Helix 1.7 for Beginners
by BJ Gleason and Drew Fahey

HelixManual@gmail.com
# Table of Content

**Introduction** ........................................................................................................ 4
  Thanks .................................................................................................................. 4
  Revision History .................................................................................................... 5

**Advice to Beginners** .......................................................................................... 6

**Helix** .................................................................................................................. 7
  What is Helix? ......................................................................................................... 7
  Why Helix Different .............................................................................................. 7
  Operating Modes .................................................................................................. 7
  The Windows Side ................................................................................................ 8
  The Linux Side ...................................................................................................... 9

**Helix Main Screen (Windows Side)** .................................................................. 11
  Preview System Information ................................................................................. 15
  Acquire a “live” image of a Windows System using dd ....................................... 18
    Using dd ............................................................................................................. 18
    FTK Imager ......................................................................................................... 20
  Incident Response tools for Windows Systems ................................................... 22
    Windows Forensic Toolchest (WFT) ................................................................. 24
    Incident Response Collection Report (IRCR2) ................................................ 27
    First Responder’s Evidence Disk (FRED) ....................................................... 29
    First Responder Utility (FRU) ......................................................................... 32
    SecReport ......................................................................................................... 35
    Md5 Generator .................................................................................................. 38
    Command Shell ................................................................................................. 40
    Rootkit Revealer ............................................................................................... 41
    File Recovery ..................................................................................................... 45
    File Recovery ..................................................................................................... 45
    PuTTY SSH ........................................................................................................ 50
    Screen Capture .................................................................................................. 51
    Messenger Password ......................................................................................... 52
    Mail Password Viewer ....................................................................................... 54
    Protect Storage Viewer ..................................................................................... 55
    Network Password Viewer ............................................................................... 57
    Registry Viewer ................................................................................................. 58
    IE History Viewer .............................................................................................. 60
    Asterisk Logger ................................................................................................... 61
    IE Cookie Viewer ............................................................................................... 62
    Mozilla Cookie Viewer ...................................................................................... 63
    Chain of Custody ............................................................................................... 64
    Preservation of Digital Evidence ...................................................................... 66
    Linux Forensic Guide for Beginners ............................................................... 66
    Forensic Examination of Digital Evidence ..................................................... 67

**Browse contents of the CD-ROM and Host** .................................................... 68

**Scan for Pictures from a live system** ................................................................. 70

**Exiting Helix** ..................................................................................................... 72

**Bootable Helix (Linux Side)** ............................................................................. 73
Introduction

e-fense, Inc. developed Helix as an internal tool to provide the ability to acquire forensically sound images of many types of hard drives and partitions on systems running unique setups such as RAID arrays. It quickly grew to include many open source, and some closed source, tools for the forensic investigators at e-fense, and became the internal standard to image “live” systems as well as systems running RAID setups. This enabled us to easily deal with the issue in the corporate world that some systems could never be taken off-line to do a more traditional forensic acquisition. Since most corporate systems run Microsoft Windows, we developed a Windows functionality to facilitate the capture of live Windows systems’ volatile data, as well as to conduct a forensic acquisition while the system remained on-line.

Helix was first publicly released on 23 Nov 2003. Its popularity grew quickly, and Rob Lee started using it at SANS to teach the forensics track. Helix has been going strong ever since and has been downloaded countless times. Many Government agencies and Law Enforcement community across the globe have turned to Helix as their forensic acquisition standard due to its functionality and cost effectiveness (who can beat FREE)! The National White Collar Crime Center (NW3C) has chosen to use Helix to teach Law Enforcement Linux forensics on bootable Cd’s.

The name Helix was chosen for no particular reason other than it fit with the sound of the name Linux. Also since forensics is a science the helix dna symbol seemed to apply. So Helix was born.

Helix is a work in progress and is not meant to be used by individuals without proper incident response and/or forensics training. While many complex commands are simplified with a GUI interface, it is the responsibility of the end user to know what these commands are doing so that you don’t inadvertently delete evidence, of so if called upon to testify, you don’t look like an idiot when you can’t explain your actions on the witness stand.

Helix is released under the terms of the GNU General Public License, version 2. Helix is distributed as is WITHOUT ANY WARRANTY; without the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Thanks

This manual is a compilation of many sources. While most of this information can be found in other locations on the Internet, I wanted to pull them al together into a single reference manual for my students, and for anyone else who is interested in learning more about computer forensics.

The list of people who belong on this list is probably incomplete. If you think someone is missing, or if I have misidentified someone, please let me know…

Drew Fahey – Creator of Helix and the Helix Handbook
Klaus Knopper – Creator of Knoppix
Nirsoft – developers of many of the windows based tools
Jesse Kornblum, Harlan Carvey, Kevin Mandia, Chris Prosise, Matt Pepe, Brian Carrier

And to the countless others who have contributed their time and efforts developing these tools.
Dear Helix User:

Thank you for taking the time to read this document. This is a work in progress, and hopefully, you will find it useful.

As Helix is being updated, this manual will be updated. There are several things that are not quite completed yet, but hopefully they will be in the next few revisions.

If you have something you would like to contribute to this documentation project, or if you have any suggestions, corrections, compliments or complaints, please send them to me at HelixManual@gmail.com. Please include the version number of the manual from the cover of the document, and any related page numbers.

While I could work on this forever, and never have it quite the way I want it, there comes a time in which you can not procrastinate any longer and have to get it out the door. So for the near future, I plan to release an update of the manual on the 1st of each month while all the kinks are being worked out.

Some of the upcoming updates include:

- Add references and sources
- Update the Linux Side to reflect version 1.7
- Add more hands-on labs to allow users to practice and refine their skills

I have learned so much from Helix, and from the many other forensic tools and websites that are out there. This is my contribution to give back a little of what I have taken.

I’m looking forward to hearing what you think of this manual.

Respectfully,

BJ Gleason
27 Dec 2005, Seoul, Korea
Advice to Beginners

Helix is a very powerful tool. But with great power comes great responsibility, and as a potential forensics investigator, it is your responsibility to learn how to use this tool properly. It is expected that if you have downloaded and created a bootable Helix disk, you have an interest in digital forensics.

But just as you can use a hammer to build a house, you can not build a house just using a hammer. To successfully build a house, you need architects, lawyers, construction workers, many tools, supplies, and inspectors. The same is true in the field of digital forensics. Before you exam any system, you need to make sure that you have permission to examine that system. You need to know the legal aspects of collection, documentation, and preservation of digital evidence. You need to know how to use the tools of the trade (such as those on the Helix CD).

Simple mistakes and good intentions can completely destroy digital evidence. It is strongly recommended that aspiring investigators learn about digital forensics, and practice on controlled systems before attempting to collect evidence from a real system.

Some recommended books on digital forensics include:


I would also recommend that you create a home lab in which to practice with these tools. I recommend 2 systems, running Windows 2000 or XP, with a network connection between them, either via a switch or a crossover cable. Since some of these tools transfer data via the network, make sure you disable any firewalls, such as the one built-in to XP service pack 2, which can interfere with network connections. I would label one machine as “Suspect”, and at the other as “Forensic”. To experiment with disk imaging, I would recommend having machines with floppy disks, and the suspect system should have a small hard drive (4 gig) or less, since copying larger drives over a network can take a very long time, and require a lot of space on the forensic system. For the forensic system, I would recommend having two hard drives (or at least two partitions) – one for the operating system, and one for the collected evidence.
Helix

What is Helix?

Helix is a customization of the standard Knoppix\(^1\) distribution. As such it owes everything to the work already done by Klaus Knopper and borrows heavily from work done by several individuals at [www.knoppix.net](http://www.knoppix.net). In fact, knoppix.net is the first place to go if you’re looking for information on how to customize. There are many other LiveCD distributions available that have been around longer than Helix, but many of them are no longer maintained or are not updated on a frequent enough basis. Many of the original ideas for Helix originated from these distributions: Knoppix, Knoppix-STD\(^2\), FIRE\(^3\), Morphix\(^4\), Insert\(^5\).

Why Helix Different

Helix is a heavily modified version of Knoppix. However, while there are many variants on the original Knoppix, Helix is different in that much of the code has been tweaked for forensic purposes. Some of the code has been compiled from scratch and it is a distribution dedicated strictly for incident response and forensics.

Some of the major changes Helix incorporated into Knoppix are:

1. Helix will NEVER use swap space found on a system - even if forced.
2. The Helix automounter will set up drives it finds but will force a mount point to be ro, noatime, noexec, nodev, noauto, user
3. Helix sees all the filesystems identified by Knoppix (ext2, ext3, vfat, ntfs), but will also see xfs, resier, and jfs and more.
4. Helix incorporates as many open source forensics/incident response tools that could be found.
5. Added capability for “Knock and Talks.” This feature allows a parole officer to preview a system for graphic images that may violate a parole.
7. Added an overlay file system to allow writes to the CD.
8. Updated at least every 3 months to keep current.

Operating Modes

Helix operates in two different modes – Windows and Linux.

Helix is a forensically sound bootable Linux environment much like Knoppix, but a whole lot more. The “other side” of Helix, a Microsoft Windows executable feature, contains approximately 90 MB of incident response tools for Windows. The rationale behind this was that a majority of incidents require interaction with a live Windows system, the dominant operating system in the computer market.

\(^1\) [http://www.knopper.net/knoppix/index-en.html](http://www.knopper.net/knoppix/index-en.html)  
\(^3\) [http://fire.dmzs.com/](http://fire.dmzs.com/)  
\(^5\) [http://www.inside-security.de/insert_en.html](http://www.inside-security.de/insert_en.html)
As such Helix was broken down into the live response side and the bootable Linux OS side.

Windows: In the Windows Mode, it runs as a standard windows application used to collect information from “live” (still turned on and logged in) Windows system. It should be noted, that when a target system is live, its state is constantly changing. Not matter what tools you use on a live system, you will disturb the state of the live system – even doing “nothing” changes the state of a live system, since it is still running the operating system. However, since turn off the system can result in the lost of potentially important forensics information, the tools can be used to collect volatile information. It can also be used to collect information off of systems that can not be turned off, such as servers and other critical resources that can not be turned off. Finally, the Windows side of Helix can be used a portable forensic environment since it provides access to many windows based forensic utilities.

Linux: In the Linux mode, it is a bootable, self-contained operating system that can be used for in-depth analysis of “dead” (powered-off) systems. When Helix boots, it runs entirely off the CD, and only mounts the hard drives in read-only mode, so they can not be modified. Aside from the standard Linux tools, this side includes numerous forensic analysis tools that can use to examine the target system.

The Windows Side

For a live response in any Windows environment, one can simply insert the Helix CD and “explore” the directories on the CD for the needed environment binaries. The binaries are static so they will run off the CD without any need for any additional libraries and or files. This makes a perfect trusted CD for an incident response where you cannot rely on the systems tools or programs.

The other option you have, at least in a Windows environment, is the Helix.exe. It will normally automatically load the menu if auto run is not disabled. Running Helix.exe or relying on auto run will bring up the Helix Windows environment in which several options become available. Of course these options are not new; a user could duplicate them manually. The Helix environment simply puts the options together in a forensically safe, easy to use, manner.

Let’s start by dissecting the live response side of Helix. The cornerstones of the live response side are the tools. Helix contains static binaries for Linux, Solaris, and Windows using GNU utilities and Cygwin tools. There are several other tools to include George Garners Forensic Acquisition Utilities suite, Sysinternal’s tools, Foundstone’s open source tools, the Windows Debugger, the Windows Forensic Toolchest, and many more. All of these tools have been tested and placed into Helix using a GUI.

The Helix GUI will only operate within a live Windows environment. It has been tested on Windows 98SE, Windows NT4, Windows 2000, and Windows XP. There are slight differences in running the Helix CD on each. The most important note to remember is that since Windows is required to run the above interface, many DLL files will be used by Helix from the operating system. This is not a problem however as long as you are aware of it. Some of the DLL files that will be used are shown in the table to the right.
These DLL files were not included on the CD because of the nature of the various versions of Windows. There is no way with the current build to have the Helix executable not access the built in Windows DLL files. The incident response / forensics tools included on the Helix CD are self sufficient - most of them will use their own libraries and not the libraries and/or file from the running system.

Helix can and will use other DLL files depending upon the system it is running. The other DLL files that are used are hooks into the specific hardware. So you must be aware of other files you may touch while using Helix in a live environment.

Some of the newer features in Helix on the Windows side include the ability for user input to some of the major tools like Windows Forensic Toolchest. Prior to Version 1.5 the input was static and could not be changed without remastering the Helix CD.

While many of the more common tools can be accessed via the Helix graphical user interface, many more tools can be accessed via a forensic command tool. Many of these tools are listed on the next page, however, since Helix is updated often, you can always check the /IR folder on the Helix CD to see what tools are included.

The Linux Side

One of the greatest benefits of Helix is the bootable environment. Helix will boot on all x86 architectures which make up a majority of the computers in the world. It is for this reason that Helix for the immediate future will remain on a CDROM. Almost every computer in the world has a CDROM, but most do not have DVD’s, etc. While derivatives like Helix USB will be forthcoming, it is most stable on the CD platform. Helix, like Knoppix, will boot into a self contained Linux environment. This environment has been tweaked for forensic purpose. While there are many distributions of Knoppix such as Knoppix-STD, Helix only concentrates on Incident Response and Forensics.

C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\comdlg32.dll
C:\WINDOWS\system32\CRYPT32.dll
C:\WINDOWS\system32\DNSAPI.dll
C:\WINDOWS\system32\dsound.dll
C:\WINDOWS\system32\GDI32.dll
C:\WINDOWS\system32\IMAGEHLP.dll
C:\WINDOWS\system32\Kernel32.dll
C:\WINDOWS\system32\Ksuser.dll
C:\WINDOWS\system32\midimap.dll
C:\WINDOWS\system32\MSACM32.dll
C:\WINDOWS\system32\msacm32.drv
C:\WINDOWS\system32\MSASN1.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\mslcbui.dll
C:\WINDOWS\system32\msvcr71.dll
C:\WINDOWS\system32\OLEAUT32.dll
C:\WINDOWS\system32\oledlg.dll
C:\WINDOWS\system32\OLEPRO32.DLL
C:\WINDOWS\system32\RASADHLP.dll
C:\WINDOWS\system32\RPCRT4.dll
C:\WINDOWS\system32\Secur32.dll
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\SHLWAPI.dll
C:\WINDOWS\system32\USER32.dll
C:\WINDOWS\system32\uxtheme.dll
C:\WINDOWS\system32\VERSION.dll
C:\WINDOWS\system32\wdmaud.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\WINPSPOOL.DRV
C:\WINDOWS\system32\WINTRUST.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\WSHELP.dll
C:\WINDOWS\system32\WSOCX52.dll
### Helix Tools

**DRIVE ACQUISITION:**

- **CYGWIN Tools:** (dd, md5sum, shasum, tee, split)
- **FAU by George Garner:** (dd, nc, md5sum, volume-dump, wipe)
- **GNU Tools:** (dd, md5sum, shasum, tee, split)

**INCIDENT RESPONSE TOOLS:**

- Windows NT: (cmdnt.exe, doskey.exe, ipconfig.exe, ...)
- Windows 2000: (cmd2k.exe, doskey.exe, netstat.exe, net.exe, ...)
- Windows XP: (cmdxp.exe, doskey.exe, ipconfig.exe, ...)

**OTHER TOOLS:**

- Cygwin: (version 2.427)
- Somarsoft: (DUMPEVT, DUMPSEC, dumpreg)
- wft: (Version: v1.0.03 (2003.09.20) by Monty McDougal)
- getinfo: (Version: 3.02.10 by Alexander Kotkov)
- Microsoft Debugging Tools: (Version: 6.2)
- GNU-Win32 Static-Binaries
- Linux Static-Binaries
- Solaris Static-Binaries

### FOUNDSTONE’S OPEN SOURCE TOOLS:

<table>
<thead>
<tr>
<th>AFind</th>
<th>Audited</th>
<th>CIScan</th>
<th>DACLchk</th>
<th>DSScan</th>
<th>FPipe</th>
<th>FileStat</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFind</td>
<td>MessengerScan</td>
<td>MyDoomScanner</td>
<td>NetSchedScan</td>
<td>RPSScan2</td>
<td>SFind</td>
<td>SNScan</td>
</tr>
<tr>
<td>SQLScan</td>
<td>SuperScan4</td>
<td>Vision</td>
<td>attacker</td>
<td>bintext</td>
<td>bopping</td>
<td>ddosping</td>
</tr>
<tr>
<td>filewatch</td>
<td>galleta</td>
<td>pasco</td>
<td>rifiuti</td>
<td>showin</td>
<td>sl</td>
<td>trout</td>
</tr>
</tbody>
</table>

### SYSINTERNALS OPEN SOURCE TOOLS:

<table>
<thead>
<tr>
<th>AccessEnum</th>
<th>DiskView</th>
<th>EFSdump</th>
<th>Filemon</th>
<th>HOSTNAME</th>
<th>LogonSessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTPSINFO</td>
<td>Regmon</td>
<td>TDIMON</td>
<td>TOKENMON</td>
<td>Tcpview</td>
<td>authoruns</td>
</tr>
<tr>
<td>autoruns</td>
<td>livekd</td>
<td>proexp</td>
<td>psexec</td>
<td>psgetsid</td>
<td>pskill</td>
</tr>
<tr>
<td>psloglist</td>
<td>pspasswd</td>
<td>psshutdown</td>
<td>pssuspend</td>
<td>strings</td>
<td>tcpvcon</td>
</tr>
</tbody>
</table>

### NTSECURITY OPEN SOURCE TOOLS:

<table>
<thead>
<tr>
<th>browselst</th>
<th>dumpusers</th>
<th>efsview</th>
<th>etherchange</th>
<th>filehasher</th>
<th>gplist</th>
</tr>
</thead>
<tbody>
<tr>
<td>gsd</td>
<td>listmodules</td>
<td>lns</td>
<td>macmatch</td>
<td>periscope</td>
<td>pmdump</td>
</tr>
<tr>
<td>promiscdetect</td>
<td>pstoreview</td>
<td>wino</td>
<td>winrelay</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### PERL TOOLS BY HARLEN CARVEY:

<table>
<thead>
<tr>
<th>ads</th>
<th>bho</th>
<th>finfo</th>
<th>keytime</th>
<th>rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>share</td>
<td>sigs</td>
<td>ver</td>
<td>windata</td>
</tr>
</tbody>
</table>
Helix Main Screen (Windows Side)

Helix operates in two modes, a Windows side, and a bootable Linux environment. The windows side can be used to perform a preliminary evaluation to see if there is any that warrants further investigation of the system. It can also be used to capture system that can not be turn off or taken offline for the extended periods of time it take to perform a forensic duplication.

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 can not be taken offline.

Booting the Windows Side

If the CD autorun features is enabled (which is the Windows default), a Helix license Window should appear. If autorun is disabled, you can run Helix by double clicking on the helix.exe file on the CD.

The user can select the default language that Helix will use via the drop-down box. English is the default, but French and German are also available.
To use Helix, you should read the agreement and then press “I Agree” to continue. Once the user accepts the agreement, the main screen will appear.

Users can select any of these options by clicking on the associated icons.

This Main screen doesn’t behave as a standard window – it doesn’t show up in the taskbar, and you can not 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.

The main screen provides examiners with six main options to examine the system under investigation. These options are described below.
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.

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.

Incident Response tools for Windows Systems
This option provides access to 20 tools, all of which can be run directly from the CDROM. Once your 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.

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.

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 can not be prevented. This is one of the problems with examining a live system – the investigator’s actions may modify the system.

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.

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
Page – Allows the user to jump directly to any of the utility screens
Help – Displays information about the program, and the license agreement.

Note: Since these tools run directly off the CDROM, and most CDROM spin down when not in use, when you click on an icon, it may take a moment for the CDROM to spin up before there is a response from the application.
Note: All the tools run at the same level as the current logged in user. Normal users may have many restrictions on them that prevent some of these tools from running. Accessing the system using the Administrator account will provide the most access.
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 if the current user has administrator privileges.
- “NIC:” is the MAC access 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 (such as A:\, E:\, and G:\ in the example above) typically indicate removable drives with no media inserted.

Clicking on the small triangle next to the Preview Icon 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.
FAQ: Why don’t we just use the built in “task manager” to display this information? If the system has been hijacked by a rootkit, 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 can not be modified, and should be able to display all the programs currently running on the system.
Acquire a “live” image of a Windows System using dd

There are two tools provided to make images of physical memory or disk drives. One the first page, there is a graphical front-end to the command line version of dd, a common disk duplication utility. On the second page, the investigator has access to the FTK Imager from AccessData. Clicking on the small triangle next to the Acquisition Icon will display the FTK Imager. Clicking on the triangle will flip the between the two image acquisition tools.

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, or a network drive. The image name is the user chosen name, and the standard extension is “.dd”.

The Options include:

- Netbios/Local: check this option to save the image to a local drive, or a network share.
- NetCat: check this option to transfer the image to a netcat server located on the network. With this option you will need to specify the IP address and port number of the netcat 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 2 gig file size limitation.

Once you enter all the parameters, and press the “Start” 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 floppy 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.
FTK Imager

From the FTK help topics, “FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with AccessData® Forensic Toolkit® (FTK™) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence.

With FTK Imager, 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 “Start Imager” to launch the actual application.
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.
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.

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
The Windows Forensic Toolchest (WFT) was written by Monty McDougal. It is available from http://www.foolmoon.net/security/wft/index.html

From the website: The Windows Forensic Toolchest (WFT) was written to provide an automated incident response [or even an audit] on a Windows system and collect security-relevant information from the system. It is essentially a forensically enhanced batch processing shell capable of running other security tools and producing HTML based reports in a forensically sound manner. A knowledgeable security person can use it to help look for signs of an incident (when used in conjunction with the appropriate tools). WFT is designed to produce output that is useful to the user, but is also appropriate for use in court proceedings. It provides extensive logging of all its actions along with computing the MD5 checksums along the way to ensure that its output is verifiable. The primary benefit of using WFT to perform incident responses is that it provides a simplified way of scripting such responses using a sound methodology for data collection.

When the WFT program is started, it will prompt for an output folder. The investigator should point to a folder on removable media (floppy, zip, USB device), or a shared folder on the network to prevent the tool from modifying the suspect drive.

Once the folder is selected, the program will prompt the user if they want to run some detailed collection utilities? These can take up to an hour or more to run, depending on the system of the system, the amount of RAM, and many other factors.

Next the program will ask if the user wants to run some programs that can write information to the suspect’s system. These tools can compromise the integrity of the system, so this option should be used with care.

Finally, the program will display the command and ask for conformation.
Once the user clicks “Yes”, a command tool will open, and the collection process will start. Depending on the options selected, this collection process can take anywhere from a few minutes to a few hours.

Once the collection is finished, the user will be returned to the Helix program. If the user examines the destination folder, there is a now a file “index.html”. This file can be examined with a browser of your choice. To prevent addition contamination of the suspect system, it should be viewed on another system.

A sample output is shown below.

The output can be navigated use the highlight hyperlinks. WFT produces an impressive collection of information from the system. In addition, the LOG tab shows the commands that were executed, and the CONFIG tab shows the WFT configuration file.

From the website: Windows Forensic Toolchest (WFT) was designed to be useful both for a security administrator and as a tool to be used in a court of law. One of the biggest issues involved in a court case is ensuring that you have an adequate record of all the actions that you have taken. It is also necessary to have the appropriate safeguards in place to ensure that the data being presented has not been altered.

WFT seeks to meet both of these requirements. One of the most important features of WFT is the fact that it logs every action it takes as part of running commands.

An investigator using Windows Forensic Toolchest (WFT) would need some level of knowledge to interpret the data produced by running it. If the configuration file is used properly, then WFT is self documenting to some degree as each HTML report produced will have the Description of the tool
as part of its output. Ultimately, the investigator needs to have a working knowledge of the tools that are being invoked via WFT to be able to interpret its output. WFT's primary benefit to the investigator is its ability to provide a scripted, automated response while promoting forensic integrity and detailed logging.

Windows Forensic Toolchest (WFT) provides output in two data formats. Each of these serves a specific purpose as described below.

The first and more useful format is HTML output. Opening the index.htm file produced by WFT provides an easy to read and easy to navigate interface to the output of the various tools invoked via WFT. Each of the reports produced under WFT includes the MD5 checksum for the binary being run, the exact command line issued to generate the output, a description of the tool, and the output produced by the tool along with the MD5 checksum associated with the output. The HTML reports are designed to be self-documenting via the text provided in the configuration file.

The second type of output produced by WFT is the raw text output from the tools. This format allows the viewer to see the output of the individual command exactly as it was produced. It is generally a bad idea to, in any way, manipulate data being used as evidence in a court of law. WFT seeks to preserve the original data while providing a user-friendlier HTML version for viewing. The MD5 checksums produced for each of the output files during collection provides a safeguard to ensure the output can be verified at a later date.
Incident Response Collection Report (IRCR2)


From the readme file: The Incident Response Collection Report is a script to call a collection of tools that gathers and/or analyzes data on a Microsoft Windows system. You can think of this as a snapshot of the system in the past. Most of the tools are oriented towards data collection rather than analysis. The idea of IRCR is that anyone could run the tool and send the output to a skilled computer security professional for further analysis.

To prevent the suspect system from being modified, this tool sends the output to a listener system that is connected via a network connection. On the listener system, you need to run netcat. For this example, we have executed the command on a machine with the IP address of 192.168.1.2:

```
nc -l -p 8888 > IRCR2OutputReport.txt
```

On the suspect system, when the IRCR2 program is started, it will prompt the user for the address of the listener system.

Next, it will ask for the port of the listener.

Finally, it will show the command and ask for confirmation.
Depending on the speed of the system and the speed of the network, this program can take a while to run. It is not unusual for the program to generate several errors. Once the program is finished, the output file will contain a detailed report of the suspect system.

Sample Output File

```plaintext
Incident Response Collection Report

Name:
Computer Name: tal_mc
OS: Microsoft Windows XP [Version 5.1.2600]

START -- Time: 21:30:47.45 Date: Mon 12/12/2005

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT Schedule List</td>
<td>There are no entries in the list.</td>
</tr>
<tr>
<td>doskey /history</td>
<td>MS-DOS history list</td>
</tr>
<tr>
<td>ipconfig /all</td>
<td>Displays configuration information</td>
</tr>
</tbody>
</table>

Windows IP Configuration
Host Name . . . . . . . : tal_mc
Primary Dns Suffix . . . . . : 
Node Type . . . . . . . . : Mixed
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix : VMware Virtual Ethernet Adapter for VMnet8
Description . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Physical Address . . . . . . . : 00-50-56-C0-00-08
Dhcp Enabled. . . . . . . . . : No
IP Address . . . . . . . . . : 192.168.95.1
Subnet Mask . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . : 

MEM.exe /d
Displays memory usage

<table>
<thead>
<tr>
<th>Address</th>
<th>Name</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td></td>
<td>000400</td>
<td>Interrupt Vector</td>
</tr>
<tr>
<td>000400</td>
<td></td>
<td>000100</td>
<td>ROM Communication Area</td>
</tr>
<tr>
<td>000500</td>
<td></td>
<td>000200</td>
<td>DOS Communication Area</td>
</tr>
<tr>
<td>000700</td>
<td>IO</td>
<td>000370</td>
<td>System Data</td>
</tr>
<tr>
<td>CON</td>
<td></td>
<td></td>
<td>System Device Driver</td>
</tr>
<tr>
<td>AUX</td>
<td></td>
<td></td>
<td>System Device Driver</td>
</tr>
<tr>
<td>PRN</td>
<td></td>
<td></td>
<td>System Device Driver</td>
</tr>
</tbody>
</table>
```
First Responder’s Evidence Disk (FRED)

Written by Special Agent Jesse Kornblum of the Special Investigations Office of the United States Air Force. For more information on his work, see http://research.jessekornblum.com/

FRED is the First Responder’s Evidence Disk. This MS/DOS batch file will collect a large amount of information from the system and store it in a text file.

There are 3 icons available for FRED that determine where the output file will be located. The three icons indicate: Floppy, Netcat and Other Storage Device.

Output to Floppy

If the suspect system has a floppy drive, the first icon will write the information to a floppy disk.

If the user clicks “Yes”, two files will be created on the floppy disk. The output of the report will be in a:\audit.txt, and the MD5 signature of the audit.txt file will be in the a:\audit.MD5.

Output via NetCat

The second icon will transmitted the output via netcat to another system. This is useful if the system is connected to a network, and doesn’t have a floppy disk. On the listener system, you need to run netcat. For this example, we have executed the command on a machine with the IP address of 192.168.1.2:

nc -l -p 8888 > FREDOutputReport.txt

On the suspect system, when the F.R.E.D. program is started, it will prompt the user for the address of the listener system.

Next, it will ask for the port of the listener.
Finally, it will show the command and ask for confirmation.

Once the program is finished, press <CTRL>-C on the listener system. The output file will contain a detailed report of the suspect system.

Unlike the other two options, this option will not automatically create a MD5 file for the output. You should now run the md5sum on the acquired audit log, and save that number. Do not modify the original file, since that will change the MD5 signature. It is recommended that the MD5 is written down on the evidence tag for the floppy.

Output to Other Storage Device

Finally, the third icon will allow the user to select the output folder. It is recommended that the output be send to a removable drive, or a network share. The output should not be written to the suspect’s system, as this can compromise the integrity of the system.

The program will confirm the output directory.
The program will then confirm the command.

If the user clicks “Yes”, two files will be created in the destination folder. The output of the report will be in audit.txt, and the MD5 signature of the audit.txt file will be in the audit.MD5.

Sample Output File

FRED v1.4 - 6 October 2005 [modified for HELIX 10/2005]
=================================================================
START TIME
=================================================================
Time: 21:52:54.84 Date: Mon 12/12/2005
=================================================================
PSINFO
=================================================================
System information for \TAL_MC:
Uptime: 12 days 23 hours 21 minutes 22 seconds
Kernel version: Microsoft Windows XP, Multiprocessor Free
Product type: Professional
Product version: 5.1
Service pack: 1a
Kernel build number: 2600
Registered organization:
Registered owner:
Install date: 12/22/2004, 6:54:16 AM
Activation status: Activated
IE version: 6.0000
System root: C:\WINDOWS
Processors: 2
Processor speed: 3.2 GHz
Processor type: Intel(R) Pentium(R) 4 CPU
Physical memory: 1536 MB
Video driver: Intel(R) 82845G/GL/GE/PE/GV Graphics Controller
=================================================================
NET ACCOUNTS
=================================================================
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 42
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.
=================================================================
NET SHARE
=================================================================
<table>
<thead>
<tr>
<th>Share name</th>
<th>Resource</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC$</td>
<td></td>
<td>Remote IPC</td>
</tr>
<tr>
<td>D$</td>
<td>D:\</td>
<td>Default share</td>
</tr>
<tr>
<td>C$</td>
<td>C:\</td>
<td>Default share</td>
</tr>
<tr>
<td>F$</td>
<td>F:\</td>
<td>Default share</td>
</tr>
<tr>
<td>ADMIN$</td>
<td>C:\WINDOWS</td>
<td>Remote Admin</td>
</tr>
<tr>
<td>R$</td>
<td>F:\</td>
<td>Default share</td>
</tr>
</tbody>
</table>
First Responder Utility (FRU)


From the website: The First Responder Utility (FRU) is used by a first responder to retrieve volatile data from "victim" systems. The current version of the FRU is a CLI (command line interface) tool called FRUC. The FRUC operates using a combination of an INI file and command line options.

To prevent the suspect system from being modified, this tool sends the output to a listener system that is connected via a network connection. On the listener system, you need to run netcat. For this example, we have executed the command on a machine with the IP address of 192.168.1.2:

```
nc -l -p 8888 > FRUOutputReport.txt
```

On the suspect system, when the FRU program is started, it will prompt the user for the address of the listener system.

Next, it will ask for the port of the listener.

It will then ask you the location of the fruc.ini file. The user should select the default file, unless they have created their own fruc.ini file.
Finally, it will show the command and ask for confirmation.

```
fruc.exe -s 192.168.1.2 -p 8888 -f "F:\IR\FSP\fruc.ini"
```

Once the user clicks “Yes”, the command will be placed into the clipboard.

When the command shell opens, the user should right-click inside of it, and select Paste to insert the command into the command shell.
Pressing Enter will execute the command.

Once the program is finished, press <CTRL>-C on the listener system. The output file will contain a detailed report of the suspect system.

You should now run the md5sum on the output file, and save that number. Do not modify the original file, since that will change the MD5 signature. It is recommended that the MD5 is written down on the evidence tag for the floppy.
SecReport

SecReport is a freeware tool available from http://members.verizon.net/~vze3vkmg/index.htm.

From the website: It is a small suite of two command-line tools for collecting security-related information from Windows-based system (SecReport) and comparing any two reports either from any two systems or from same system after some time (Delta). I use these tools to quickly assess level of securing of Windows system and to compare results to baseline. The tools are useful both in daily security administration and during incident response - for fast collection of information. Tools do not need to be installed on system and can be run directly from hard or CD-R disk or network drive (mapped or UNC). Format of reports - XML. Reports can be viewed with IE 6.0 browser. MD5 hash file for report automatically created.

Supported platforms: Windows 2000, XP, 2003 - full support; NT4 (SP6 or later) - limited support

Helix provides the investigator with a graphical front end for the application. Clicking on the SecReport Icon generate the following window:

The output should be directed to removable media to prevent contamination of the suspect’s system. Enter the drive name and click OK.

Information on hotfixes requires a fast connection to the Internet. The default is No. Click OK to continue. The confirmation prompt will show the command and its parameters.
Clicking YES will open a command shell, which will execute the command. After a few minutes, the program will complete and prompt the user to press any key to continue.

Pressing any key will close the window. The investigator will find two output files at the specified location. securityreport.xsl is the stylesheet for the report, and machinename_date.xml file. Double clicking on the .xml file will open the report in Internet Explorer.

This report goes on for several pages, detailing the following information:

- Network Configuration
- Audit Policy
- Event Log Configuration
- Services
- Applications
- Hotfixes
- Ports Open
- Page File Settings
- Hardware
- Processors
- Fixed Disks
- Mixed Checkpoints
Security Report TAL_MC

Hostname: TAL_MC
Date and time of report: 2005-10-03, 11:12, (GMT+09:00)
Operating System: Microsoft Windows XP Professional 5.1.2600
Service Pack: 1.0
Server Domain: MLC
Server Role: Standalone Workstation
IE Version: 6.0.2600.1106
Media Player Version: 8.0.0.4490
WSH Version: 5.6

Network Configuration
NIC Brand and Model: Intel(R) PRO/1000 MTW Network Connection - Packet Scheduler Miniport
IP Address: 192.168.1.100
Gateway: 192.168.1.1
DNS Server: 144.0.0.44
DNS Server: 143.0.0.44
DNS Server: 142.0.0.44
MAC Address: 23EB:1F:96:23:EB

Audit Policy
Policy
Account Logon
Account Management
Directory Service Access
Logon
Object Access
Policy Change
Privilege Use
Process Tracking
System

Security setting
No
No
No
No
No
No
No
No
No

Event Log configuration
Log Name
Application
Security
System
Max Size (KB)
512
512
512
Overwrite Old Events
7
7
7
Overwrite Policy
Outdated
Outdated
Outdated

Services
Total number of services: 94, Number of Running services: 49, Number of Automatic services: 42, Number of Manual services: 48
Service
Start Type
Status
Service full name
Account
Md5 Generator

On page 2 of the Incident Response tools, you will see an input box that will allow you to generate the MD5 signature of any file.

Start by pressing the button “…”. This will bring up a file manager that you can use to select a file.
Select a file, and once it has been listed in the “FILE:” textbox, the user can click on the “HASH” button to generate the MD5 of the file.
Command Shell

This is a forensically sound command shell, which means runs only trusted, non-compromised, binaries that are included on the CD.

All the standard commands are available, as well as access to the command line versions of many of the forensics tools included on the CD. The path command will show all the directories that are searched to find the command.

Since several directories can contain commands with the same name, if the user wants a specific command, they should specify the entire path to the specific command.

```
22:32:49.43 I:\IR> path
PATH=I:\IR\FAU\;I:\IR\Cygwin\;I:\IR\bin\;I:\IR\WFT\;I:\IR\IRCR\;I:\IR\unxutils\;I:\IR\sysInternals\;I:\IR\Microsoft\;I:\IR\SystemTools\;I:\IR\ntsecurity\;I:\IR\perl\;I:\IR\Foundstone\;I:\IR\2k\;I:\IR\2k3\;I:\IR\FSP\;I:\IR\nt\;I:\IR\xp\;I:\IR\shells\;I:\IR\nirsoft\;I:\IR\windbg

22:32:53.43 I:\IR>
```
Rootkit Revealer

This is a freeware tool from SysInternals (http://www.sysinternals.com/Utilities/RootkitRevealer.html). According to the website, “It runs on Windows NT 4 and higher and its output lists Registry and file system API discrepancies that may indicate the presence of a user-mode or kernel-mode rootkit. RootkitRevealer successfully detects all persistent rootkits published at www.rootkit.com, including AFX, Vanquish and HackerDefender.”

What is a rootkit? It is a series of malware applications that replace the standard windows utilities with Trojan horse programs, in an attempt to take over your system. This rootkits modify the operating system so that it can successfully hide and avoid traditional means of detection. For example, it may modify the Windows Explorer and DIR commands so the user will not be able to see the directory the rootkit is installed in. In addition, the rootkits open up backdoors to the system to allow the remote control of the system for sending out spam, launching denial-of-service attacks, or for pirating software.

For more information on rootkits, see www.rootkit.com and Microsoft’s page on rootkit research research.microsoft.com/rootkit/.

To run the application, click on the rootkit revealer icon. At the confirmation window, click Yes to run the program. The main scanning windows will appear.
As with many other tools, this program will only run at the level of the currently logged in user. It would be best to run this as the system administrator for the most accurate results. Below is an example of the program detecting the HackerDefender rootkit (from the Sysinternals website).

When the scan is completed, the output can be saved to a file using the File / Save as option. To interpret the output, the following information is taken from the sysinternals website.

Hidden from Windows API.

These discrepancies are the ones exhibited by most rootkits, however, if you haven't checked the Hide NTFS metadata files you should expect to see a number of such entries on any NTFS volume since NTFS hides its metadata files, such as $MFT and $Secure, from the Windows API. The metadata files present on NTFS volumes varies by version of NTFS and the NTFS features that have been enabled on the volume. There are also antivirus products, such as Kaspersky Antivirus, that use rootkit techniques to hide data they store in NTFS alternate data streams. If you are running such a virus scanner you'll see a Hidden from Windows API discrepancy for an alternate data stream on every NTFS file. RootkitRevealer does not support output filters because rootkits can take advantage of any filtering. Finally, if a file is deleted during a scan you may also see this discrepancy.

This is a list of NTFS metadata files defined as of Windows Server 2003:

- $AttrDef
- $BadClus
- $BadClus:$Bad
- $BitMap
- $Boot
- $LogFile
- $Mft
- $MftMirr
- $Secure
- $UpCase
• $Volume
• $Extend
• $Extend$Reparse
• $Extend$ObjId
• $Extend$UsnJrnl
• $Extend$UsnJrnl:$Max
• $Extend$Quota

Access is Denied.

RootkitRevealer should never report this discrepancy since it uses mechanisms that allow it to access any file, directory, or registry key on a system.

Visible in Windows API, directory index, but not in MFT.
Visible in Windows API, but not in MFT or directory index.
Visible in Windows API, MFT, but not in directory index.
Visible in directory index, but not Windows API or MFT.

A file system scan consists of three components: the Windows API, the NTFS Master File Table (MFT), and the NTFS on-disk directory index structures. These discrepancies indicate that a file appears in only one or two of the scans. A common reason is that a file is either created or deleted during the scans. This is an example of RootkitRevealer’s discrepancy report for a file created during the scanning:

C:\newfile.txt
3/1/2005 5:26 PM
8 bytes
Visible in Windows API, but not in MFT or directory index.

Windows API length not consistent with raw hive data.

Rootkits can attempt to hide themselves by misrepresenting the size of a Registry value so that its contents aren’t visible to the Windows API. You should examine any such discrepancy, though it may also appear as a result of Registry values that change during a scan.

Type mismatch between Windows API and raw hive data.

Registry values have a type, such as DWORD and REG_SZ, and this discrepancy notes that the type of a value as reported through the Windows API differs from that of the raw hive data. A rootkit can mask its data by storing it as a REG_BINARY value, for example, and making the Windows API believe it to be a REG_SZ value; if it stores a 0 at the start of the data the Windows API will not be able to access subsequent data.

Key name contains embedded nulls.

The Windows API treats key names as null-terminated strings whereas the kernel treats them as counted strings. Thus, it is possible to create Registry keys that are visible to the operating system, yet only partially visible to Registry tools like Regedit. The Reghide sample code at Sysinternals demonstrates this technique, which is used by both malware and rootkits to hide Registry data.

Data mismatch between Windows API and raw hive data.

This discrepancy will occur if a Registry value is updated while the Registry scan is in progress. Values that change frequently include timestamps such as the Microsoft SQL Server uptime value, shown below, and virus scanner "last
scan” values. You should investigate any reported value to ensure that it's a valid application or system Registry value.

HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\RECOVERYMANAGER\MSSQLServer\uptime_time_utc
3/1/2005 4:33 PM
8 bytes

This tool will only help find rootkits, and will not remove them. Depending on the nature of the investigation, the detection of the rootkit needs to be documented, and the system preserved for further investigation. If the investigator believes a rootkit has been found, and the rootkit needs to be removed from the production system, there are typically only two ways to remove the rootkit. The first is to search the web to find removal instructions, and the second is to reformat the entire system and reinstall Windows from a trusted source.
File Recovery

This button launches PC Inspector File Recovery from http://www.pcinspector.de/file_recovery/UK/welcome.htm. This freeware utility can be used to detect and recover deleted files. It supports file recovery from FAT 12/16/32 and NTFS file systems. [Developer’s note: version 4.0 is now available].

According to the website, it can finds partitions automatically, even if the boot sector or FAT has been erased or damaged; Recovers files with the original time and date stamp; Supports the saving of recovered files on network drives; Recovers files, even when a header entry is no longer available. Competition products cannot recover such files. The "Special Recovery Function" supports the following disk formats: ARJ AVI BMP CDR DOC DXF DBF XLS EXE GIF HLP HTML HTM JPG LZH MID MOV MP3 PDF PNG RTF TAR TIF WAV ZIP.

If the hard disk is no longer recognized by the BIOS, or is having mechanical problems (such as grinding sounds), this program will not be able to help.

To use the program, click on the file recovery icon, and answer yes to the confirmation dialogue. The main program will start, and open up a file recovery wizard. The program allows the investigator to select the language of their choice.
The main window will appear, giving several options.

![Image of PC Inspector File Recovery window]

Clicking on any of the options will scan the system and present a list of recognized drives.

![Image of Select drive window]

Notice: Select a logical drive to recover data. Optionally find logical drives on an existing physical/logical one.
Select the drive to examine. To continue, select the green checkmark icon. Each option will provide different methods on how to recover data.

In the recovered deleted files options, the program will display a windows explorer-like interface.

In this screen, in the deleted folders, we see that we can recover the _ULA.PDF file. To recover the file, right click on the filename and select “Save To…”
There are also other options, such displaying the properties, renaming the file, and viewing it either as a hex dump or as a text file.
VNC Server

http://www.realvnc.com/

From the website: VNC stands for Virtual Network Computing. It is remote control software which allows you to view and interact with one computer (the "server") using a simple program (the "viewer") on another computer anywhere on the Internet. The two computers don't even have to be the same type, so for example you can use VNC to view an office Linux machine on your Windows PC at home.

To use VNC, click on the icon next to VNC server. It will provide a confirmation prompt:

Click YES to continue. WinVNC will open a properties box. For the most part, you can leave it as it is, with one exception. You must enter a password in the password dialog box. VNC server will not accept incoming connections without a password.

To access this system from another location, you can use a VNC viewer, or a web browser. To use a web browser (from the Real VNC website): The VNC servers also contain a small web server. If you connect to this with a web browser, you can download the Java version of the viewer, and use this to view the server. You can then see your desktop from any Java-capable browser, unless you are using a proxy to connect to the web. The server listens for HTTP connections on port 5800+display number. So to view display 2 on machine 'snoopy', you would point your web browser at:

http://snoopy:5802/

The applet will prompt you for your password, and should then display the desktop.

From the viewer, you should now have full control of the system that the server is running on.

This is useful if the system you are examining and the system you are using to collect the date are too far apart work on them at the same time.
PuTTY SSH

Written and maintained primarily by Simon Tatham. It is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/

From the website: PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator.

This tool allows the user to remotely logon to a remote system and issue commands. This can be use to login into a remote system and run a netcat listener. The remote system must have a SSH server up and running.

Once selected, the program will display a confirmation.

Clicking on “Yes” will launch the PuTTY SSH program and display the configuration window.

For normal operations, the user should only have to enter the Host name or IP address, and click “Open”.

![PuTTY Configuration Window](image)
Screen Capture

http://www.hoverdesk.net/freeware.htm

From the website: HoverSnap is a free handy snapshot tool with jpg, png, bmp and gif support. HoverSnap can take snapshots of the full screen, active window or a selected area. It can even capture layered windows (alphablended ones under 2K / XP). You can even FTP upload your screenshots. In addition, you can set up the capture folder / filename and format, reduce the capture size, and auto-generate filename option will add the time stamp (date/time) to your filename in order to be able to take several captures without having to change the filename.

When you select the HoverSnap icon, it will present a confirmation prompt. When the user clicks “Yes”, there will be a HoverSnap icon in the system tray.

Clicking on this icon will display the configuration screen.

It is recommended that you change the destination folder to your removable evidence collection drive. In addition, checking “Auto-generate filename on new capture” option will automatically create filenames that start with the name in the filename box and automatically add a datetime stamp to the filename. Here is a sample auto-generated filename:

Capture12-12-2005-11.15.55 PM.png

To capture the full screen, the user presses the PrintScreen button. To capture the active window, press ALT+PrintScreen, and to select a custom area, press CTRL+PrintScreen.

With CTRL+PrintScreen, the cursor will change to a crosshair. Move the cursor to the upper left corner, then click and hold the left-mouse button and drag the cursor to the lower right corner. Release the mouse button to take the picture.

Once you have finished the screen captures, you should generate to the MD5 of the screen to ensure they are not modified.
Messenger Password

http://www.nirsoft.net/utils/mspass.html

From the website: MessenPass is a password recovery tool that reveals the passwords of the following instant messenger applications:

- MSN Messenger
- Windows Messenger (In Windows XP)
- Yahoo Messenger (Versions 5.x and 6.x)
- ICQ Lite 4.x/2003
- AOL Instant Messenger (only older versions, the password in newer versions of AIM cannot be recovered)
- AOL Instant Messenger/Netscape 7
- Trillian
- Miranda
- GAIM

MessenPass can only be used to recover the passwords for the current logged-on user on your local computer. You cannot use it for grabbing the passwords of other users.

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically start and display any passwords it can find.

From the website: When you run MessenPass, it automatically detects the Instant Messenger applications installed on your computer, decrypts the passwords they stores, and displays all user
name/password pairs that it found in the main window of MessenPass. If from some reason, MessenPass fails to locate the installed Instant Messenger application, you can try to manually select the right folder of your IM application by using 'Select Folders’ option (from the File menu). On the main window of MessenPass, you can select one or more password items, and then copy them to the clipboard in tab-delimited format (you can paste this format into Excel or Open-Office Spreadsheet), or save them into text/html files.
Mail Password Viewer

http://www.nirsoft.net/utils/mailpv.html

From the website: Mail PassView is a small password-recovery tool that reveals the passwords and other account details for the following email clients:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP and SMTP Accounts)
- IncrediMail
- Eudora
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail - If the password is saved in Yahoo! Messenger application.
- Hotmail/MSN mail - If the password is saved in MSN Messenger application.
- Gmail - If the password is saved by Gmail Notifier application.

For each email account, the following fields are displayed: Account Name, Application, Email, Server, Server Type (POP3/IMAP/SMTP), User Name, and the Password.

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically start and display any passwords it can find.
Protect Storage Viewer

http://www.nirsoft.net/utils/pspv.html

From the website: Protected Storage PassView is a small utility that reveals the passwords stored on your computer by Internet Explorer, Outlook Express and MSN Explorer. The passwords are revealed by reading the information from the Protected Storage. Starting from version 1.60, this utility reveals all AutoComplete strings stored in Internet Explorer, not only the AutoComplete password, as in the previous versions.

This utility can show 4 types of passwords:

1. **Outlook passwords**: When you create a mail account in Outlook Express or a POP3 account in Microsoft Outlook, and you choose the "Remember password" option in the account properties, the password is saved in the Protected Storage, and this utility can instantly reveal it.
   
   Be aware that if delete an existing Outlook Express account, the password won't be removed from the Protected Storage. In such a case, the utility won't be able to obtain the user-name of the deleted account, and only the password will be shown.
   
   Starting from version 1.50, the passwords of Outlook Express identities are also displayed.

2. **AutoComplete passwords in Internet Explorer**: Many Web sites provides you a logon screen with user-name and password fields. When you log into the Web site, Internet Explorer may ask you if you want to remember the password for the next time that you log into this Web site. If choose to remember the password, the user-name and the password are saved in the Protected Storage, and thus they can be revealed by Protected Storage PassView.
   
   In some circumstances, multiple pairs of user-name and passwords are stored for the same logon window. In such case, the additional passwords will be displayed as sub-items of the first user-password pair. In sub-items, the resource name is displayed as 3 dots ("...")

3. **Password-protected sites in Internet Explorer**: Some Web sites allows you to log on by using "basic authentication" or "challenge/response" authentication. When you enter the Web site, Internet Explorer displays a special logon dialog-box and asks you to enter your user-name and password. Internet Explorer also gives you the option to save the user-name/password pair for the next time you log-on. If you choose to save the logon data, the user-name and the password are saved in the Protected Storage, and thus they can be revealed by Protected Storage PassView.
   
   In this category, you can also find the passwords of FTP servers.

4. **MSN Explorer Passwords**:
   
   The MSN Explorer browser stores 2 types of passwords in the Protected Storage:
   
   - Sign-up passwords
   - AutoComplete passwords

By default, this utility shows all 4 types of passwords. You can select to show or hide a specific type of password, by choosing the right password type from the View menu.

This utility can only show the passwords of the current logged-on user. it cannot reveal the passwords of other users.

When the user clicks on the icon, Helix presents a confirmation message.
Once the user clicks “Yes”, the program will automatically start and display any passwords it can find.

The Protected Storage information is saved in a special location in the Registry. The base key of the Protected Storage is located under the following key:

"HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider"

You can browse the above key in the Registry Editor (RegEdit), but you won't be able to watch the passwords, because they are encrypted. Also, some passwords data are hidden by the operating system.
Network Password Viewer

http://www.nirsoft.net/utils/network_password_recovery.html

From the website: When you connect to a network share on your LAN or to your .NET Passport account, Windows XP allows you to save your password in order to use it in each time that you connect the remote server. This utility recovers all network passwords stored on your system for the current logged-on user.

Which passwords this utility can recover?
- Login passwords of remote computers on your LAN.
- Passwords of mail accounts on exchange server (stored by Outlook 2003)
- Password of MSN Messenger account (Only until version 7.0, for Newer versions - Use MessenPass)

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically start and display any passwords it can find.
Registry Viewer

http://www.nirsoft.net/utils/regscanner.html

From the website: RegScanner is a small utility that allows you to scan the Registry, find the desired Registry values that match to the specified search criteria, and display them in one list. After finding the Registry values, you can easily jump to the right value in RegEdit, simply by double-clicking the desired Registry item.

When the user clicks on the icon, Helix presents a confirmation message.

![Notice]

Once the user clicks “Yes”, the program will automatically start and display registry scan options page. This can be used to limit the searches, which can greatly speed up the process.

![Registry Scan Options]

Once the user clicks “OK”, the scanner will display registry keys matching their options.
<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKCU\Software\IrSoft\pspv</td>
<td>ShowMsnExplorer</td>
<td>REG_DWORD</td>
<td>0x00000001</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Internet Explorer\AdvancedOpti...</td>
<td>Text</td>
<td>REG_SZ</td>
<td>Show Internet E</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Internet Explorer\AdvancedOpti...</td>
<td>Text</td>
<td>REG_SZ</td>
<td>Automatically check</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\IE Setup\Options</td>
<td>UninstallDir</td>
<td>REG_SZ</td>
<td>F:\Program Files</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninst...</td>
<td>UninstallString</td>
<td>REG_SZ</td>
<td>F:\WINNT\System</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninst...</td>
<td>UninstallString</td>
<td>REG_SZ</td>
<td>F:\Program Files</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\JavaSoft\Java Plugin\1.4.0_01</td>
<td>UseJavaIEExplorer</td>
<td>REG_DWORD</td>
<td>0x00000000</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\JavaSoft\Java Plugin\1.4.2_05</td>
<td>UseJavaIEExplorer</td>
<td>REG_DWORD</td>
<td>0x00000001</td>
</tr>
<tr>
<td>HK\Software\Microsoft\Windows\CurrentVersion\RunOnce\</td>
<td>User Shell Folders</td>
<td>REG_SZ</td>
<td>My Computer\HK</td>
</tr>
</tbody>
</table>

939 Item(s), 1 Selected
IE History Viewer

http://www.nirsoft.net/utils/iehv.html

From the website: Each time that you type a URL in the address bar or click on a link in Internet Explorer browser, the URL address is automatically added to the history index file. When you type a sequence of characters in the address bar, Internet Explorer automatically suggests you all URLs that begins with characters sequence that you typed (unless AutoComplete feature for Web addresses is turned off). However, Internet Explorer doesn't allow you to view and edit the entire URL list that it stores inside the history file.

This utility reads all information from the history file on your computer, and displays the list of all 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 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, as long as you have permission to access the history folder.

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically display the URL history.
Asterisk Logger

http://www.nirsoft.net/

From the website: Many applications, like CuteFTP, CoffeeCup Free FTP, VNC, IncrediMail, Outlook Express, and others, allows you to type a password for using it in the application. The typed password is not displayed on the screen, and instead of the real password, you see a sequence of asterisk (****) characters. This utility can reveal the passwords stored behind the asterisks in standard password text-boxes.

Asterisk Logger is a successor of AsterWin utility. It reveals the asterisk passwords in the same way as AsterWin utility, but it has some advantages over the previous utility:

- You don't have to press a button in order to reveal the asterisk passwords. Whenever a new window containing a password box is opened, Asterisk Logger automatically reveals the password inside the password-box, and add a record to passwords list in the main window of Asterisk Logger.
- Asterisk Logger displays additional information about the revealed password: The date/time that the password was revealed, the name of the application that contains the revealed password box, and the executable file of the application.
- Asterisk Logger allows you the save the passwords to HTML file and to 3 types of text files.

When the user clicks on the icon, Helix presents a confirmation message.

![Notice]

You are about to run:
The Helix Asterisk Logger program from Nirsoft

IS THIS OK?

Yes  No

Once the user clicks “Yes”, the program will automatically start and display any passwords it can find.

![Asterisk Logger]
IE Cookie Viewer

http://www.nirsoft.net/utils/iecookies.html

From the website: 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.

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically display the cookies on the system.
Mozilla Cookie Viewer

http://www.nirsoft.net/utils/mzcv.html

From the website: MozillaCookiesView is an alternative to the standard ‘Cookie Manager’ provided by Netscape and Mozilla browsers. It displays the details of all cookies stored inside the cookies file (cookies.txt) in one table, and allows you to save the cookies list into text, HTML or XML file, delete unwanted cookies, and backup/restore the cookies file.

When the user clicks on the icon, Helix presents a confirmation message.

Once the user clicks “Yes”, the program will automatically display the cookies on the system.
Documents pertaining to Incident Response, Computer Forensics, Computer Security & Computer Crime

This section 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.

These documents can be accessed by clicking on its respective icon.

Chain of Custody

This is a sample chain of custody form used during investigation by e-fense.inc. There should be a separate chain of custody form created for each piece of evidence collected.
# EVIDENCE CHAIN OF CUSTODY FORM - FOR FOREnsic IMAGES ONLY

## HARD DRIVE/COMPUTER DETAILS

<table>
<thead>
<tr>
<th>Name #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model #</th>
<th>Serial #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## IMAGE DETAILS

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Created By</th>
<th>Method Used</th>
<th>Image Name</th>
<th>Segments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage Drive</th>
<th>HASH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## CHAIN OF CUSTODY

<table>
<thead>
<tr>
<th>Tracking No.</th>
<th>Date/Time</th>
<th>FROM:</th>
<th>TO:</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Preservation of Digital Evidence

The full title of this paper is “Preservation of Fragile Digital Evidence by First Responders”, and was written by Special Agent Jesse Kornblum, Air Force Office of Special Investigations in 2002.

From the Introduction: The nature of computer based evidence makes it inherently fragile. Data can be erased or changed without a trace, impeding an investigator’s job to find the truth. The efforts of first responders are critical to ensure that the evidence is gathered and preserved in a simple, secure, and forensically sound manner. This paper describes the challenges first responders face and some strategies for dealing with them. As an example, the paper also details a sample tool for first responders to incidents on Windows based computers.

This paper also describes the creation of F.R.E.D, the First Responder’s Evidence Disk, which is included on the Helix disk. While F.R.E.D has been updated significantly since this paper was originally published, this paper provides the basic details on how to preserve as much evidence as possible while disturbing as little as possible.

Linux Forensic Guide for Beginners

One of the first and most extensive guides on using Linux for forensic analysis, “The Law Enforcement and Forensic Examiner Introduction to Linux: A Beginner’s Guide” by Barry J. Grundy, Special Agent of the NASA Office of Inspector General, Computer Crimes Division. First written in 1998, the most recent revision was in 2004.

While this is not Helix specific, it provides a lot of background information for those investigators who are willing to boot into the Helix bootable Linux environment.

From the foreword: This purpose of this document is to provide an introduction to the GNU/Linux (Linux) operating system as a forensic tool for computer crime investigators. There are better books written on the subject of Linux (by better qualified
professionals), but my hope here is to provide a single document that allows a user to sit at the shell prompt (command prompt) for the first time and not be overwhelmed by a 700-page book.

Tools available to investigators for forensic analysis are presented with practical exercises. This is by no means meant to be the definitive “how-to” on forensic methods using Linux. Rather, it is a starting point for those who are interested in pursuing the self-education needed to become proficient in the use of Linux as an investigative tool. Not all of the commands offered here will work in all situations, but by describing the basic commands available to an investigator I hope to “start the ball rolling”. I will present the commands, the reader needs to follow-up on the more advanced options and uses. Knowing how these commands work is every bit as important as knowing what to type at the prompt. If you are even an intermediate Linux user, then much of what is contained in these pages will be review. Still, I hope you find some of it useful.

Over the past couple of years I have repeatedly heard from colleagues that have tried Linux by installing it, and then proceeded to sit back and wonder “what next?” You have a copy of this introduction. Now download the exercises and drive on.

**Forensic Examination of Digital Evidence**

Published in April 2004 by the U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, this special report “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”, provides the digital forensic investigator a detailed guide on how to collect, process, and document digital evidence.

From the foreword: To assist law enforcement agencies and prosecutorial offices, a series of guides dealing with digital evidence has been selected to address the complete investigation process. This process expands from the crime scene through analysis and finally into the courtroom. The guides summarize information from a select group of practitioners who are knowledgeable about the subject matter. These groups are more commonly known as technical working groups. This guide is the second in a series.

Browse contents of the CD-ROM and Host

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.

If the “Calculate MD5 hash on files” is selected, the MD5 of the hash will also be displayed with the rest of the file information. It is turned off by default, since it can sometimes take a while to generate the MD5 for very large files.

Due to the nature of the windows operating system, the first time you select a file (on any read/write media, such as a hard drive) 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 can not be easily prevented. This is one of the problems with examining a live system – the investigator’s actions may modify the system.

Here is an example:
In this list of recovered files, we see that the accessed date on CONVAR10.jpg is Thursday, September 29, 2005. If another file is selected, and then CONVAR10.jpg is selected again, we will see that the accessed data has changed to the today’s date. Everything else has remained the same.
Scan for Pictures from a live system

This tool will allow 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. This feature was added to support “Knock and Talks.” This allows a parole officer to preview a system for graphic images that may violate a parole.

When the scan for pictures icon is selected, this window appears:

The investigator should select “Load Folder” and select the drive they wish to examine. Be aware that depending on the size of the hard drive, the amount of memory, and the speed of the system, this can take a while. A reminder windows pops up to inform the investigator. Scanning will not begin until the “OK” button is pressed.

Investigators will need to examine each drive letter separately.
Double-clicking on any thumbnail will open the image in the local viewer. You can enlarge or decrease the size of the thumbnails by clicking “Enlarge” or “Decrease”. Be advised that this will increase or decrease the size of all the thumbnails, and may take a few moments to complete, depending on the number of thumbnails.

Also be aware that this application will change the last access time on just about every file on the system, since it examines the file headers to determine if the file is a graphic.
Exiting Helix

There are several ways to exit the Helix application.

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

Note that the first two ways to exit will save a copy of all your transactions, while exiting from the system tray icon will not.

If you chose to save the output, you will be prompted where to save the file. It should be saved on a network share or a removable evidence collection drive to prevent any contamination of the suspect computer. The default filename is Helix_Audit_Log.pdf.

Sample Output

```
Helix Started on: 12/12/2005 at 23:45:59
=================================================================================
Operating System:Windows XP Service Pack 1
Operating System Version: 5.1.2600
User Information:
Owner: 
Organization: 
Admin: No
Admin Rights: Yes
Network Information:
Host: TAL_MC
User: bgleason
IP: 152.168.1.102
NIC: 005056c00008
Domain: TAL_MC
Detected Drives:
A: (Removable drive)
C: (Attached (fixed) drive)
D: (Attached (fixed) drive)
N: (Attached (fixed) drive)
=================================================================================
23:46:16 - Helix displayed the Scan for Images page.
23:47:10 - The Chain of Custody Form was opened.
=================================================================================
Helix Stopped on: 12/12/2005 at 23:47:33
```
Bootable Helix (Linux Side)

One of the greatest benefits of Helix is the bootable environment. Helix will boot on all x86 architectures which make up a majority of the computers in the world. It is for this reason that Helix for the immediate future will remain on a CDROM. Almost every computer in the world has a CDROM, but most do not have DVD’s, etc. While derivatives like Helix USB will be forthcoming, it is most stable on the CD platform.

Helix, like Knoppix, will boot into a self contained Linux environment. This environment has been tweaked for forensic purpose. While there are many distributions of Knoppix such as Knoppix-STD, Helix only concentrates on Incident Response and Forensics.

Bootable Basics

The first step you must accomplish to boot into Helix is to make sure that your BIOS is setup to boot from the CDROM before any other device. If your BIOS does not support booting from a CDROM, then you must result to booting from a floppy disk (time to upgrade your system).

All that is required to boot Helix is to place the Helix CD into the CDROM drive and reboot/turn on the computer. When the system passes the POST, you should see the screen:

As you can see you are presented with a graphical boot menu courtesy of Grub (Grand Unified Bootloader). You can choose the option that is best for you and your environment. The initial default setting should work for most people; however there are occasions when that won’t work. Some laptops and other hardware do not like some of the standard options like using DMA on all devices. So you must choose the option to turn off DMA. Some of the other popular options that are available are using failsafe mode, and console mode. See Appendix A for a list of all the boot
methods. Helix defaults to using the 2.6.10 Kernel although the older 2.4.27 kernel is still available.

While there are many options pre-determined for you in the boot screen, it may sometimes be necessary to add or delete extra commands. In order to do this within grub just type in or delete the commands you want by simply typing. The boot options will change as you type. As an example below, the quiet and BOOT_IMAGE=helix option have been deleted simply by pressing the backspace key.

Once you select your boot option and hit the ENTER key, you will see the Helix startup screen. This screen will show you boot progress. If you want to see a more verbose output then you will need to press the F2 key to see what Helix is doing during the boot process.

In the verbose mode you will see the devices that Helix finds as well as provides you with kernel information, which could be important if there are problems in loading Helix.
Once Helix finishes the boot process, X Windows will automatically start and present you with the screen in Figure 20 which is the Helix desktop. Helix uses the Xfce\(^6\) desktop environment as it is extremely lightweight and very versatile. All of the other former Desktop environments such as KDE, Fluxbox, larswm, etc have been removed from Helix entirely, although many KDE applications still exist.

\(^6\) [http://www.xfce.org/](http://www.xfce.org/)
Much of what you will need from Helix is available via the Xfce panel on the bottom of the screen. The panel has links (icons) for Grab, SMART, Clamscan, F-Prot, Autopsy, pyFLAG, and Retriever. It also has links for Sguil, Firefox, Xffm, and many terminals which all have logging capability turned on. In addition many of the icons have an associated link that will open a submenu when pressed. These submenus generally contain the associative manuals and or HOWTOs.
The Helix Filesystem

Obviously Helix is run from a CDROM which uses the ISO9660 standard for its file system. This has its benefits and drawbacks. The largest benefit is that files on the CDROM cannot be changed making it a permanent storage and security solution. You can use the CD in an incident response role and not have to worry about your files being altered. However this also is the largest drawback in that you cannot change any of the files once they are in place.

Why would you want to change a file? Well the biggest reason is to updated configuration settings. So how do you do this on a write once medium like a CDROM? There are actually two ways to do this, the old way and the new way. The old way consisted of linking the files that needed to be changed into a specific area that was stored into a RAM disk. This worked but was a poor solution do to the amount of files that would need to be linked and the fact that the files would have to be linked prior to burning the iso file to a CDROM. The new way involves using a file system overlay called Unionfs.

Unionfs

Unionfs merges directories into a single unified view. A collection of merged directories is called a union, and each physical directory is called a branch. Each branch is assigned precedence and a branch with a higher precedence overrides a branch with a lower precedence. Unionfs operates only on directories as opposed to devices (like cowloop). If a directory exists in two underlying branches, the contents and attributes of the Unionfs directory are the combination of the two lower directories. Unionfs automatically removes any duplicate directory entries.

Copy-On-Write Unions
Unionfs can mix read-only and read-write branches. In this case, the union as a whole is read-write, and Unionfs uses copy-on-write semantics to give the illusion that you can modify files and directories on read-only branches.

If the CD-ROM is mounted on /mnt/cdrom, and an empty directory is created in /tmp/cd, then Unionfs can be mounted as follows:

```bash
EXAMPLE – Copy-On-Write Union

# mount -t unionfs -o dirs=/tmp/cd,/mnt/cdrom none /mnt/cdrom-rw
```

When viewed through /mnt/cdrom-rw, it appears as though you can write to the CD-ROM, but all writes actually will take place in /tmp/cd. Writing to read-only branches results in an operation called a copyup. When a read-only file is opened for writing, the file is copied over to a higher-priority branch. If required, Unionfs automatically creates any needed parent directory hierarchy. With a simple modification, Helix uses Unionfs as an overlay mount. Meaning that, the Helix CDROM becomes writable by replacing /HELIX/ /tmp/HELIX with the unified view:

```bash
EXAMPLE – Copy-On-Write Union with Overlay

# mount -t unionfs -o dirs=/home/cpw/linux:/usr/src/linux=ro none /home/cpw/linux
```

Helix automatically uses Unionfs and creates the union upon bootup and initialization. You will be able to “write” to all of the directories. This makes installing software or updating configuration files very simple.

* NOTE so for this only works on the 2.6.10 kernel within Helix.

Cowloop

Cowloop is a copy-on-write loop driver (block device) that is used on top of another block driver. The cowloop-driver protects the original lower driver from any write accesses. It instead diverts all write-accesses to an arbitrary regular file.

The cowloop-driver allows files or block-devices to be used in a read-write fashion without modifying the file or block-device itself. Modified data-blocks are not written back to the original read-only device, instead they are written to a separate file called the copy-on-write file or cowfile.

The cowloop driver is installed by default in the Helix 2.6.10 kernel for users who choose to utilize the cowloop functionality.

Image Acquisition Basics

The first step in any forensics process is to acquire an image for analysis. There are many different ways to accomplish this. Some of the most common are through Commercial-off-the-Shelf (COTS) products like EnCase, Forensic Tool Kit (FTK), and Safeback. However, the best tool for the job is the very FREE utility - dd.
Raid Essentials

Although RAIDs can be the hardest devices to image, especially the proprietary kind from Dell and Compaq, Helix provides a fairly simple solution. Helix can see most hardware RAIDs as the RAID card initializes the RAID before Helix even boots. Helix also has many RAID drivers for both software and hardware RAIDS.

Depending on the actual RAID device, Helix may not place the RAID in the /mnt directory like other devices, but that does not mean Helix does not see the RAID. For instance, to identify a Compaq Raid Devices, do a “dmesg” and look for “cpqarray.” If you see that you should see the devices that the Compaq RAID sees. The device should show partitions as:

<table>
<thead>
<tr>
<th>Example – Compaq Array Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ida/c0d0: p1 p2 p3</td>
</tr>
<tr>
<td>so partitions will be:</td>
</tr>
<tr>
<td>/dev/ida/c0d0p1</td>
</tr>
<tr>
<td>/dev/ida/c0d0p2</td>
</tr>
<tr>
<td>/dev/ida/c0d0p3</td>
</tr>
</tbody>
</table>

Helix has many built in RAID drivers in the kernel and many more as loadable modules. If for some reason Helix does not see the RAID you will have to try and load the appropriate modules by:

<table>
<thead>
<tr>
<th>Example – Loading a Kernel Module for an Adaptec 2120 RAID</th>
</tr>
</thead>
<tbody>
<tr>
<td># modprobe aacraid</td>
</tr>
</tbody>
</table>

This will load the aacraid module into the running kernel so that you can access the Adaptec RAID.
Understanding DD

**dd** has an interesting history. The most interesting is what dd stands for; most people assume dd stands for “device dump,” or “device-to-device,” or “data dump.” Some think it stands for “copy and convert” but that it was renamed to dd because the letters “cc” were reserved for the C compiler. The most interesting definition is that dd stands for “death and destruction” for what happens if you mess up the options; which is most definitely true. In actuality dd stands for “data definition,” if it can be said to stand for anything at all. The reason is that it was derived from the IBM OS/360 JCL (Job Control Language) command of the same name. IBM System/360 JCL had an elaborate dd "Dataset Definition" specification suitable for copying block-oriented I/O devices.

The dd command is used in computer forensics to perform a physical backup of hardware device media. What makes the dd command special is that it has special flags that make it suitable for imaging block-oriented devices such as tapes. dd is capable of addressing these block devices sequentially. In order to proceed, it is very important to understand the basic syntax of the dd command:

<table>
<thead>
<tr>
<th><strong>DD – Understanding Syntax</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dd if=source of=destination</strong></td>
</tr>
</tbody>
</table>

Where:
- **if** = input file, or device you are copying (a hard disk, tape, etc.)
- **source** = source of image
- **of** = output file, or copy of image
- **destination** = where you want to place the copy

For example:
- if the device to be imaged is /dev/hda, the following would produce an exact copy with the name of 'ForensicCopy.img':

```
dd if=/dev/hda of=/mnt/hdd1/ForensicCopy.img
```

As mentioned earlier, dd is very useful when copying and/or restoring block-oriented devices such as tapes. Some of the options available to dd which make it very useful are:

- **bs** = block size
- **ibs** = input block size
- **obs** = output block size
- **count** = number of blocks to copy
- **skip** = number of blocks to skip at start of input
- **seek** = number of blocks to skip at start of output
- **conv** = conversion
These options are extremely useful in many instances. For example, if you wanted to just acquire the Master Boot Record (MBR) from a hard drive, you would need to obtain the first 512 bytes from the hard drives partition table. In order to do this you would need to pass some options to `dd` to only grab the first 512 bytes, otherwise `dd` would acquire the entire hard drive. So to accomplish this you would type in:

```
Example – Acquiring the MBR using DD

dd if=/dev/hda of=/mnt/hdd1/MBR.img bs=512 count=1
```

Another example of using `dd` is to use it to split up a large image into much smaller images. This is a long way of accomplishing this as you would normally use the `split` utility, but this serves as just an example of the power of `dd`. For our example lets assume we have a 4GB device and we want to split the image up into four 1GB files.

```
Example – Splitting an image file using DD

Using dd with the flags below will create four images each 1GB in size.

dd if=/dev/hda count=1000000 of=image1
dd if=/dev/hda count=1000000 skip=1000000 of=image2
dd if=/dev/hda count=1000000 skip=2000000 of=image3
dd if=/dev/hda count=1000000 skip=3000000 of=image4
```

Now each image is 1GB in size rather than the original 4GB. The first thing you should notice is that the first command takes 1GB (count=1000000) and copies it, naming the copy 'image1.' The second command `skips` the first 1GB (skip=1000000) and then copies the next 1GB (count=1000000), naming this image 'image2' and so on. This is the purpose of the 'count' and 'skip' flags.
**Traditional Acquisition (Dead Imaging)**

The process by which an image is acquired when the hard drive has been powered down is also known as dead imaging. This is the best method for obtaining the most forensically sound image. It is also the method that law enforcement uses as their primary practice.

There are many ways you can accomplish this task in a lab environment, but one of the easiest methods to use Helix. Helix is valuable in many ways but mostly for the ability to quickly image systems that utilize RAID devices. It is far more economical to image a RAID device at the logical level than to individually image each drive and try to rebuild the RAID device later on.

Boot the Helix CD in the system to be imaged (evidence system). You may need to boot into failsafe mode in order to be operational. There are some instances with proprietary raids like the Compaq Proliants using the SMART-2/P Raid controller in which Helix will not boot normally it will just hang during the auto detection phase.

Once Helix has booted, you have several options that you can use to image the system. You will need to make a decision whether to image the entire drive (physical) or the individual partitions (logical). In either case, your image will contain deleted files, slack space, and unallocated space. If you choose a logical image, the only thing you will be missing is the MBR and swap space if you forget to image it. Currently Autopsy cannot parse a physical image. So if you plan on using Autopsy you need the logical images.

**Imaging to a Samba Server**

The first thing you need to do after booting the system to be imaged with Helix is set up a Samba server on your Acquisition system. Samba is very easy to implement and is generally the best method to use. Samba is configured by the smb.conf file located in /etc/samba. See Appendix 1 for an example of a working Samba Forensics Server smb.conf file.

There are a few tricks that you must be aware of with a Samba Forensic Server. First you must mount the drive you want to use as your collection/harvest drive and that drive must be writable. The easiest way to accomplish this is by the following mount command:

```
Example – Mounting a device for use as a Samba share

mount -o rw,umask=000 /dev/hd?? /mnt/images
where:
?? = linux device that is your collection/harvest drive i.e. /dev/hdd1
/mnt/images = mount point of your collection/harvest drive.
```

Start your Samba server after you have mounted your collection/harvest drive by simply typing:

```
service smb start  OR   service smb restart
```

You are now ready to use the Samba share as your image destination. The only step that remains is to mount the Samba share on the Helix system. To mount the Samba share (**GRAB WILL DO THIS FOR YOU**):
Example – Mounting a Samba or Windows share within Helix

```
mount -wt smbfs -o username=username,password=password //<IP>/<share> /<mount_point>
```

where:

- `-wt smbfs` = mount read/write and set file system type to samba fs
- `-o username=username,password=password` = set username and password
- `//<IP>` = netbios flag and IP address of the Samba/Windows System
- `/<share>` = share name you want to mount
- `/<mount_point>` = place you want to mount the share drive to

* You can also add dmask=0777,fmask=0777 to the options for read/write

The nice thing about setting up a Samba Forensics Server and imaging to it is that you can direct all of your commands to the local file system as that is where your Samba/Windows share will be located. It will appear as if you are writing to another directory on your local system when in fact the data will be traversing over the network.

**EXAMPLE – Imaging to a samba share**

```
dcfldd if=<device> | tee >(sha1sum > /(case#)/<filename.sha1 ) | split -a 3 -d -b 1436m - /(case#)/<filename_img.>
```

Imaging to a Netcat/Cryptcat Listener

There may be rare occasions in which you use Netcat rather than Samba. For example, if for some reason Helix does not work, you could use Netcat or Cryptcat.

Netcat is a networking utility which reads and writes data across network connections using the TCP/IP protocol. Cryptcat is the standard Netcat enhanced with twofish encryption. Helix does not use the default secret key (metallica), the key has been changed for Helix. You can change the key by using the `-k` option.

You still need to mount your collection/harvest drive which is the same method as above. The next step would be to set up a Netcat listener on the forensics server depending on what you want to collect. If you want to acquire the entire physical drive:

**Example – Using a Netcat/Cryptcat server**

Issue the following command the Forensics Server:
```
nc –v –n –l –p 8888 –O myimage.img
```

On the Helix system you can then run `dd`:
```
dd if=/dev/<device> | nc <IP> 8888
```
GRAB

Rather than recreate the wheel, GRAB was based upon the AIR (Automated Image & Restore) code. AIR was created by Steve Gibson and can be downloaded from: http://air-imager.sourceforge.net/. GRAB is a GUI front-end to dd/dcfldd/sdd and was designed to simplify the creating of forensic bit images.

GRAB Features

GRAB has several features and abilities, they include the following:

- auto-detection of IDE and SCSI drives, CD-ROMs, and tape drives
- choice of using either dd, dcfldd, or sdd
- image verification between source and copy via MD5 or SHA1
- image compression/decompression via gzip/bzip2
- image over a TCP/IP network via Netcat/Cryptcat, or SAMBA (NetBIOS)
- supports SCSI tape drives
- wiping (zeroing) drives or partitions
- splitting images into multiple segments
- Detailed logging with date/times and complete command-line used.

Using GRAB to acquire your image

Since GRAB is just a front end to dd, you are really using dd to acquire your images. GRAB just makes the long and sometimes ugly command line easier to manage. You should be familiar with the dd syntax before you embark on using GRAB as your acquisition tool, but it is not necessary. Just keep in mind YOU CAN CAUSE PERMANENT DATA LOSS ON YOUR HARD DRIVES if you reverse the source and destination devices.

As you can see, GRAB is fairly intuitive. The options have been kept to a minimum for simplicity. The default values should work for most users, although more advanced users can obviously choose options that they need. Upon starting, GRAB will list all of the devices it can see in the session log area.
The first part of GRAB that you should notice is what devices are connected, or what devices GRAB can see. This is easily accomplished by looking at the top center of the GRAB GUI.

As you can see by Figure 25, there are a few connected devices and a few special devices which are always present. Generally you will always see the device HDA as that is normally the first IDE hard drive. The special devices are always Zero, Null, and Net. Zero is used to wipe device, Null is a through away bit bucket. The Net device is used when you want to send an image to a server or use GRAB to act as a server. The Net device button will be discussed in more detail later on in this document.

First you should choose the device that you want to image/acquire. For the purposes of this document we will use the HDA device. So select the HDA button. After you select that button a new dialog window will open.

As you can see from Figure 26 the dialog window that opens provides you with a few more new options. You can choose to display the device information which is ALWAYS the first selection you should make.

When you select the “Device Info” button the screen from Figure 25 will be displayed in the GRAB status window showing you the geometry of the device you are looking at. If you want to see the partitions on that device to understand what you will be imaging simply choose the “Partitions” button and GRAB will display the information in Figure 28.

You can now either select to set this device as the source or as the destination, or you can cancel and return to the main screen. If this is the device that you want to acquire than you need to
choose “Set as Source” otherwise you may inadvertently wipe that drive which would be disastrous.

You can always choose the source and destination device by simply typing in the devices/paths in the user input areas or you can select the hard coded devices in the drop down boxes from the main screen.

If you want to send the acquired image to a network server through Netcat/Cryptcat or Samba using NetBIOS then choose the special devices NET button. A dialog box will open revealing Figure 29. You must choose whether to set the remote destination as the source or destination. In almost all cases you will want to select the “Destination” button. Upon selecting the destination button you will be presented with the network IP/Port, share screen.

The network IP/Port, share screen will allow you to choose how you want to send the acquisition image. You can either use Netcat/Cryptcat or NetBIOS using Samba or a Windows share. You only use ONE option. If you want to use Netcat/Cryptcat, then type in the server’s IP address and port number that the Netcat/Cryptcat server is listening on. Then click on the “Use NC” button. Otherwise you type in the Windows share you are going to use in the “Dest Share” input box and click on the “Use Share” button. The only “gotcha” that you need to be aware of is that the Windows nomenclature is reversed in Linux. So the traditional “\” that you are used to, needs to be “/” instead. Also you do not want to have a trailing slash (/). So to send an image you are going to acquire to a Samba share you would type in the following:

**EXAMPLE – Samba Share**

```
//forensics/images
```

Where “forensics” is the system name of the server and “images” is the name of the shared folder.

When you click on the “Use Share” button you will be presented with a dialog box that tells you to click on the start button to proceed. This is normal even though you have not typed in a username or password for the share that you want to use. That will happen when you click on start. Once you do click on start you will notice that before anything starts to work a dialog box will open telling you that the remote share must be mounted. GRAB will use smbfs
too mount the share to the local system. Choose yes to mount the share and you will be prompted for a mount point which can normally be the default, and a username/password combination. Click the “Mount” button and GRAB will mount the share for you to use.

As you can see, GRAB mounted the remote share to the local file system so that it (GRAB) can now write the image files to the network share. The success or failure log will show up in the Session Log window of GRAB letting you know if it worked or if there were problems. A majority of the problems people have is not using the correct syntax in the share name, i.e. using the incorrect nomenclature like \ instead of //.

Once you have all of your images you need to verify the image compare with the sum of the whole drive you just imaged. This can be done easily with the cat program.
EXAMPLE – Verifying a Split image

cat <images> | sha1sum --check <image>.sha1
where <images> = all of the images you have like image.001
<image>.sha1 = What you called the sha1sum check file

If everything went ok you should see the sha1sum check return the filename with "OK". If you do not see that you either have a problem with your images or you may have cat’d files together that were not part of your original image.

Retriever

Retriever is a new tool created by me exclusively for the Helix CD. Retriever is an image (picture/video) capturing utility for “knock & talks”, “quick peeks”, and general searches. Retriever will scan a mounted device and locate all of the images and movie files and place them onto a USB key (or local drive) as well as open an image viewer to view them.

When you start Retriever you will be presented with a welcome screen that will self close after 10 seconds. This splash screen explains what Retriever is and does. You can also close it by pressing the OK button.

When the introductory splash screen disappears you will be presented with a dialog box that asks where you want to store the files that Retriever locates. You will have two choices for storage; One to the hard drive or Two to a USB-Key. In both case the storage location is hard coded to save all the images to the directory “/images/retriever.” The only difference is that if you choose to save the images to the hard drive Retriever will not copy the located files, rather it will create symbolic links to those files to conserve memory/hard drive space.
After you have chosen a location to save the image too, Retriever will display two windows. One window is the display/log window, while the other is where you will choose which device you want to scan.

The above dialog that asks you to choose a directory is where you will select the device that you want to scan. Keep in mind that Retriever is a compliment to the Helix CD and as such all devices that Helix sees are located under the /mnt directory. So to choose the device you want to scan select the appropriate directory under /mnt and select OK. After you select OK you will be presented with another dialog box that looks like the one in Figure 39. This is just a confirmation box for the device you just selected. Once you select the OK button Retriever will start scanning the device for all image files and movie files. Retriever does NOT search by file extension but rather by file type, this will ensure that all graphic files and movie files will be found. This version of Retriever will NOT find files that have been deleted, for that you will need to image the hard drive using Grab, SMART or another similar tool.
Once Retriever has started scanning a device for images you will see the images that are located appear in the progress window. Another program will also open to display images that have been located. When Retriever is finished the progress window will inform you as to how many image files have been found. Retriever also does a rudimentary gathering of device information for the log file so that you can see the type of hard drive, etc that you are scanning. If you choose to save the image to a USB-Key then you will have exact copies of the located images automatically saved to your key on the fly.

Retriever is in an initial release form right now and will, like most programs, improve with age.
Practice Labs

In this section, we provide the learner with several laboratories that they can use to practice their skills.

Lab 1 – Create an Image of a suspect Floppy Disk

To be added later….

Lab 2 – Create a floppy disk from an image
Lab 3 – Preview Image of suspect Floppy disk
Lab 4 – Create an Image of suspect hard drive using netcat
Lab 1 - Create an Image of a suspect Floppy Disk

You have been given a suspect's floppy disk, and you want create an image of it. On your system, insert the Helix CD, and once the menu comes up, select the icon for “Acquire a “live” image of a Windows System using”.

Our source will be the A:\ drive, our destination will be C:\, and our image name will be “Floppy01.dd”.

Press the “Start Helix Acquisition” button, and you will be presented with a command preview box
Click “yes”. You will now receive an instruction screen explaining what you should do next:

Click “Ok”. The forensic shell tool will open:

Once the shell opens, right-click inside the shell, and select “paste” from the context menu that appears. The command line will be pasted into the shell.
Press "Enter" to execute the command. After a few minute the command will finish.

There will now be 3 files in the destination directory:

- Floppy01.dd – the image of the floppy disk
- Floppy01.dd.md5 – a file containing the MD5 of the image file.
- Audit.log – a file containing the command and the output of the program.

Forensic Acquisition Utilities, 1, 0, 0, 1035
dd, 3, 16, 2, 1035
Copyright (C) 2002-2004 George M. Garner Jr.

Command Line: ..\Acquisition\FAU\dd.exe if=\\.\A: of=C:\Floppy01.dd conv=noerror --md5sum --verifymd5 --md5out=C:\Floppy01.dd.md5 --log=C:\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 1)

29/09/2005  04:39:53 (UTC)
Current User: TAL_MC\bj gleason

unable to display device info
Copying \\A: to C:\Floppy01.dd...
\d32a686b7675c7a4f88c15522738432 [\\\A:] *C:\Floppy01.dd

Verifying output file...
\d32a686b7675c7a4f88c15522738432 [\\\A:] *C:\Floppy01.dd
The checksums do match.

Output C:\Floppy01.dd 1474560/1474560 bytes (compressed/uncompressed)
360+0 records in
360+0 records out
References

http://www.fulco.net/content/view/22/40/