# Reporting

- To complete a forensics disk analysis and examination, you need to create a report.
- Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually.
- The investigator then copied the evidence to a separate program, such as a word processor, to create a report.

- Newer Windows forensics tools can produce electronic reports in a variety of formats, such as word processing documents, HTML Web pages, or Acrobat PDF files.

These are the sub functions of the reporting function:

- Log reports
- Report generator

.....

- Many forensics tools, such as FTK, ILook, and X-Ways Forensics, can produce a log report that records activities the investigator performed.
- Then a built-in report generator is used to create a report in a variety of formats.
- The following tools are some that offer report generators displaying bookmarked evidence:
- EnCase
- FTK
- ILook
- X-Ways Forensics
- ProDiscover

- The log report can be added to your final report as additional documentation of the steps you took during the examination, which

can be useful if repeating the examination is necessary.

# Computer Forensics Software Tools

- Whether you use a suite of tools or a task-specific tool, you have the option of selecting one that enables you to analyze digital evidence through the command line or in a GUI.
- The following sections explore some options for command-line and GUI tools in both

# Windows and UNIX/Linux.

# Command-Line Forensics Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.
- One of the first MS-DOS tools used for computer investigations was Norton Disk Edit.
- This tool used manual processes that required

investigators to spend considerable time on a typical 500 MB drive.

.....

- Eventually, programs designed for computer forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems.
- Some of these early programs could extract data from slack and free disk space; others were capable only of retrieving deleted files.
- Current programs are more robust and can search for specific words or characters, import a keyword list to search, calculate hash values, recover deleted items, conduct physical and

logical analyses, and more.

# .....

- Some command-line forensics tools are created specifically for DOS/Windows platforms;
- others are created for Macintosh and UNIX/Linux. Because there are many different versions of UNIX and Linux, these OSs are often referred to as *nix platforms.

# UNIX/Linux Forensics Tools

- The *nix platforms have long been the primary command-line OSs, but typical end users haven't used them widely.
- However, with GUIs now available with *nix platforms, these OSs are becoming more popular with home and corporate end users.
- There are several *nix tools for forensics analysis, such as SMART, BackTrack, Autopsy with Sleuth Kit, and Knoppix-STD.

.....

- SMART SMART is designed to be installed on numerous Linux versions, including Gentoo, Fedora, SUSE, Debian, Knoppix, Ubuntu, Slackware, and more.
- You can analyze a variety of file systems with SMART;
- SMART includes several plug-in utilities. This modular approach makes it possible to upgrade SMART components easily and quickly.
- SMART can also take advantage of multithreading

capabilities in OSs and hardware.

# ....

- Another useful option in SMART is the hex viewer. Hex values are color-coded to make it easier to see where a file begins and ends.
- SMART also offers a reporting feature. Everything you do during your investigation with SMART is logged, so you can select what you want to include in a report, such as bookmarks.

.....

- Helix One of the easiest suites to use is Helix because of its user interface. What's unique about Helix is that you can load it on a live Windows system, Its Windows component is used for live acquisitions
- During corporate investigations, often you need to retrieve RAM and other data, such as the suspect's user profile, from a workstation or server that can't be seized or turned off.
- This data is extracted while the system is running

and captured in its state at the time of extraction.

# .....

- To do a live acquisition, insert the Helix CD into the suspect's machine. After clicking I ACCEPT in the licensing window, you see the Helix menu.

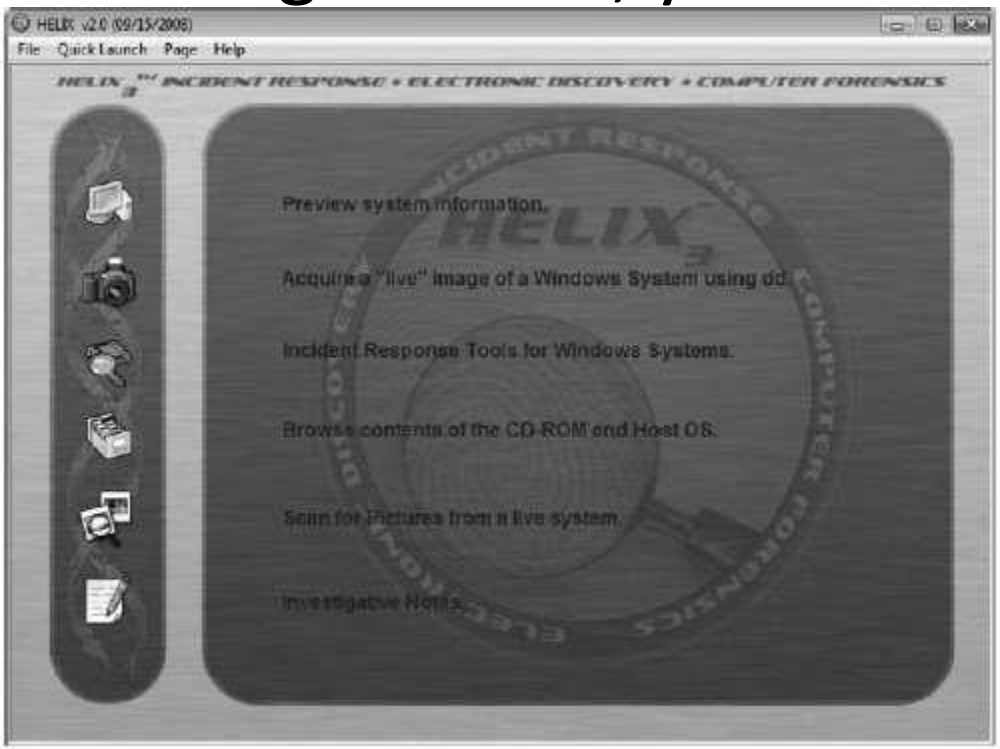


Figure 7-8 The Helix menu

- BackTrack BackTrack is another Linux Live CD used by many security professionals and forensics investigators. It includes a variety of tools and has an easy-to-use KDE interface.
- Autopsy and Sleuth Kit Sleuth Kit is a Linux forensics tool, and Autopsy is the GUI browser interface for accessing Sleuth Kit's tools.

.....

- Knoppix-STD Knoppix Security Tools Distribution (STD) is a collection of tools for configuring security measures, including computer and network forensics.
- Note that Knoppix- STD is forensically sound, so it doesn't allow you to alter or damage the system you're analyzing.
- If you boot this CD into Windows, Knoppix lists available tools. Although many of the tools have

GUI interfaces, some are still command line only.

.....

- Figure 7-9 shows what you see if you load the Knoppix-STD CD in Windows.
- You can scroll through this window and see some of the available tools


**Figure 7-9** The Knoppix-STD information window in Windows

...

- Like Helix, Knoppix-STD is a Linux bootable CD. If you shut down Windows and reboot with the Knoppix-STD disc in the CD/DVD drive, your system boots into Linux.

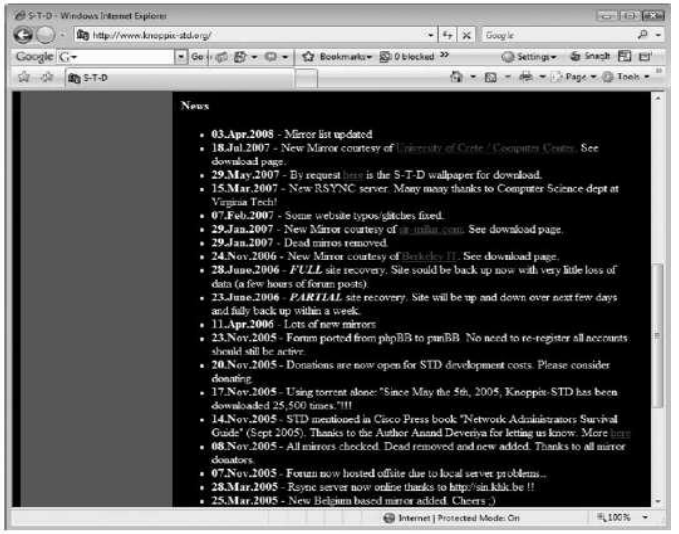


Figure 7-10 A list of forensics tools available in Knoppix-STD

# Other GUI Forensics Tools

- Several software vendors have introduced forensics tools that work in Windows.
- Because GUI forensics tools don't require the same understanding of MS-DOS and file systems as command-line tools, they can simplify computer forensics investigations.
- These GUI tools have also simplified training for beginning examiners; however, you should continue to learn about and use command-line tools because some GUI tools might miss critical

evidence.

.....

- GUI tools have several advantages, such as ease of use, the capability to perform multipletasks, and no requirement to learn older OSs.
- Their disadvantages range from excessive resource requirements (needing large amounts of RAM, for example) and producing inconsistent results because of the type of OSused, such as Windows Vista 32-bit or 64-bit systems