable media selected.

## Laboratory 3 - Incident Response tools for Windows Systems



This panel provides the investigator with a number of tools to respond to incidents. There are three pages to this panel; the other pages can be accessed by clicking on the small triangles next to the Incident Response icon in the left tool bar. We will only go through some of the options available.



The tools include:

- Windows Forensics Toolchest (WFT)
- Incident Response Collection Report (IRCR2)
- First Responder's Evidence Disk (FRED)
- First Responder Utility (FRU)
- Security Reports (SecReport)
- Md5 Generator
- Command Shell – a forensically sound command shell
- File Recovery – recover deleted files
- Rootkit Revealer – detect the presence of rootkits on the system
- VNC Server
- Putty SSH
- Screen Capture
- Messenger Password
- Mail Password Viewer
- Protected Storage Viewer
- Network Password Viewer
- Registry Viewer
- Asterisk Logger
- IE History Viewer
- IE Cookie Viewer
- Mozilla Cookie Viewer

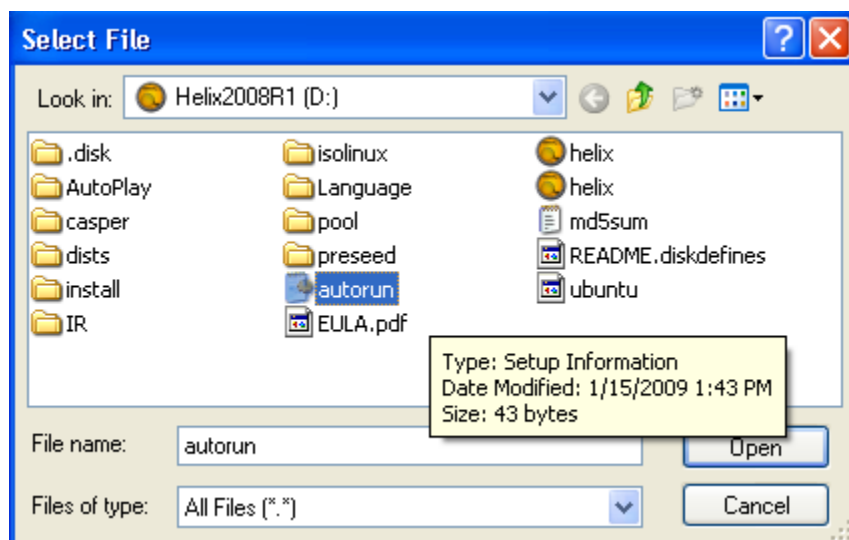
## Part A – MD5 Generator

On the top part of the second page of the incident response option you will find the option of generating the MD5 signature for any file in your system.





First click on the “...” button, this will bring up the file manager so that you may select a file from your system. Select any file you like.



Once the desired file is in the file text box you may press the “hash” button. Helix will proceed with the MD5 signature generation. And you now have the MD5 signature for the file you selected.

## Part B – Rootkit Revealer

Rootkit Revealer is a freeware tool from SysInternals. It successfully detects all rootkits published at [www.rootkit.com](http://www.rootkit.com).

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

Rootkits have become more common and their sources more surprising. In late October of 2005, security expert Mark Russinovich of Sysinternals discovered that he had a

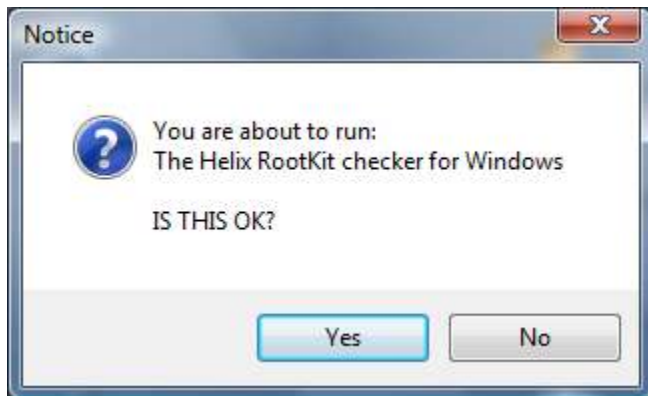
rootkit on his own computer that had been installed as part of the digital rights management (DRM) component on a Sony audio CD. Experts worry that the practice may be more widespread than the public suspects and that attackers could exploit existing rootkits. "This creates opportunities for virus writers," said Mikko Hypponen, director of AV research for Finnish firm F-Secure Corp. "These rootkits can be exploited by any malware, and when it's used this way, it's harder for firms like ours to distinguish the malicious from the legitimate."

A number of vendors, including Microsoft, F-Secure, and Sysinternals, offer applications that can detect the presence of rootkits. If a rootkit is detected, however, the only sure way to get rid of it is to completely erase the computer's hard drive and reinstall the operating system.

Let's run the application. First, click on the rootkit revealer icon.



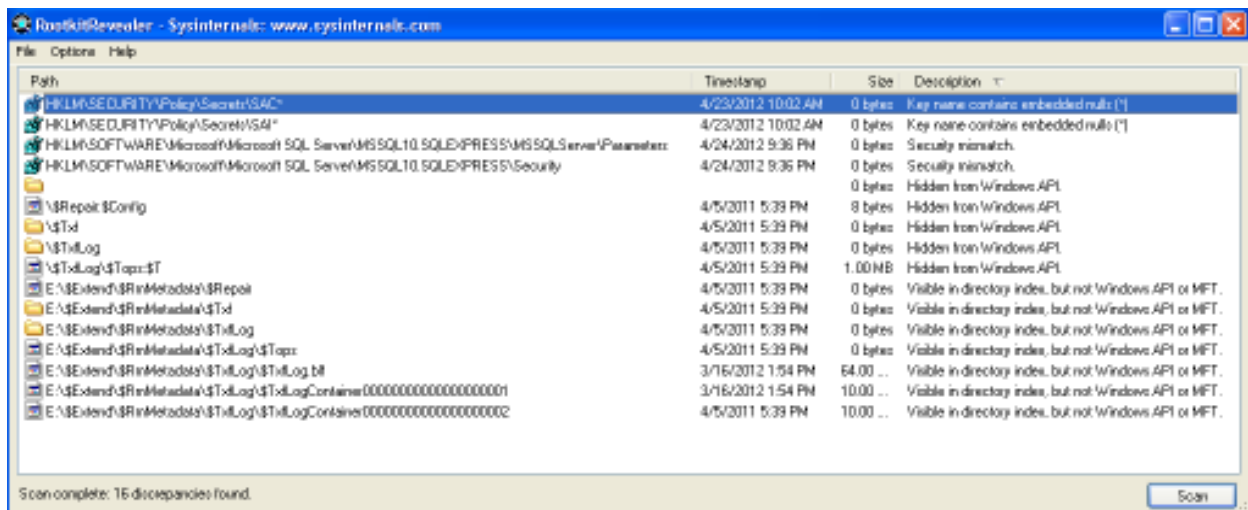
When asked for confirmation click "Yes".



You may be asked to accept the terms of agreement. If you wish to proceed, click on the "Accept" button.



The main scanning window will be presented. The program will run at the level of the currently logged in user. It would be best to run this as a system administrator for more accurate results.



In order to interpret the output you can find the meaning of the description column in the sysinternals web site. The results of the scan can be saved to a file using the File/Save option. This tool is meant to find rootkits, not remove them. Depending on the nature of the investigation the detection of the rootkit needs to be documented and the system preserved for future investigation.

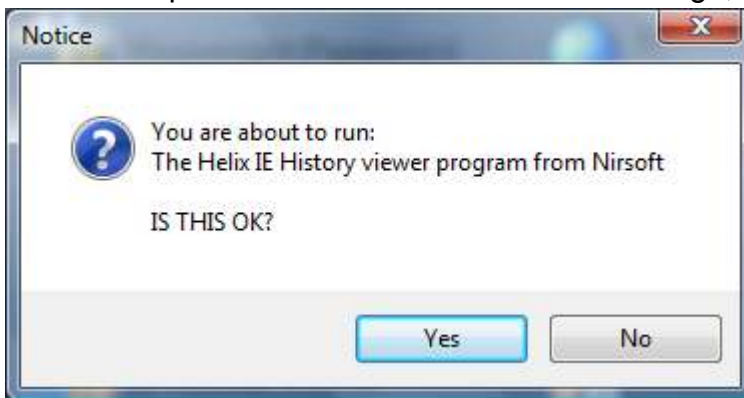
## Part C – Internet Explorer History Viewer

Each time you type a URL in the address bar or click on a link in the Internet Explorer browser, the URL address is automatically added to the history index file. This utility reads all the information from the history file on your computer, and displays the list of all the URLs that you have visited in the last few days. It also allows you to select one or more URL addresses, and then remove them from the history file or save them into a text, HTML, or XML file. In addition, you are allowed to view the visited URL list of other user profiles on your computer, and even access the visited URL list on a remote computer, so long as you have permission to access the history folder.

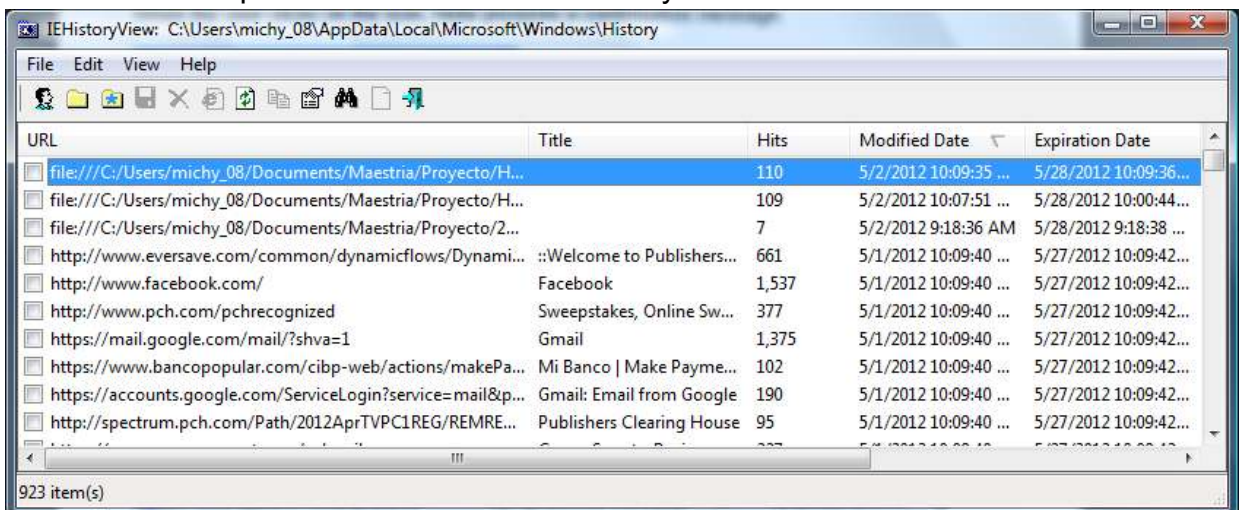


**IE History Viewer**

1. Click on the **IE History Viewer** option.
2. You will be presented with a confirmation message, click “Yes” to proceed.

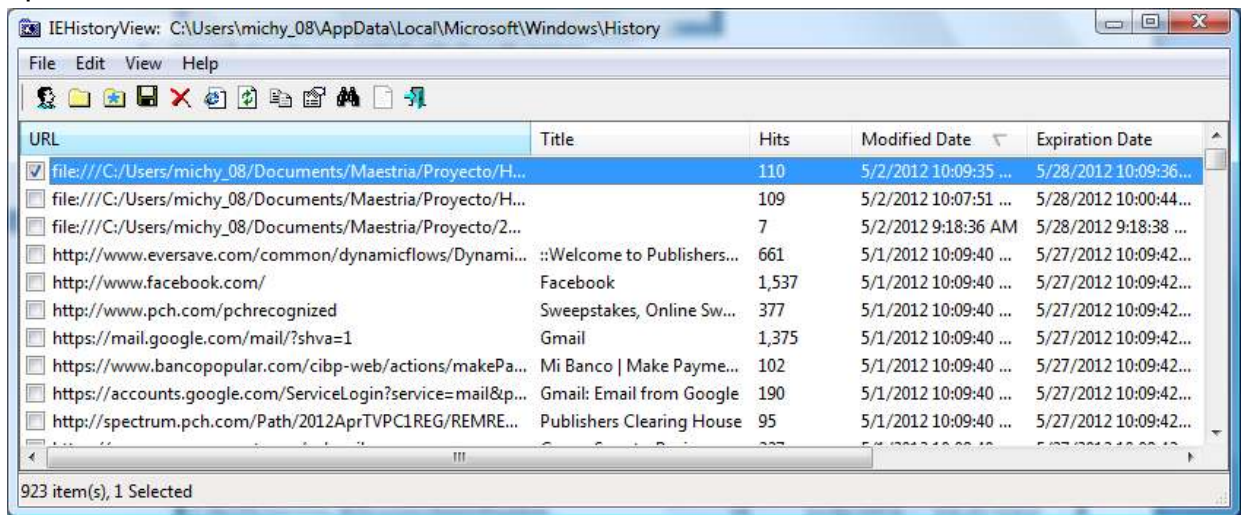


3. You will then be presented with the URL history



4. Notice the menu at the top of the URL history window. You may access the options either from the top bar containing drop down menus or the picture menu found just beneath it. When you select one of more of the URLs by checking the

checkbox at the left of each URL additional options will be habilitated. You may delete the URL, save it to a file or create a link to the URL to name a few of the options.



## Part D – Internet Explorer Cookie Viewer

IECookiesView is a small utility that displays the details of all cookies that Internet Explorer stores on your computer. In addition, it allows you to do the following actions:

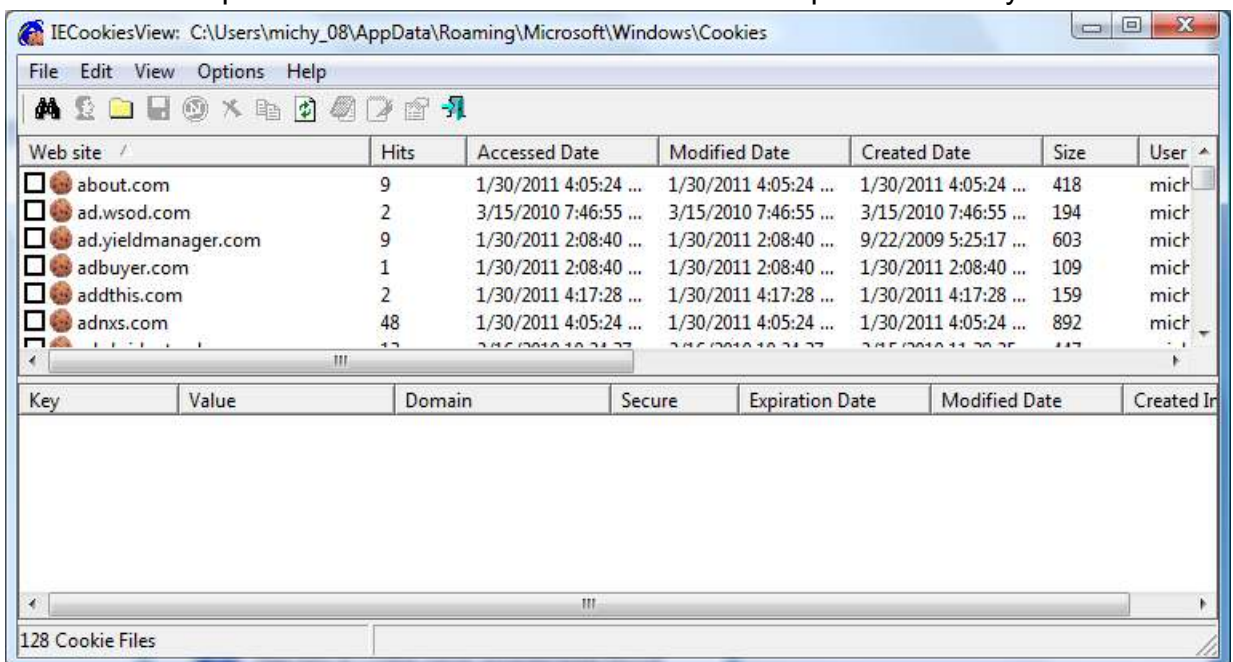
- Sort the cookies list by any column you want, by clicking the column header. A second click sorts the column in descending order.
- Find a cookie in the list by specifying the name of the Web site.
- Select and delete the unwanted cookies.
- Save the cookies to a readable text file.
- Copy cookie information into the clipboard.
- Automatically refresh the cookies list when a Web site sends you a cookie.
- Display the cookies of other users and from other computers.



1. Click on the icon **IE Cookie Viewer**
2. You will be presented with a confirmation message, click "Yes" to proceed.



3. A window will open with the cookies found for Internet Explorer in the system.



4. Many of the options that were available for the Internet Explorers URLs are available for the cookies. Delete, save, open, etc. Feel free to play with them.
5. You also have the Mozilla Cookie Viewer; it works similarly to IE cookie viewer. Follow the same steps with the only difference that you start by pressing this icon



## Laboratory 4 – Scan for pictures of a live system.

This tool allows the investigator to quickly scan the system to see if there are any suspicious graphic images on the suspect system. Many different graphic formats are recognized, and displayed as thumbnails. Use example: This allows a parole officer to preview a system for graphic images that may violate a parole.

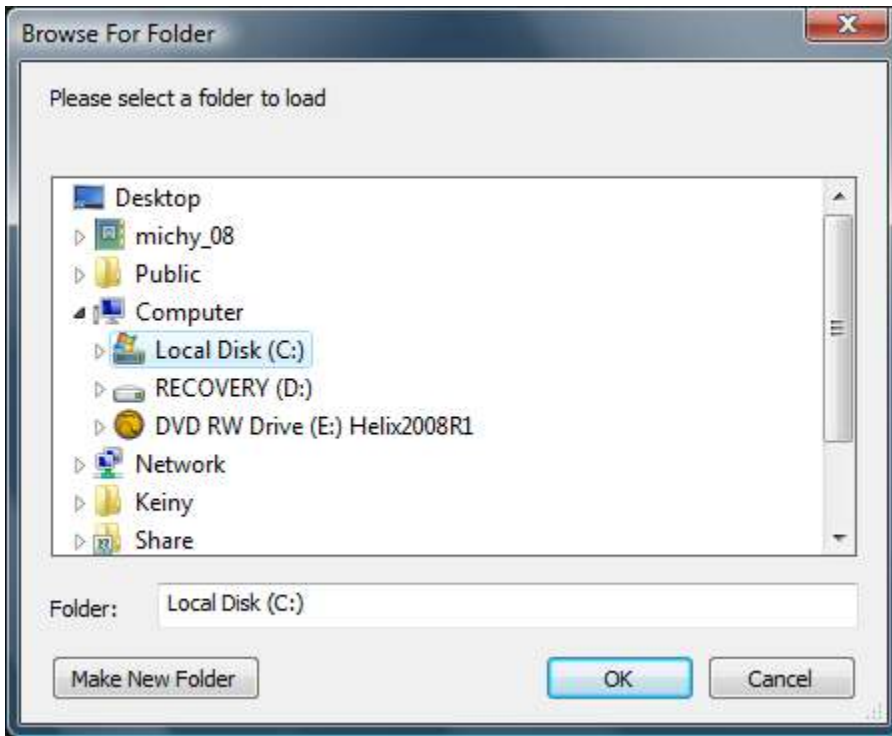


**Scan for Pictures from a live system**

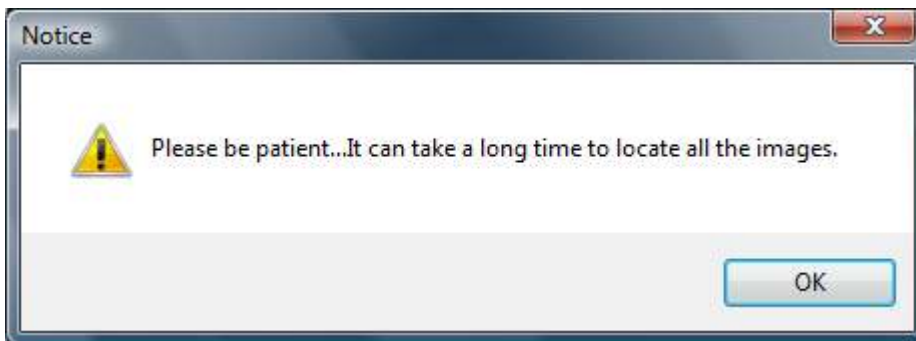
1. Select the scan for pictures icon
2. You will see the following screen



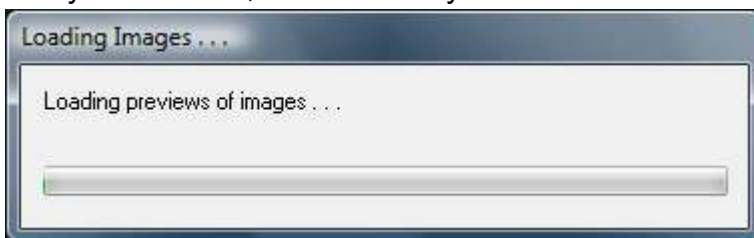
3. Notice there is a menu at the bottom of the window in light grey. Click on the "Load Folder" option and select the desired drive to scan.



4. Be aware that depending on the size of the drive, the amount of memory and the speed of the system, this could take a while. A reminder window will pop up; press the “OK” button in order for the process to continue.



After you press the “OK” button it may seem like nothing is happening, don’t worry. Let it work, after a while you should see the following screen.






Once the scan is complete you will be able to view the images recovered



Double clicking on any thumbnail will open the image in the local viewer. Be advised that this application will change the last access time on just about every file in the system, since it examines the file headers to determine if the file is graphic.

## Laboratory 5 – Exiting Helix

There are several ways to exit the Helix application.

1. File / Exit from the menu bar – This will prompt an offer to save a PDF of your transactions.
2. Click on the close windows button  – This will also an offer to save a PDF of your transactions.
3. Right –click on the Helix icon in the system tray – This will **NOT** save your transactions.

The first to exit options will save a copy of all your transactions if you will, while the last option will not. If you choose to save the output, you will be prompted in order to determine where the file will be saved. The file should be saved on a network share or on a removable evidence collection drive to prevent any contamination of the suspect computer. The default file name is Helix\_Audit\_Log.pdf

File example:

```

      HELIXTM
Incident Response · Electronic Discovery · Computer Forensics
Helix Version: 2009R1
-----
Helix Started on: 04/30/2012 at 19:58:45
-----
----- SYSTEM INFORMATION -----
Operating System:Windows XP Service Pack 2
Operating System Version: 5.1.2600
User Information:
Owner: Obed
Organization:
Admin: No
Admin Rights: Yes
Network Information:
Host: VICTIMA-01
User: Administrator
IP: 192.168.126.128
NIC: 000c292cd7ec
Domain:
Detected Drives:
A:\ (Removable drive)
C:\ (Logical drive)
D:\ (CD/DVD-ROM drive)
-----
19:58:46 - Helix displayed the Incident Response page 1.
19:58:49 - Helix displayed the Incident Response page 2.
19:58:53 - The RootKit Revealer was executed successfully.
20:02:44 - The PC Inspector File Recovery utility was executed successfully.
20:04:18 - Helix displayed the Browse Contents page.
20:04:39 - Helix displayed the Scan for Pictures page.

##### INVESTIGATIVE NOTES #####
#####

-----
Helix Stopped on: 05/03/2012 at 20:04:46
-----
```