Computer Hacking Forensic Investigator

Module XI

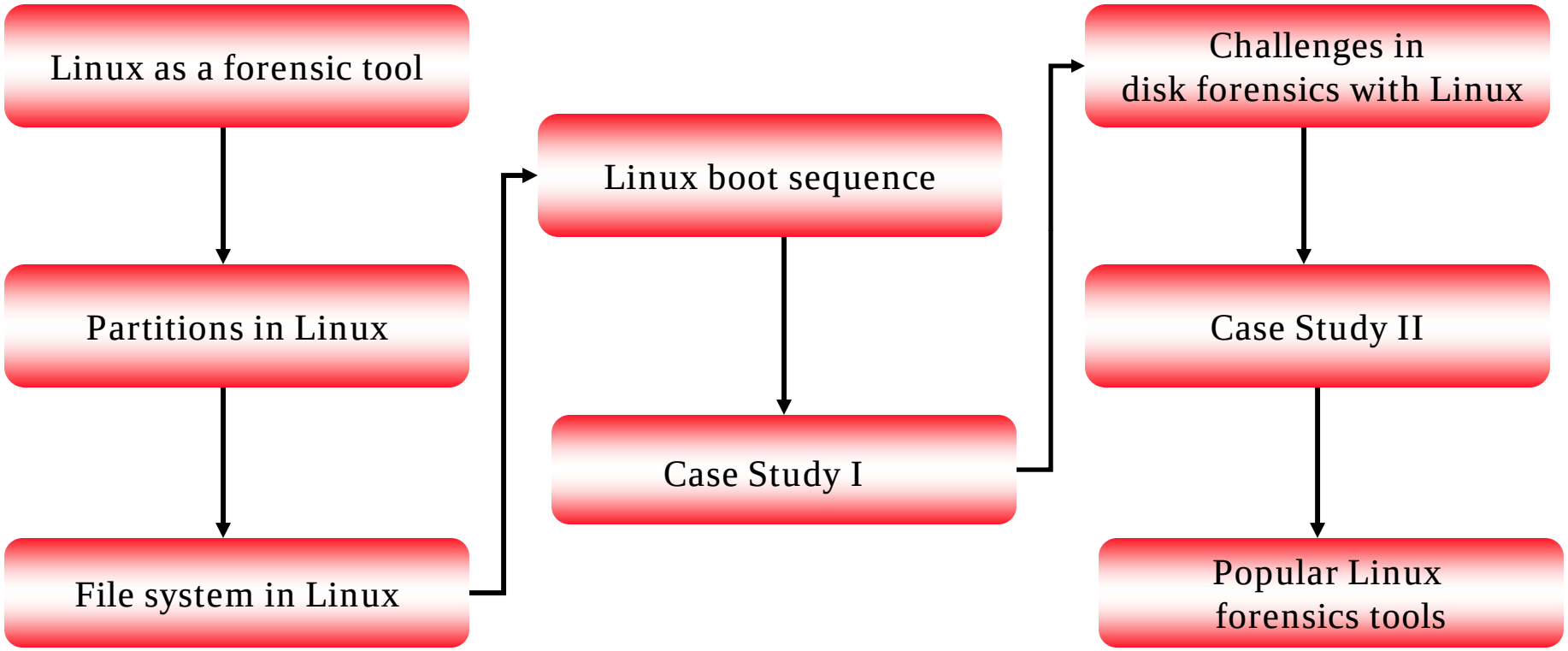
Linux Forensics

Module Objective

This module will familiarize you with the following:

- Use of Linux as a forensic tool.
- Recognizing partitions in Linux.
- Overview of the file system in Linux.
- Linux boot sequence.
- Case study – Extracting evidence from a floppy disk using Linux.
- Challenges in disk forensics with Linux.
- Case study – Extracting evidence from a hard disk using Linux.
- Popular Linux forensics tools.

Module Flow



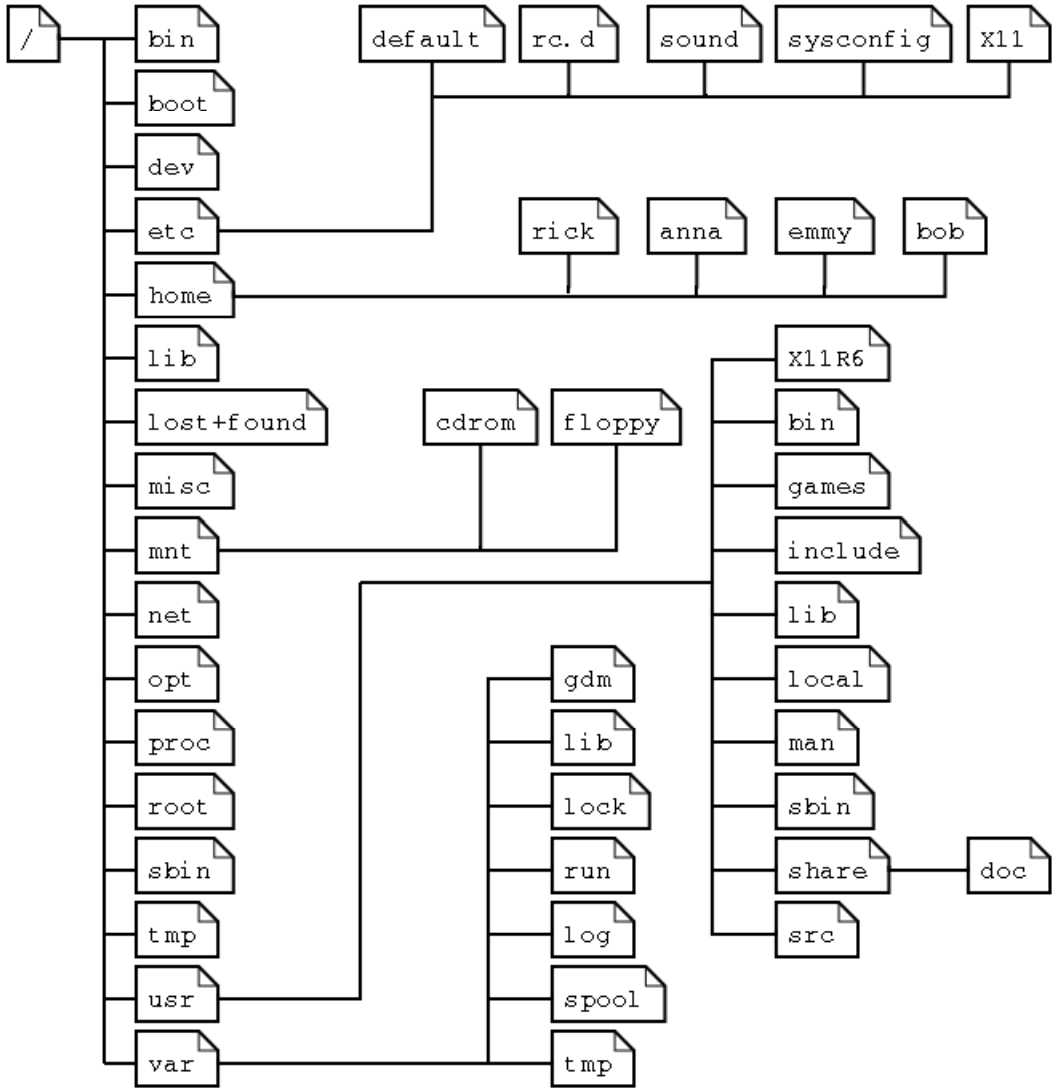
Use of Linux as a Forensics Tool

- **Why use Linux for forensics?**
  - Greater Control:
    - Treats every device as a file.
    - Does not need a separate write blocker.
  - Flexibility
    - Can be booted from a CD.
    - Can recognize several file systems.
  - Power
    - Distributions like THE FARMER'S BOOT CD and Sleuth make Linux a forensic tool in itself.

Recognizing Partitions in Linux

- If a standard IDE disk is being used, it will be referred to as "**hdx**“.
- The "**x**" is replaced with an "**a**" if the disk is connected to the primary IDE controller as master and with a "**b**" if the disk is connected to the primary IDE controller as a slave device.
- Similarly, the IDE disks connected to the secondary IDE controller as master and slave will be referred to as "**hdc**” and “**hdd**”, respectively.

File System in Linux



On most Linux distributions, the basic directory structure is organized like this.

File System Description

Directory	Content
/bin	Common programs, shared by the system, the system administrator and the users.
/boot	The startup files and the kernel, `vmlinuz`. In recent distributions also `grub` data. Grub is the GRand Unified Boot loader and is an attempt to get rid of the many different boot-loaders we know today.
/dev	Contains references to all the CPU peripheral hardware, which are represented as files with special properties.
/etc	Most important system configuration files are in `/etc`, this directory contains data similar to those in the Control Panel in Windows
/home	Home directories of the common users.
/initrd	(on some distributions) Information for booting. Do not remove!
/lib	Library files, includes files for all kinds of programs needed by the system and the users.
/lost+found	Every partition has a `lost+found` in its upper directory. Files that were saved during failures are here.
/misc	For miscellaneous purposes.
/mnt	Standard mount point for external file systems, e.g. a CD-ROM or a digital camera.
/net	Standard mount point for entire remote file systems
/opt	Typically contains extra and third party software.
/proc	A virtual file system containing information about system resources. More information about the meaning of the files in `proc` is obtained by entering the command **man *proc*** in a terminal window. The file proc.txt discusses the virtual file system in detail.
/root	The administrative user's home directory. Mind the difference between /, the root directory and /root, the home directory of the *root* user.
/sbin	Programs for use by the system and the system administrator.
/tmp	Temporary space for use by the system.
/usr	Programs, libraries, documentation etc. for all user-related programs.
/var	Storage for all variable files and temporary files created by users, such as log files, the mail queue, the print spooler area, space for temporary storage of files downloaded from the Internet, or to keep an image of a CD before burning it.

Mount Command

- Devices like floppies, CDs, hard disk partitions, and other storage devices must be attached to some existing directory on your system before they can be accessed.
- This attaching is called mounting, and the directory where the device is attached is called a mount point.
- After the device is mounted, you can access the files on that device by accessing the directory where the device is attached.
- When you're done and want to remove the floppy or CD or other device, you need to detach, unmount, it before removing it.
- When mounting, you must tell the mount command what is the device or partition you want to mount and what is the mount point. The mount point must be a directory that already exists on your system. For example, to mount your floppy:
  - `$ mount /dev/fd0 /mnt/floppy`
- When unmounting, you'll need to tell umount what mounted device to unmount:
  - `$ umount /dev/fd0`

Linux Boot Sequence

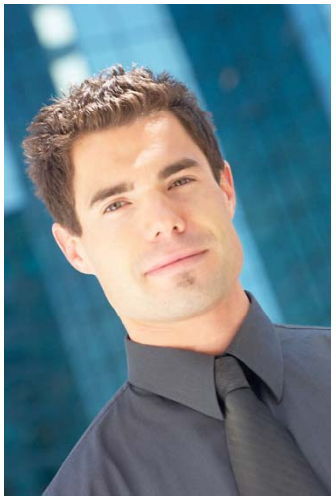
- The first step in the boot up sequence for Linux is loading the kernel. The kernel image is usually contained in the **/boot** directory.
- Details of the boot loader can be gained from LILO or GRUB using more **/etc/lilo.conf** or more **/etc/grub.conf.**
- The next step is initialization where runlevel and startup scripts are initialized and terminal process controlled.
- The file that controls the initialization is **/etc/inittab** and the file that begins the process is **/sbin/init.**

Linux Forensics

- Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier. These include:
  - **dd** - Command to copy data from an input file or device to an output file or device.
  - **sfdisk** and **fdisk** – Command to determine the disk structure.
  - **grep** – Command to search files for instances of an expression or pattern.
  - The **loop device** - Allows you to mount an image without having to rewrite the image to a disk.
  - **md5sum** and **sha1sum** – Command to create and store an MD5 or SHA hash of a file or list of files (including devices).
  - **file** – Command to read file header information in an attempt to ascertain its type, regardless of name or extension.
  - **xxd** - Command line hexdump tool.
  - **ghex** and **khexedit** -The Gnome and KDE (X Window interfaces) hex editors.

Case Example

- **Rebecca** had filed a lawsuit against Good Company, Inc. for **sexual harassment** by one of its senior directors, Mr. **Peter Samson.**
- She has submitted a floppy as evidence of Mr. Samson's advances.
- She has also discovered that Mr. Samson used to send her explicit material through floppy disks marked as legitimate work
- You, a forensic investigator, have been called to investigate the case on behalf of Good Company, Inc.
- How do you think he should proceed with the evidence?



Step-by-Step Approach to Case

1. Document all processes
   - Begin with creating a directory where all forensic activities can be done.
     - `/mkdir evidence`
   - It is desirable to create a special mount point for all physical subject disk analysis.
     - `mkdir /mnt/investigation`
2. Determine the disk structure
   - Create an image of the disk using the simple bit streaming command dd.
     - `dd if=/dev/fd0 of=image.suspectdisk`
   - Change the read-write permissions of the image to read-only using chmod.
     - `Chmod 444 image.suspectdisk`

Step-by-Step Approach to Case (cont'd)

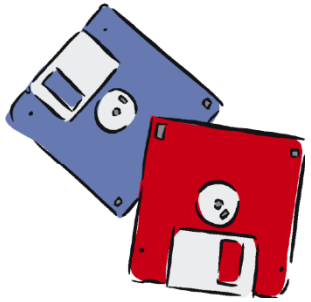
3. Mount the restored imaged working copy and analyze the contents:
   - `mount -t vfat -o ro,noexec /dev/fd0 /mnt/investigations`
   - Another option is to mount a point within the image file using the loop interface rather than mounting the contents to another location.
   - `mount -t vfat -o ro,noexec,loop image.suspectdisk /mnt/investigations`
4. Verify the integrity of the data on the imaged file by checking the file hash:
   - `md5sum /evidence/md5.image.suspectfile` or
   - `sha1sum -c /evidence/SHA. image.suspectfile`

Step-by-Step Approach to Case (cont'd)

5. Use the **ls** command to view the contents of the disk:
   - **ls –alR** to list all files including hidden files and list the directories recursively.
6. Make a list of all files along with access times:
   - **ls –laiRtu > /evidence/suspectfiles.list**
7. Search for likely evidence using:
   - **grep. grep -i xxx suspectfiles.list**
8. List unknown file extensions and changed file appearances:
   - **file changedfile**
   - Files can be viewed using **strings, cat, more** or **less.**

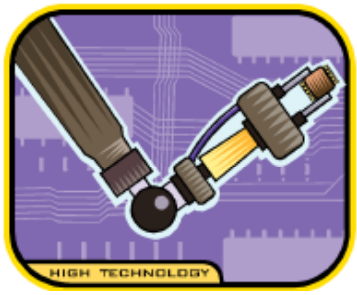
Step-by-Step Approach to Case (cont'd)

9. Search for certain keywords from the entire file list.
   - `cat /evidence/ suspectfiles.list | grep blackmailword`
   - A systematic approach to searching for keywords would be to create a keywords list. E.g. save it as:
     - `/evidence/keywordlist.txt`
   - grep the files for the keywords and save it to a file.
     - `grep –aibf keywordlist.txt image.suspectdisk > results.txt`
   - View the results:
     - `cat results.txt`
   - To analyze the files at each offset, use the hexdump tool:
     - `xxd -s (offset) image.suspectdisk | less`



Challenges In Disk Forensics With Linux

- Linux cannot identify the last sector on hard drives with odd number of sectors.
- Most Linux tools are complicated as they are used at the command line.
- Devices can be written to even if they are not mounted.
- Bugs in the open source tools can be used to question the credibility of the tool for forensics use.
- Forensic and Incident Response Environment (F.I.R.E) by William Salusky provides a good tool set.

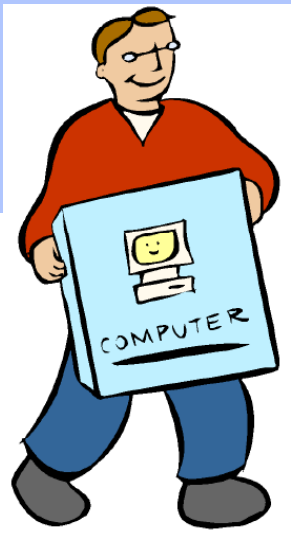


Jason Smith Case

- Mr. Jason Smith has been accused of hoarding illegal material of questionable moral content on his company network systems.
- You have been called upon to examine the suspect hard disk, and unearth evidence related to the said illegal material.
- How do you think you should proceed in extracting and preserving the evidence?

Step-by-Step Approach to Case

1. Note the model information from the hard disk label /manufacturer's Web site, and the size and total number of sectors on the drive.
2. Wipe and format a image disk drive using the ext3 file system (> 3x evidence size).
3. Fill the disk with zeros and ensure that the contents match.
   - `dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync`
4. Partition the disk and reboot.
   - `fdisk /dev/hda`
5. Format with the ext3 file system.
   - `mkfs –t ext3 /dev/image.disk`



Step-by-Step Approach to Case (cont'd)

6. Prepare the disk for imaging:
   a. Mount the freshly prepared read-write image disk.
      a. `mount /dev/hda /mnt/image.disk`
   b. Create a directory for all documentation and analysis.
      a. `mkdir /mnt/image.disk/case_no`
   c. Create a sub-directory to hold the evidence image.
      a. `mkdir /mnt/image.disk/case_no/evidence_no`
   d. Document details of the investigation in a text file including investigator's details, case background details, and investigation dates.
   e. Carry out Document details of the disk media including investigator name and organization, case number, media evidence number, date and time of imaging; make, model, and serial number of computer, IP and system hostname; make, model, and serial number of HD, source of HD and scope of investigation.

Step-by-Step Approach to Case (cont'd)

7. Image the disk.
   a. Connect both original evidence drive and drive to be imaged to the Imaging System.
   b. Verify all jumper settings – Master / Slave.
   c. Make sure that the imaging system will boot only from CD by checking the BIOS settings.
   d. Image the disk using **dd.**

      ```
      dd if=/dev/hdx of=image.disk conv=noerror,sync
      ```

      This will allow **dd** to try to ignore any errors (**conv=noerror**) and synchronize the output (**sync**) with the original.
8. Check for accuracy by comparing md5sum.
9. Mount the disk and extract evidence.
10. Images can be carved using **dd** or the hex dump tool **xxd.**

Popular Linux Forensics Tools

- The Sleuth Kit - written by Brian Carrier and maintained at http://www.sleuthkit.org.
- Autopsy – HTML front-end for sleuthkit.
- SMART for Linux- by ASR Data, is a commercial data forensics program that runs on Linux.
- THE FARMER'S BOOT CD- by farmerdude, is a bootable CD that is oriented toward fast previewing of data in a forensically sound manner.
- Penguin Sleuth - Knoppix based linux distribution with a forensic flavor.
- Forensix

The Sleuth Kit

- **The Sleuth Kit** is a collection of command line digital investigation tools. The tools run on Linux, OS X, FreeBSD, OpenBSD, and Solaris and can analyze FAT, NTFS, UFS, EXT2FS, and EXT3FS.
- **The Autopsy Forensic Browser** is an HTML-based graphical interface for the command line tools in The Sleuth Kit. This makes it much easier and faster to investigate a system.
- **mac-robber** is a tool that will collect temporal data from mounted file systems. The data can be used to make a timeline of file activity on the system using tools from The Sleuth Kit.

Tools in "The Sleuth Kit"

- File System Layer Tools
  - `fsstat`
- File Name Layer Tools
  - `ffind`
  - `fls`
- Meta Data Layer Tools
  - `icat`
  - `ifind`
  - `ils`
  - `istat`
- Data Unit Layer Tools
  - `dcat`
  - `dls`
  - `dstat`
  - `dcalc`
- File System Journal Tools
  - `jcat`
  - `jls`
- Media Management Tools
  - `mmls`
- Image File Tools
  - `img_stat`
  - `mg_cat`
- Disk Tools
  - `disk_sreset`
  - `disk_stat`
- Other Tools
  - `hfind`
  - `mactime`
  - `sorter`
  - `sigfind`

Autopsy

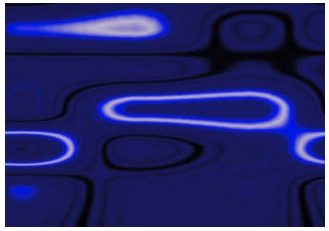
- The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).
- The Sleuth Kit and Autopsy are both Open Source and run on UNIX platforms. As Autopsy is HTML-based, you can connect to the Autopsy server from any platform using an HTML browser.
- Autopsy provides a "File Manager"-like interface and shows details about deleted data and file system structures.

The Evidence Analysis Techniques in Autopsy

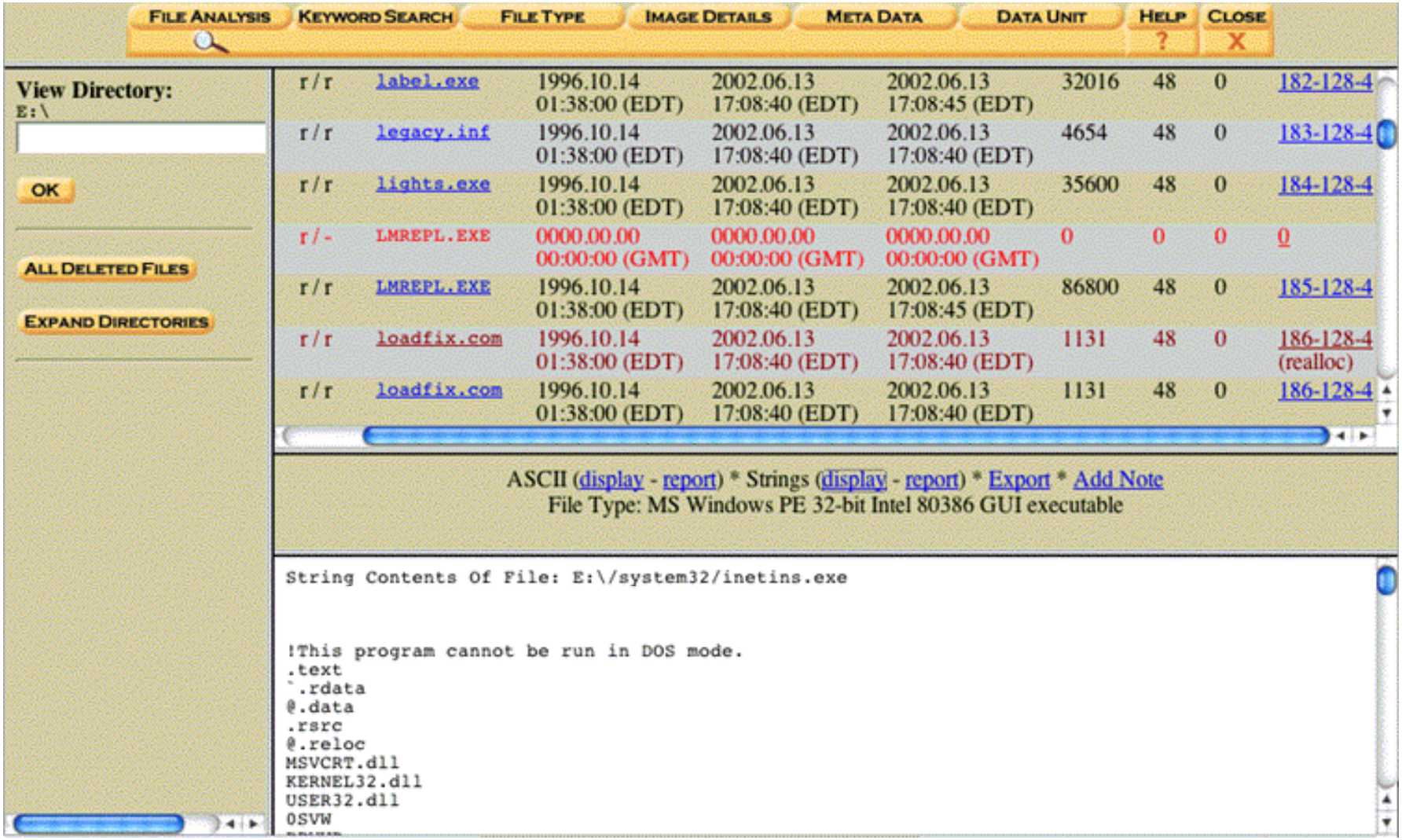
1. **File Listing:**
   - Analyze the files and directories, including the names of deleted files and files with Unicode-based names.
2. **File Content:**
   - The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted.
3. **Hash Databases:**
   - Lookup unknown files in a hash database to quickly identify it as good or bad.
4. **File Type Sorting:**
   - Sort the files based on their internal signatures to identify files of a known type.
5. **Timeline of File Activity:**
   - Create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files.

The Evidence Analysis Techniques in Autopsy (cont'd)

6. **Keyword Search:**
   - Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions.
7. **Meta Data Analysis:**
   - It allows you to view the details of any meta data structure in the file system.
8. **Data Unit Analysis:**
   - It allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings.
9. **Image Details:**
   - You can view the file system details, including on-disk layout and the time of activity so that it is possible to recover data.



Autopsy – File Listing



Autopsy – File Content

Autopsy – Hash Databases

NSRL Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe
a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

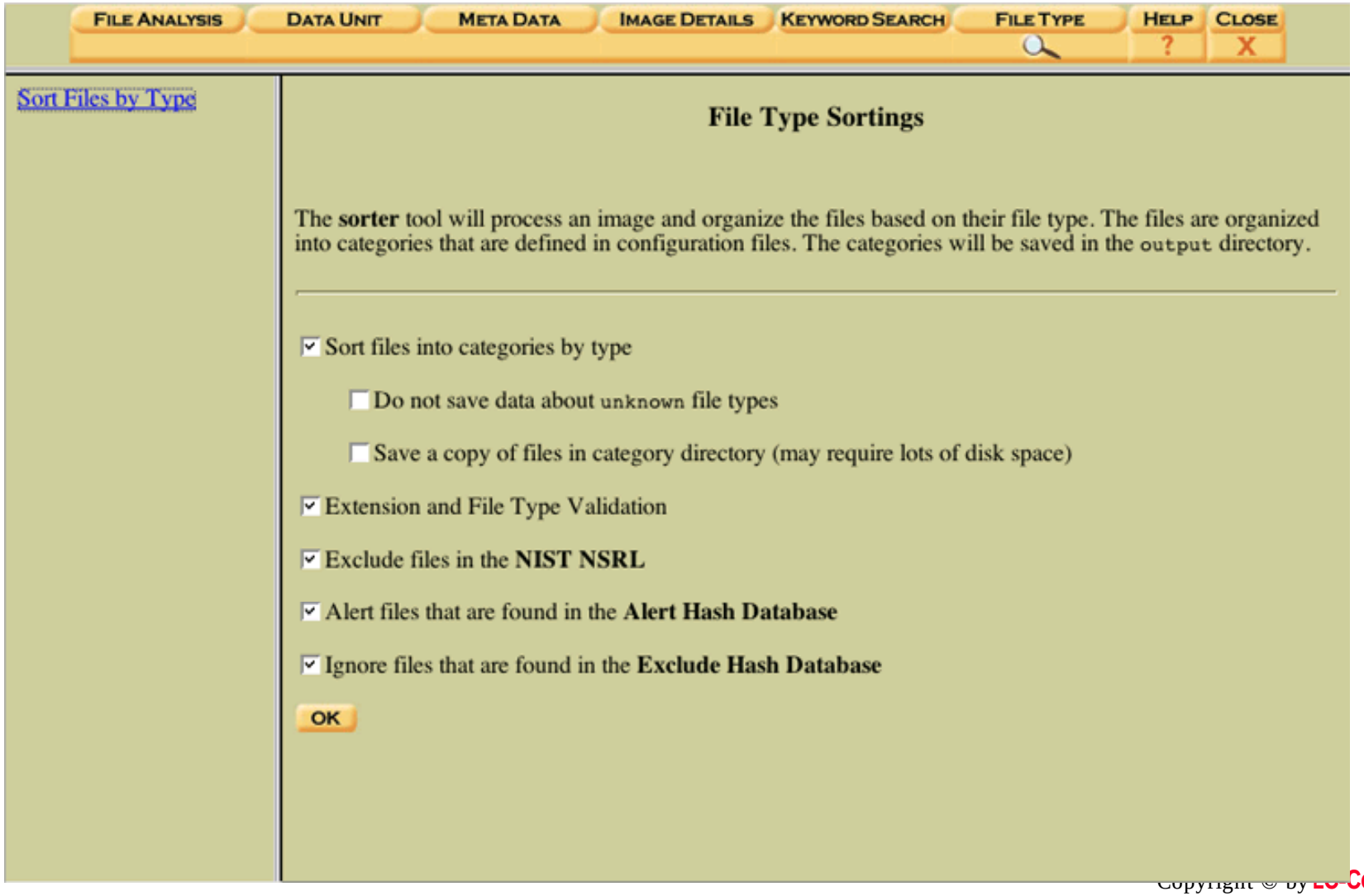
Exclude Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

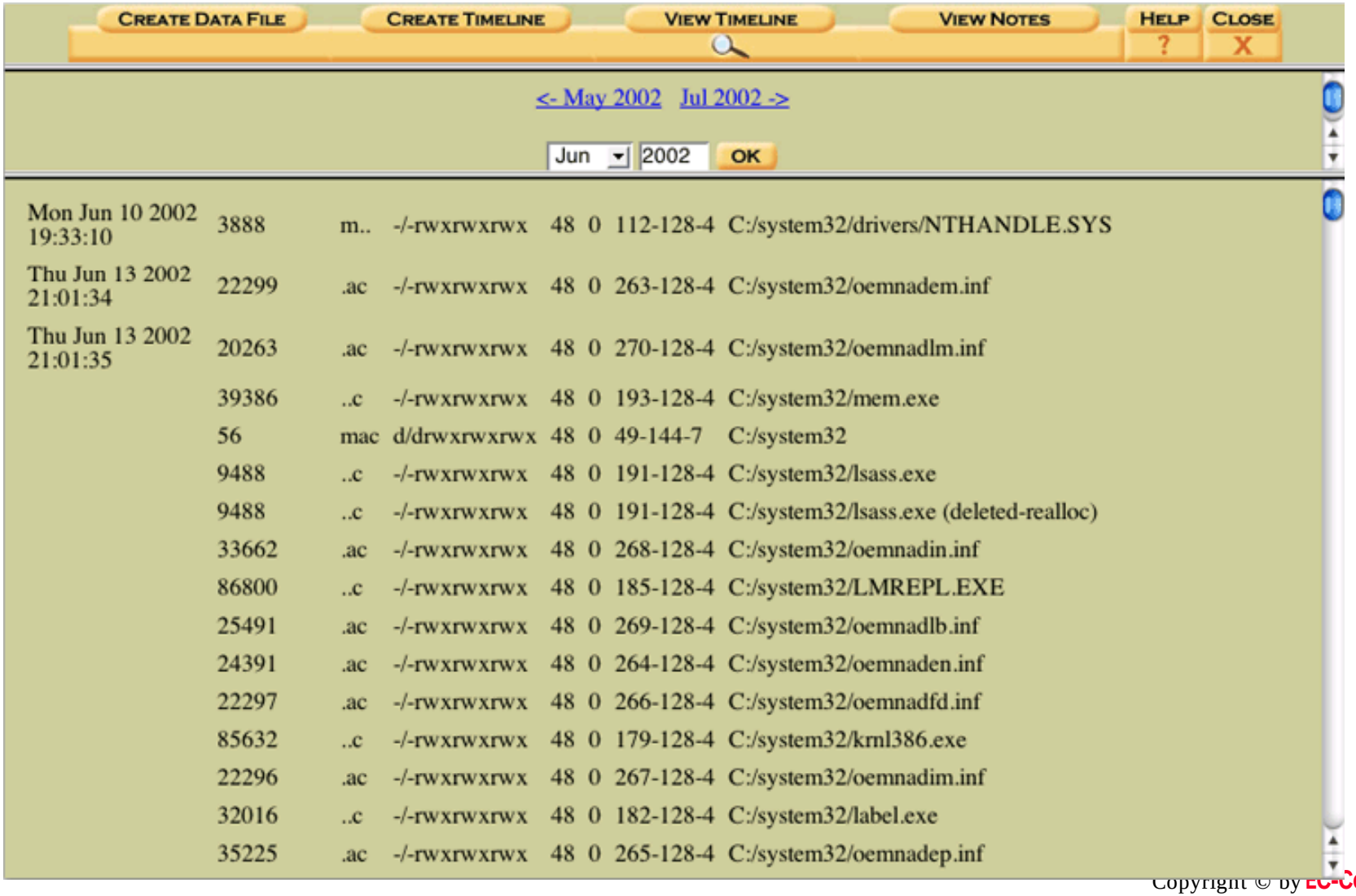
Alert Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

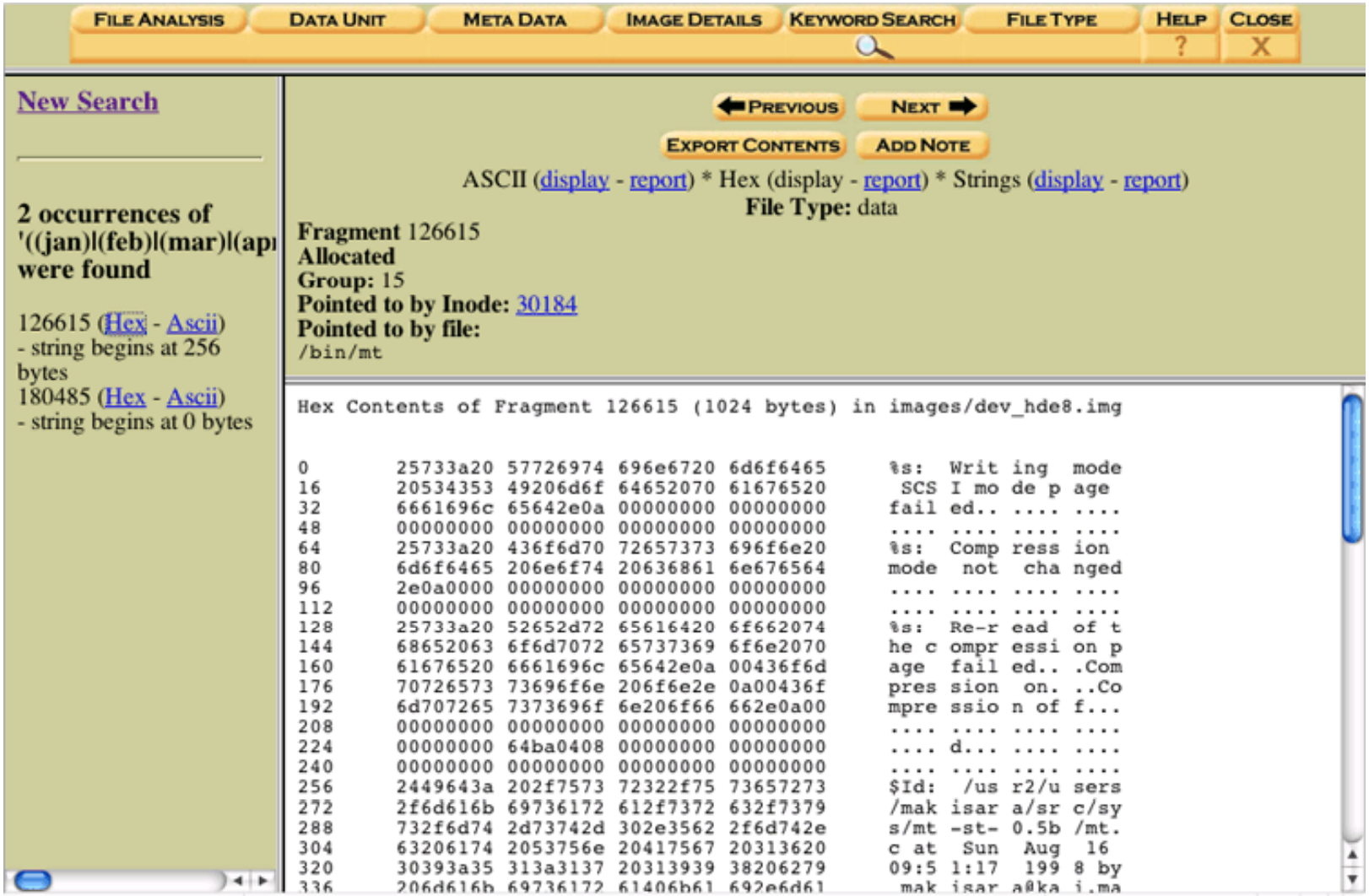
Autopsy – File Type Sorting



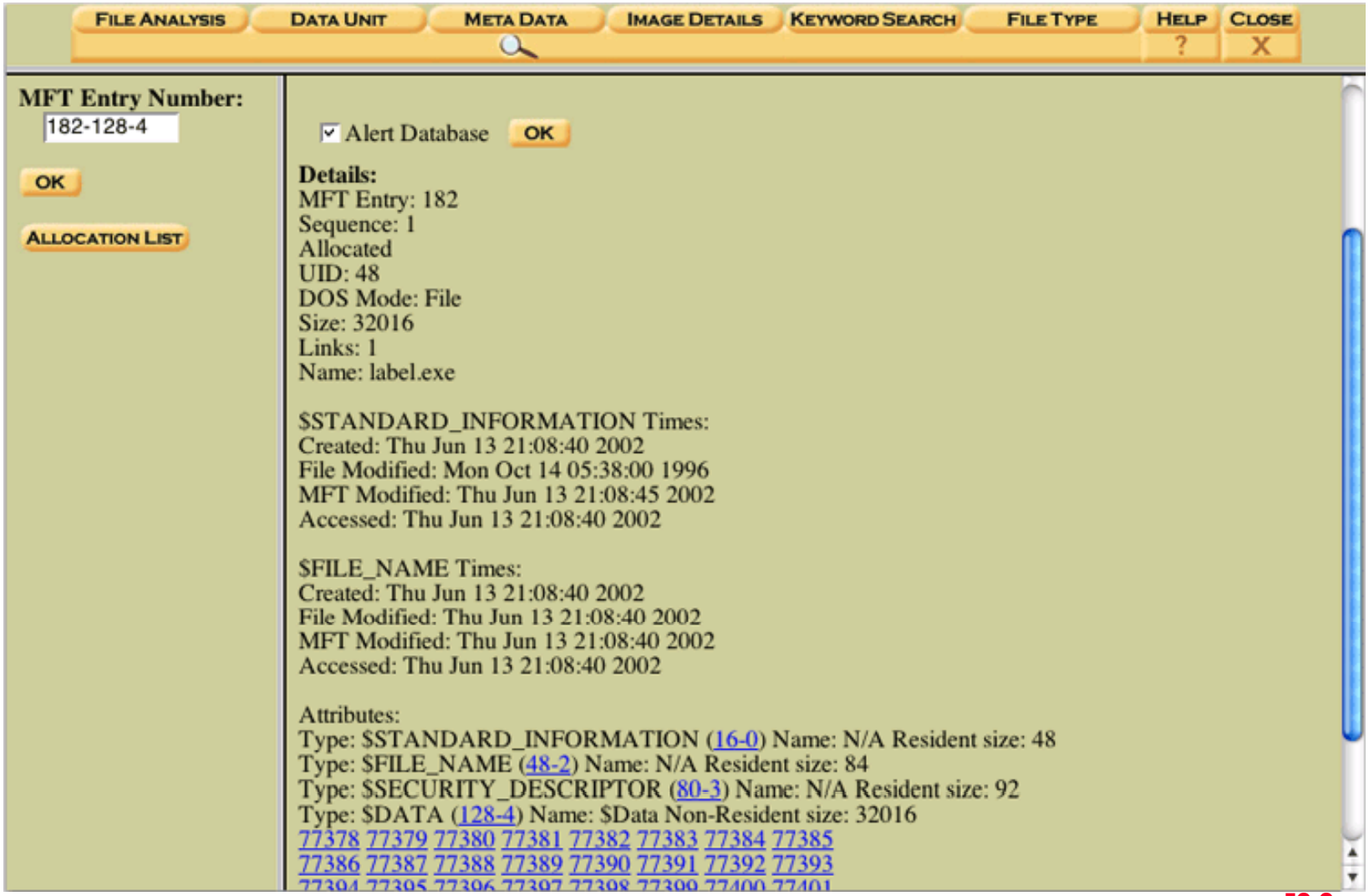
Autopsy – Timeline of File Activity



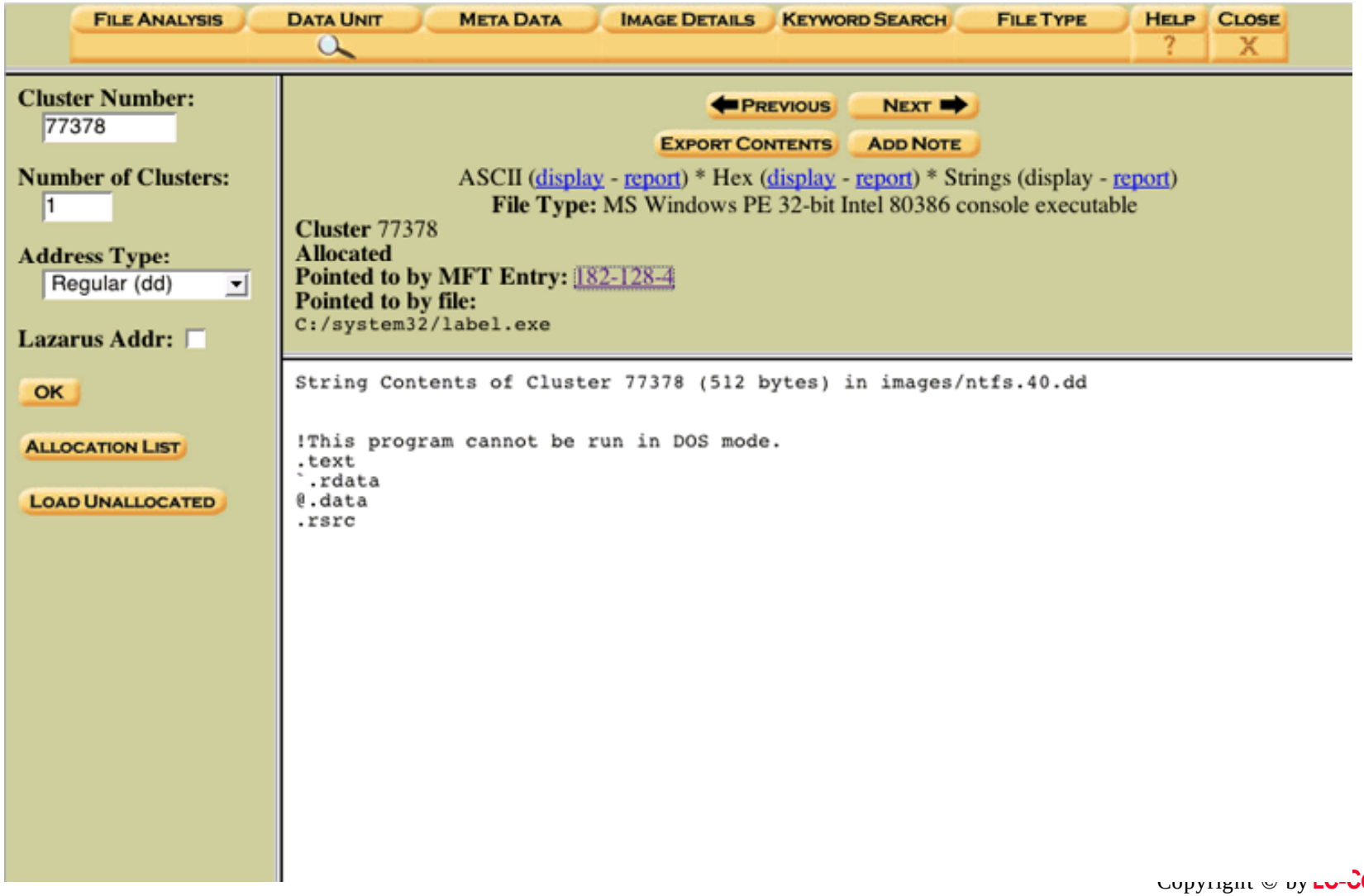
Autopsy – Keyword Search



Autopsy – Meta Data Analysis



Autopsy – Data Unit Analysis



Autopsy – Image Details

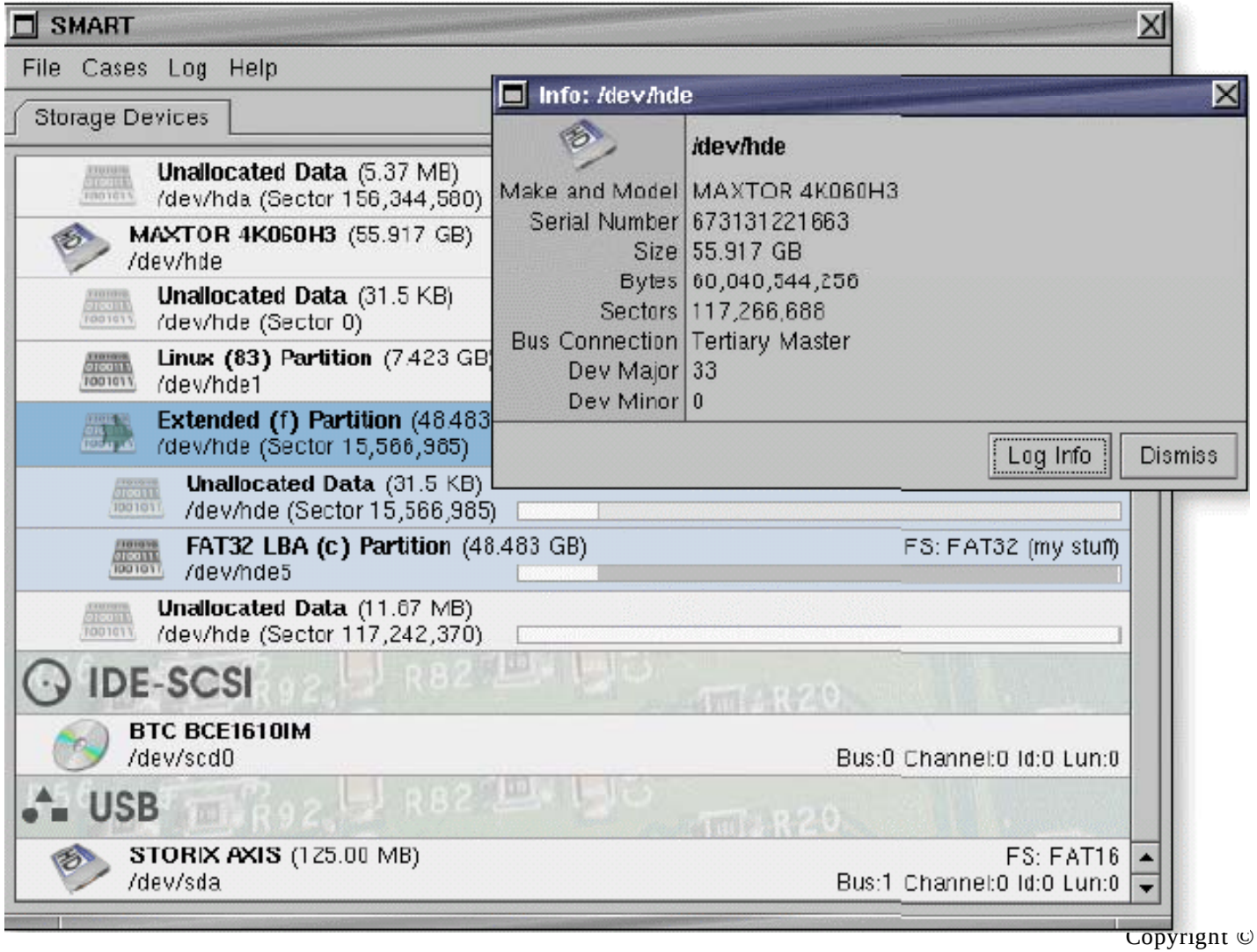
SMART for Linux

- SMART is a software utility that has been designed and optimized to support data forensic practitioners and Information Security personnel in pursuit of their respective duties and goals.
- It is known as 'The Next Generation Data Forensic Tool'.
- Functions of SMART:
  - "Knock-and-talk" inquiries and investigations.
  - On-site or remote preview of a target system.
  - Post mortem analysis of a dead system.
  - Testing and verification of other forensic programs.
  - Conversion of proprietary "evidence file" formats.
  - Baselining of a system.

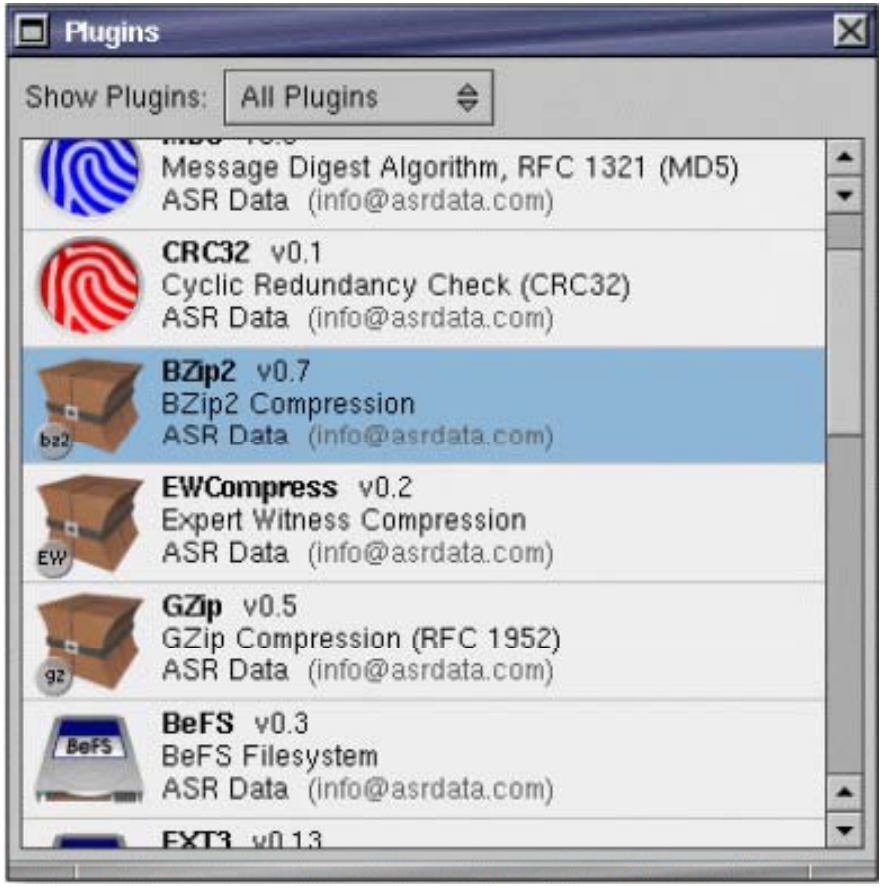
Features of SMART for Linux

- SMART lists connected storage devices in the main window list.
- It uses plugins to do much of the work, and the application itself utilizes a highly modular design philosophy.
- It is multi-threaded.
- Its powerful, flexible acquisition options allow you to create pure bit-image copies and quasiproprietary formats that support seekable compression.
- It can acquire and clone a single source to any number of images and devices simultaneously.
- It generates lots of information about hashes.
- It provides the ability to perform real authentication.
- It gives you an easy interface to linux mounts, and GUI environments like KDE and GNOME.
- It enables complex tasks and search result rules to be applied automatically.

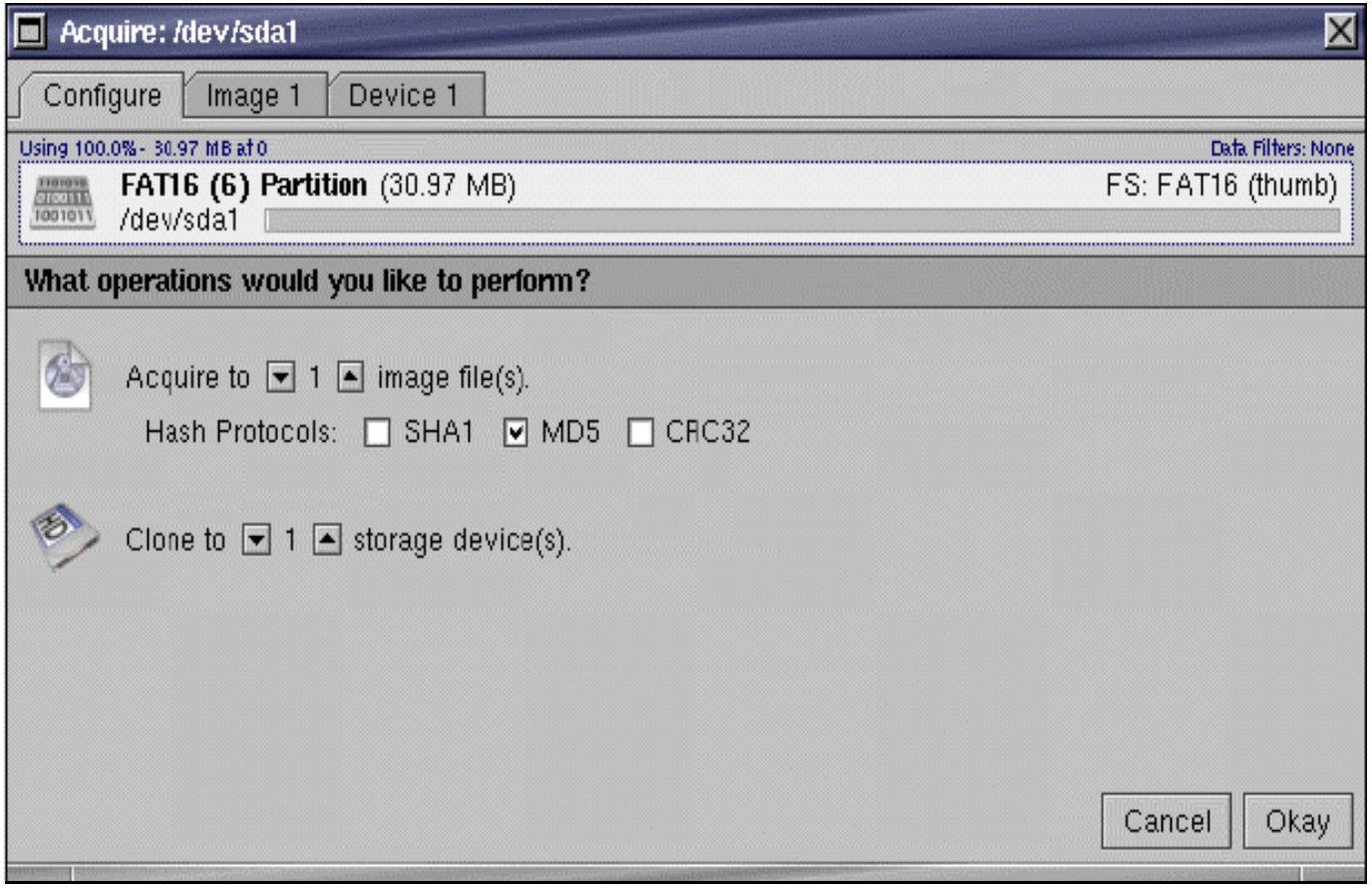
Screenshots



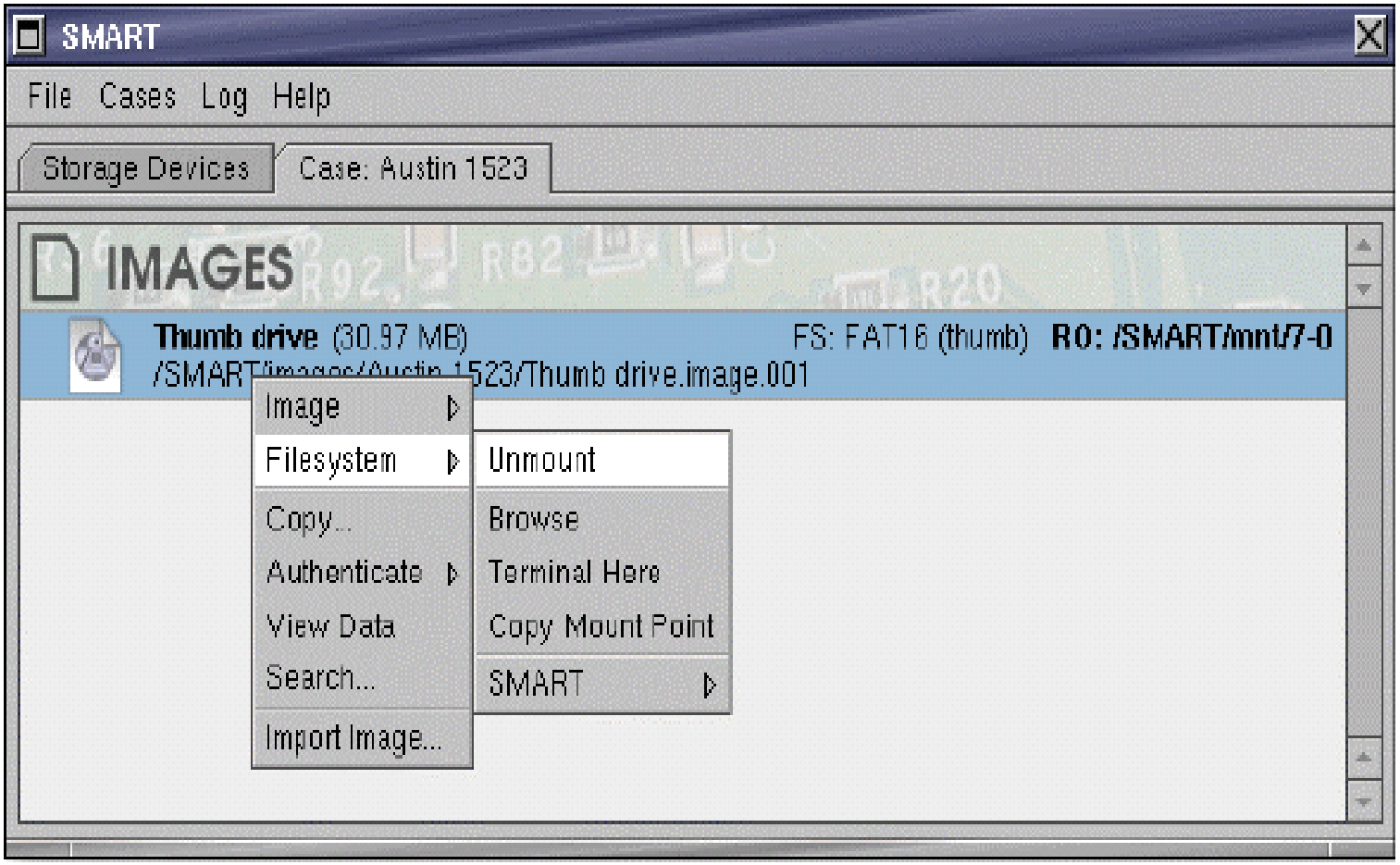
Screenshots



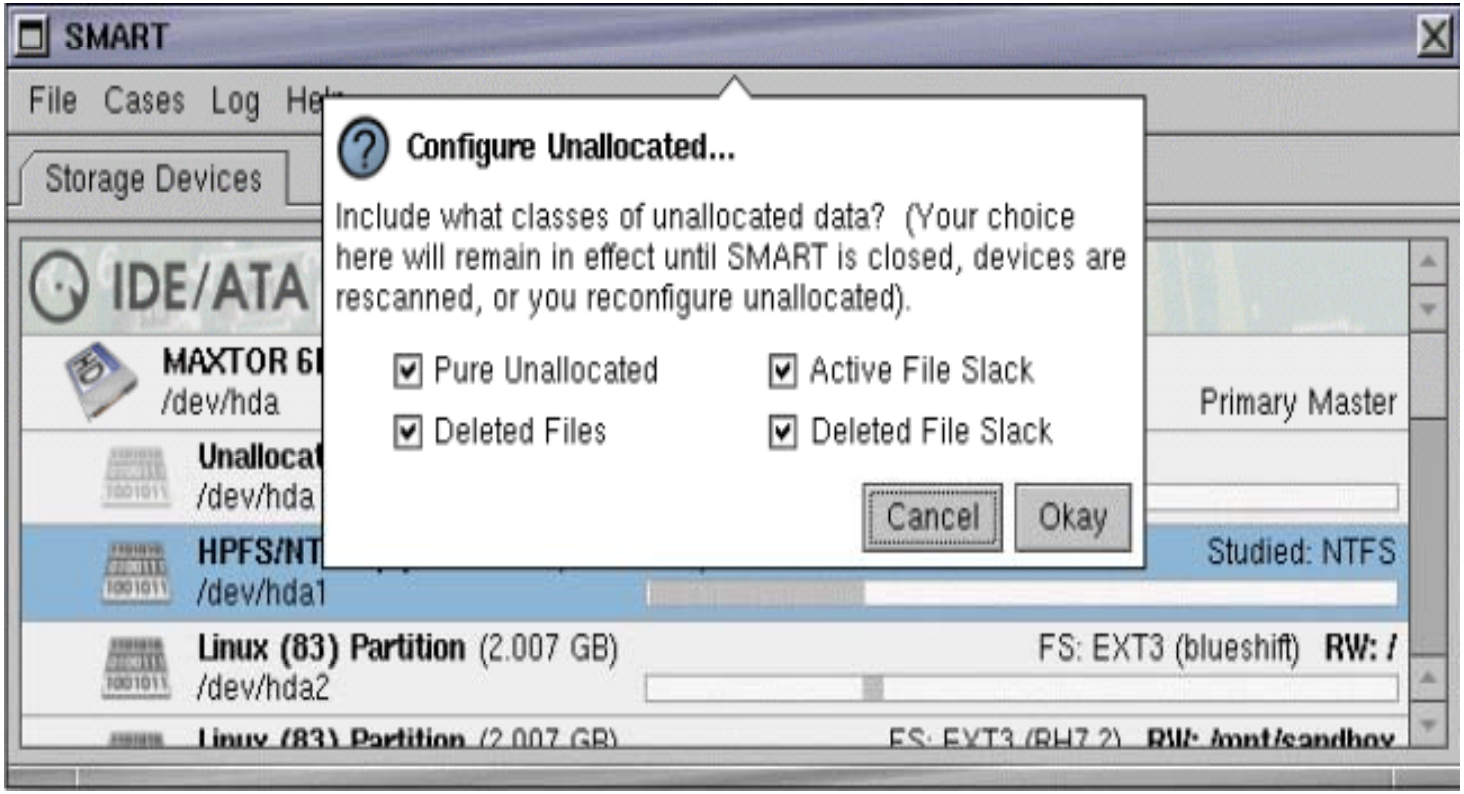
Screenshots



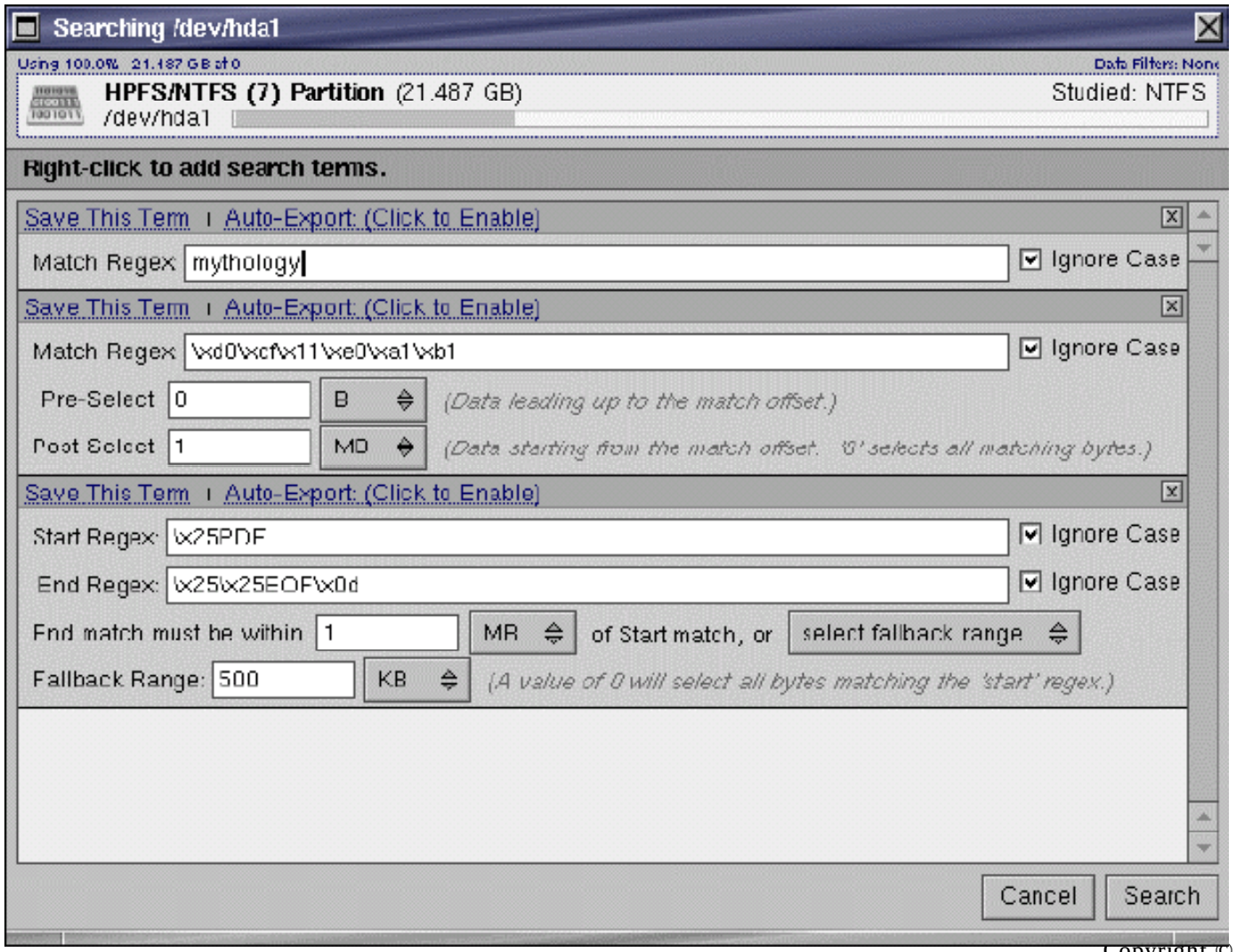
Screenshots



Screenshots



Screenshots



Penguin Sleuth

- The Penguin Sleuth Kit is a bootable Linux distribution based on KNOPPIX.
- It is the collection of some very useful tools, including The Coroner's Toolkit (TCT), Autopsy, and The Sleuth Kit, as well as penetration testing and virus scanning tools.
- It offers a GUI environment, as well as the good, old-fashioned command line environment fitting the novice user to the experienced user.

Tools Included in Penguin Sleuth Kit

- **Sleuth Kit** - Command Line Forensic Tools
- **Autopsy** - Part of Sleuth Kit
- **Foremost** - Command line data carving tool
- **Glimpse** - Command line data indexing and searching tool
- **Wipe** - Command line utility to securely wipe hard drives and files
- **Etherape** - Visual network monitor
- **Fenris** - Multipurpose tracer
- **Honeyd** - Command line honypot program
- **Snort** - Command line network intrusion tool
- **Dsniff** - Command Line network auditing and penetration testing tools
- **John The Ripper** - Command Line Password Cracking tool
- **Nikto** - Webserver scanner

Tools Included in Penguin Sleuth Kit (cont'd)

- **Nbtscan** - Command-line tool that scans for open NETBIOS nameservers
- **Xprobe** - Command line remote operating system fingerprinting tool
- **Ngrep** - Command line Network grep Function
- **Nemesis** - Command Line network packet injector
- **Fragroute** - Command line network intrusion testing tool
- **Fping** - Command line multiple host ping utility
- **TCPtraceroute** - Command line traceroute TCP packages
- **TCPReplay** - Command line utility that replays a TCP dump
- **Nessus** - Graphical Security Scanner
- **Ethereal** - Graphical Network analyzer
- **Netcat** - Command line tool to read and write over network
- **TCPdump** - Command line tool that dumps network traffic

Tools Included in Penguin Sleuth Kit (cont'd)

- **Hping2** - Command line packet assembler / analyzer
- **Ettercap** - Command line sniffer / interceptor / logger for Ethernet networks
- **Openssh** - Secure remote connection utility
- **Kismet** - Graphical wireless network sniffer
- **AirSnort** - Graphical wireless network intrusion tool
- **GPG** - Encryption utility
- **OpenSSL** - Secure remote connection utility
- **Lsof** - Command line utility that lists all open files
- **Hunt** - Command line TCP / IP exploit scanner
- **Stunnel** - SSL connection package
- **ARPwatch** - Command line Ethernet monitor
- **Dig** - Command line tool for querying domain name servers
- **Chkrootkit** - Looks for signs of root kit

Forensix

- The goal of the Forensix ("4N6") Project is to allow a system to be monitored so that, in the event of a security compromise, it is easy to track the compromise back to its source and recover from it.

  Source: http://forensix.sourceforge.net/

- Forensix performs a complete kernel event audit on the target system and streams the high-definition audit trail to a backend database that has been optimized for reconstruction queries.

- Functions:
  - Accurately replaying any and all system compromises.
  - Determining what specific data (such as credit card numbers) has been accessed on the system as a result of a compromise.
  - Automatically determining what modifications have been made to a system by an illicit user.
  - Selectively "undo"-ing illicit system modifications.

Maresware

- Linux Forensics provides tools for investigating computer records while running the LINUX operating system on Intel processors.
- Maresware is useful to all types of investigators, including law enforcement, intelligence agency, private investigator, and corporate internal investigators.
- This software enables discovery of evidence for use in criminal or civil legal proceedings.
- http://www.dmares.com/maresware/linux_forensics.htm

Maresware

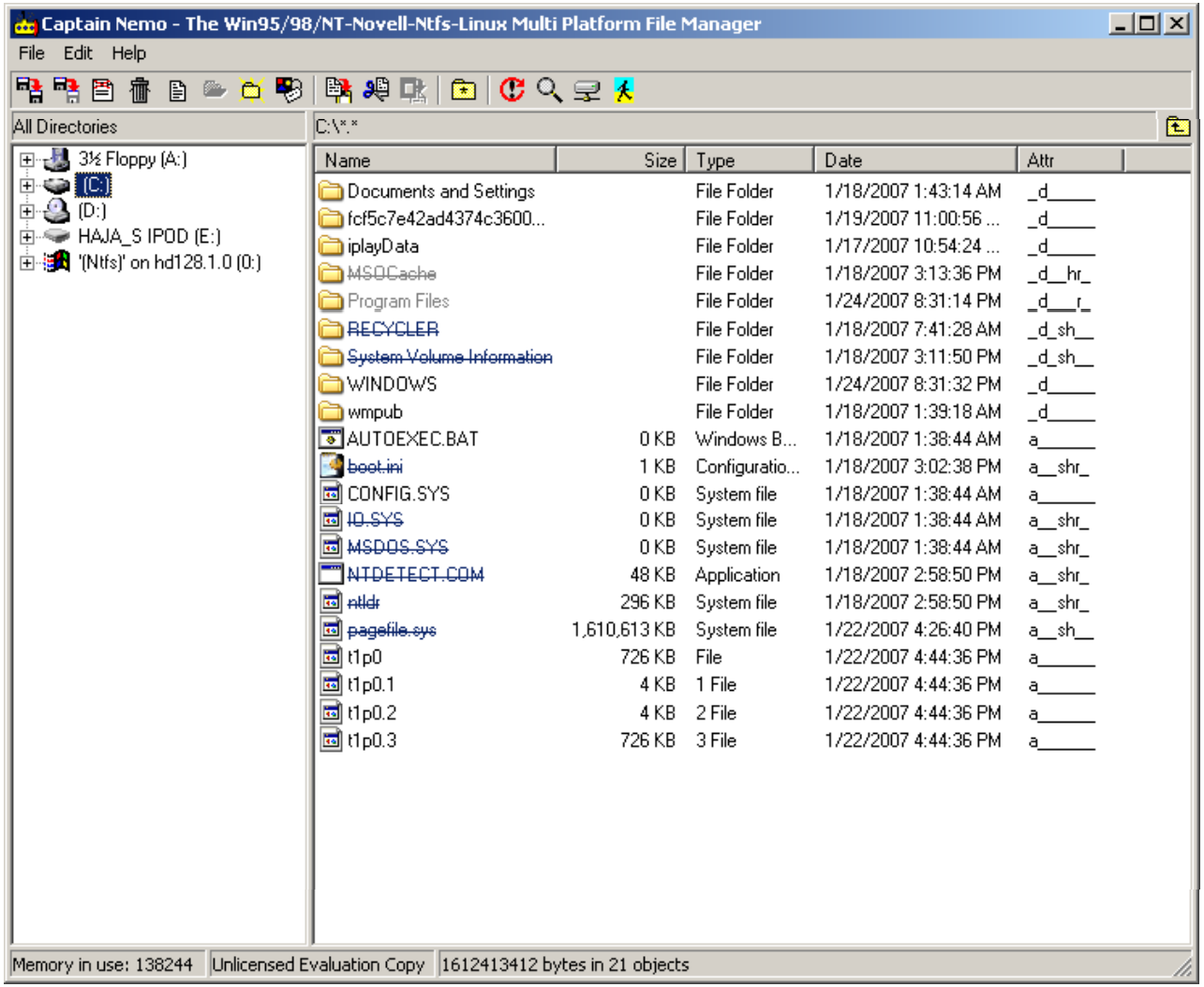
Major Programs Present in Maresware

- Bates_no:
  - A unique program for adding identifying numbers to filenames in e-documents.
- Catalog:
  - Catalogs every file on a Linux file system and identifies headers.
- Hash:
  - Performs MD5 (CRC, or SHA) hash of every file on a drive.
- Hashcmp:
  - Compares outputs of successive hash runs.
- Md5:
  - Calculates MD5 hash of a file.
- Strsrch:
  - Searches files for text strings.
- U_to_A:
  - Converts *ix text to DOS text.

Captain Nemo

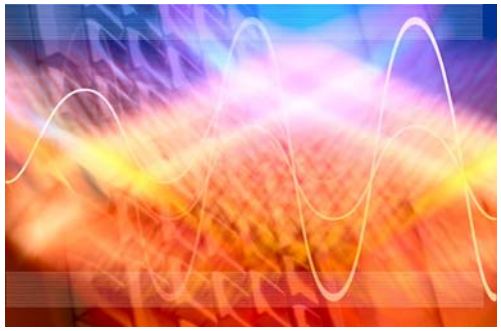
- Widely used by law enforcement personnel, forensic investigators, and network administrators. Captain Nemo enables you to access any Linux drive from your Windows computer, without requiring a network setup.
- Just connect the Linux drive to your machine, and Captain Nemo will let you mount your Linux partitions in Windows.
- You can read, search, and view all your Linux files and copy them to your Windows drive.
- Supports ext2fs and ext3fs

Screenshot

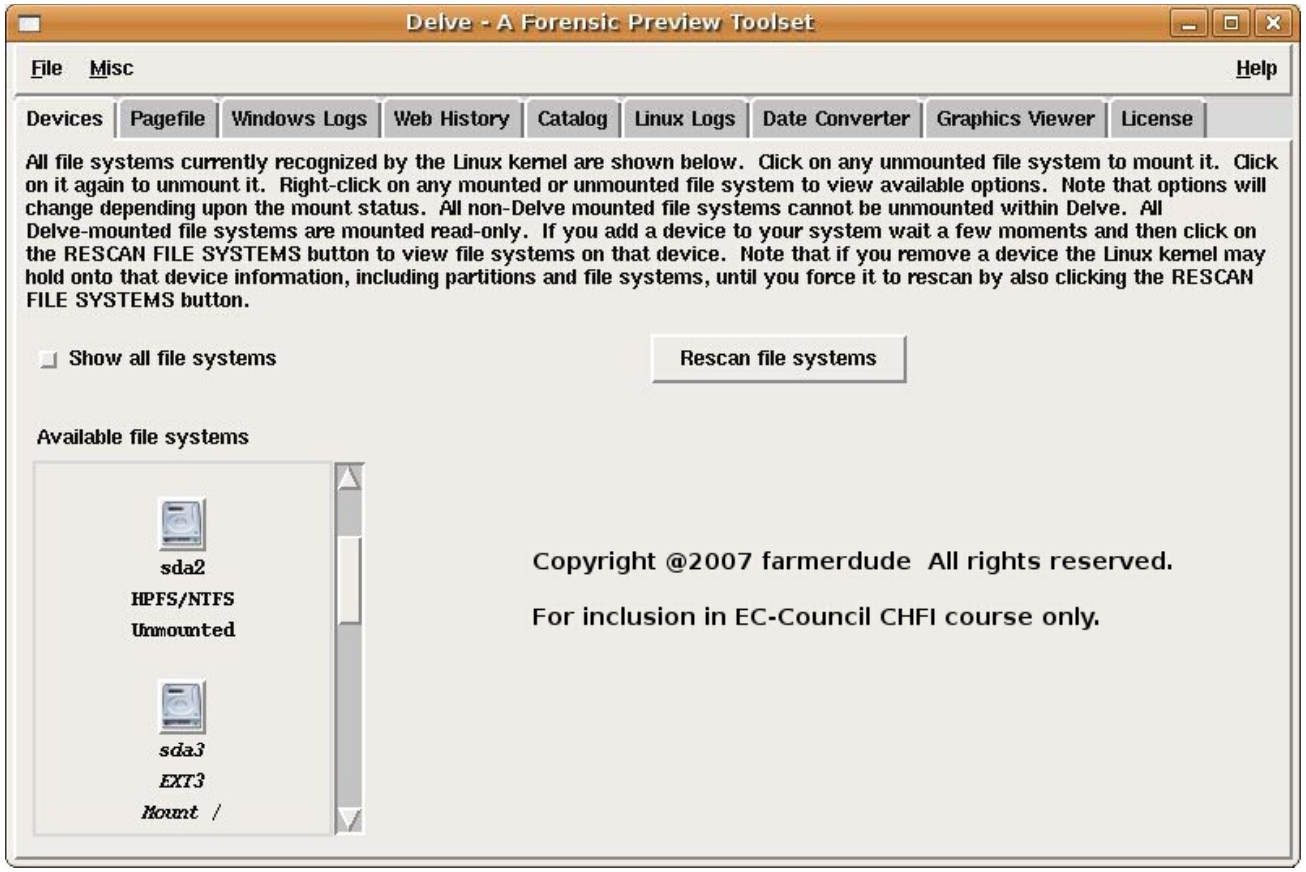


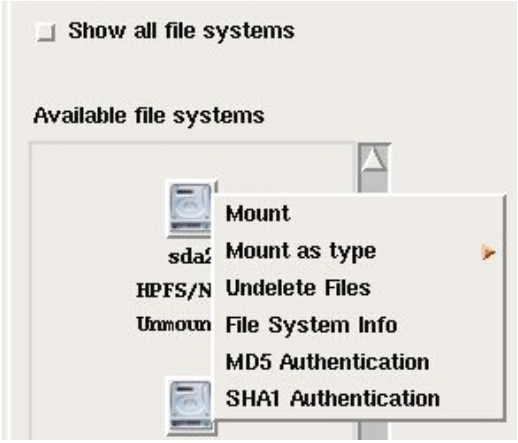
THE FARMER'S BOOT CD

- THE FARMER'S BOOT CD allows you to examine hard disks directly from Linux,
- Boots most any x86 system and mounts file systems in a forensically sound manner.
- Preview data using a single, unified graphical user interface (GUI).
- Acquire media after you've previewed the data and found it pertinent to your investigation.
- http://www.forensicbootcd.com

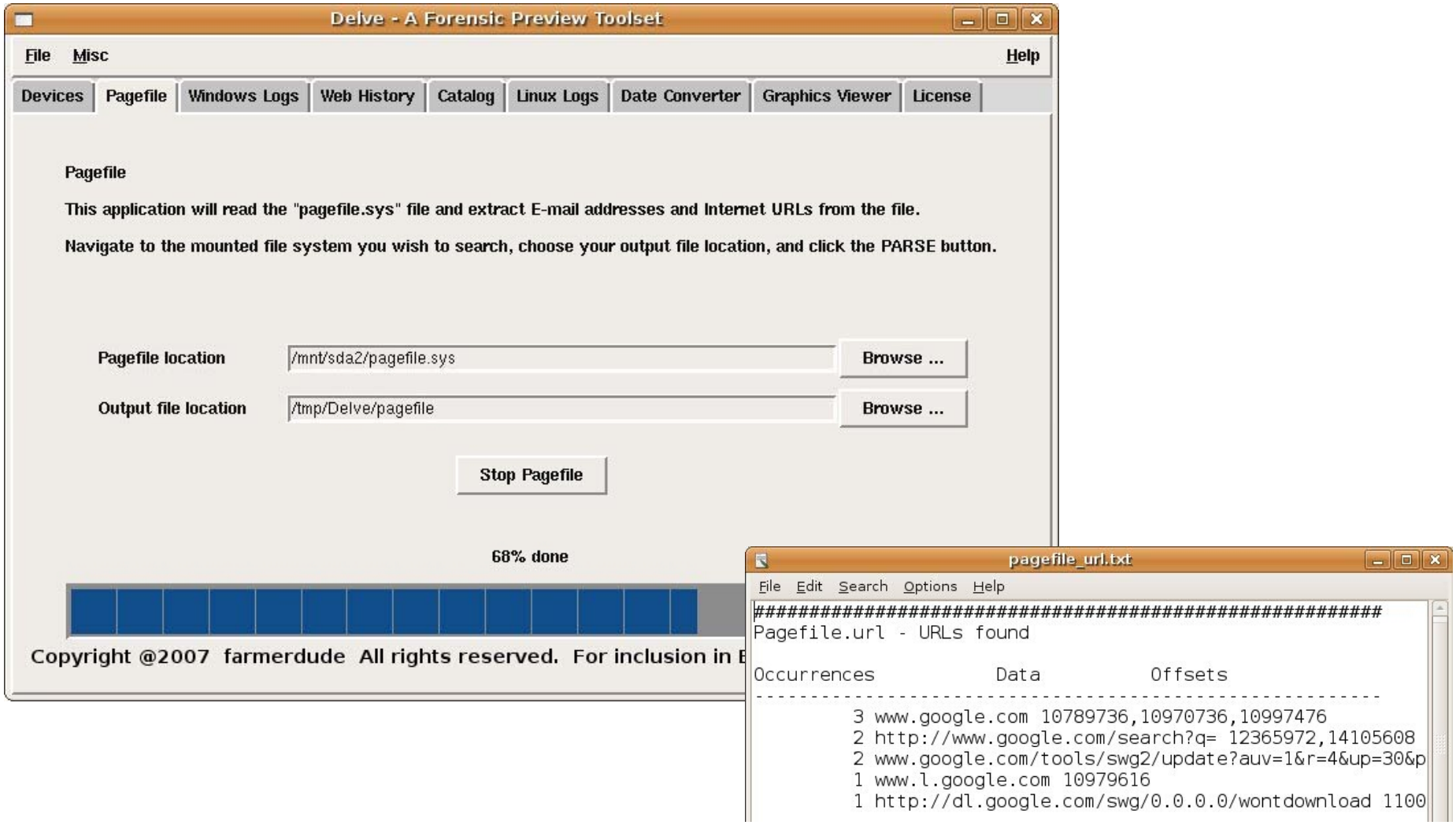


Screenshots

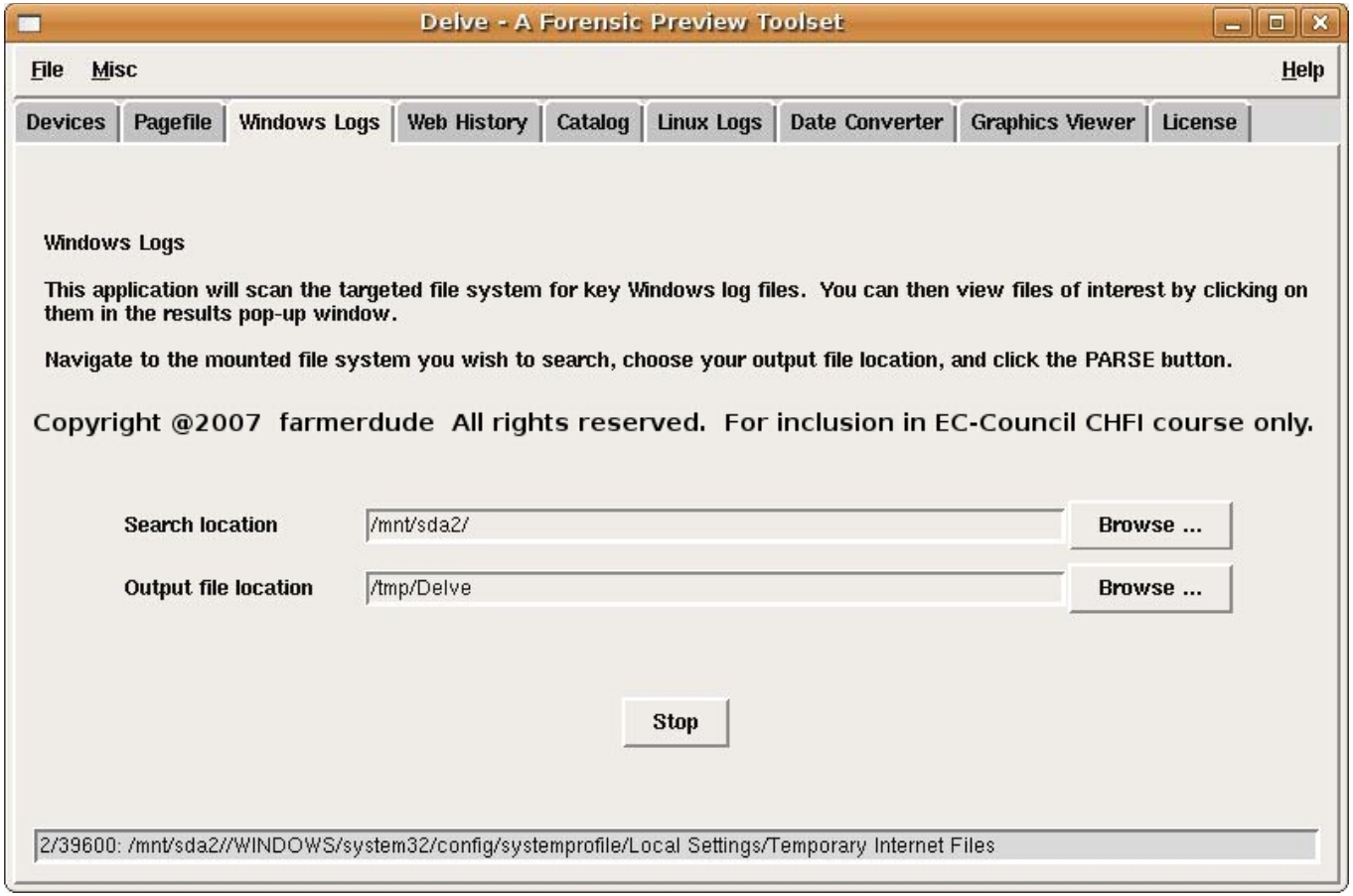




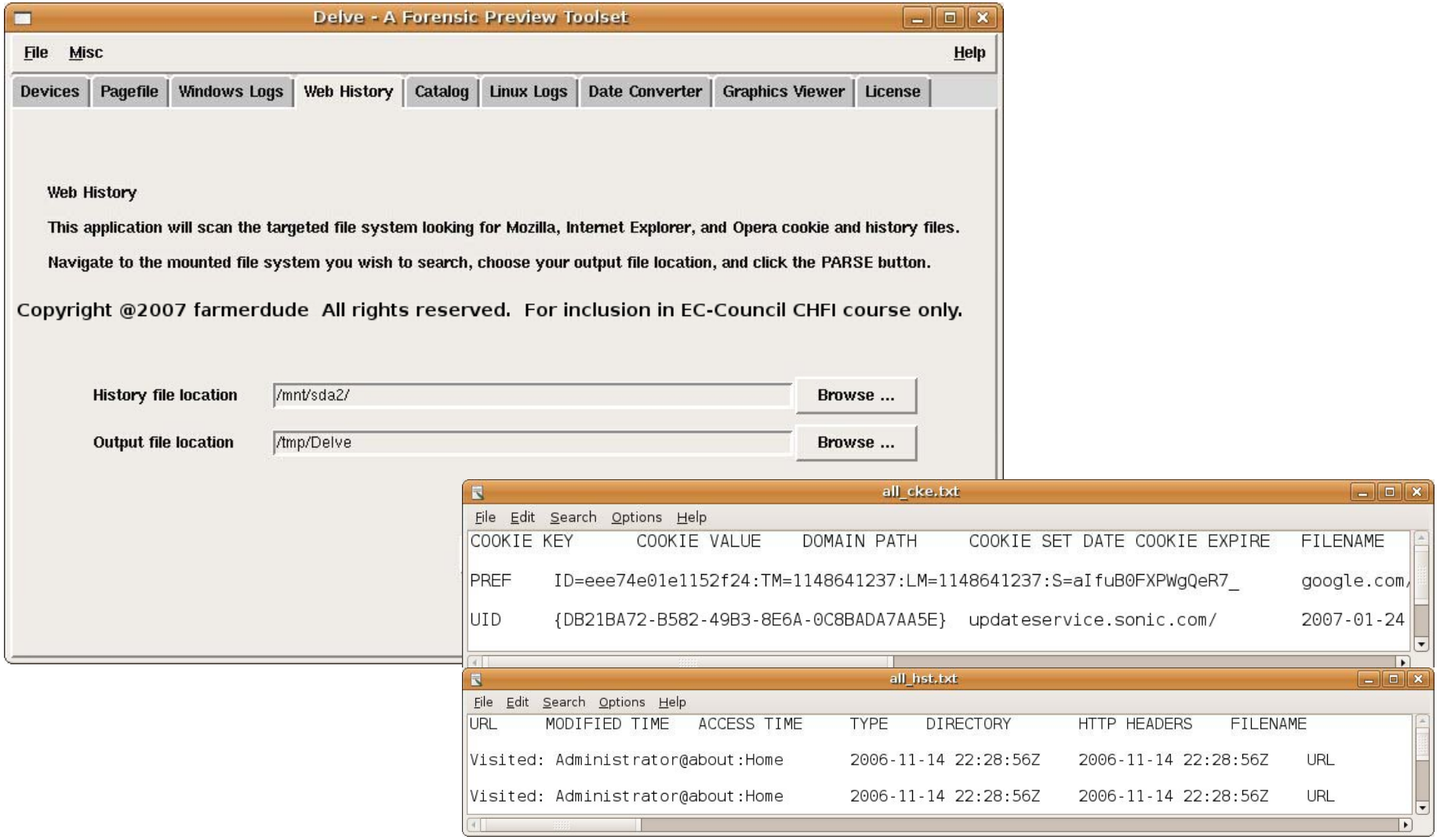
Screenshots



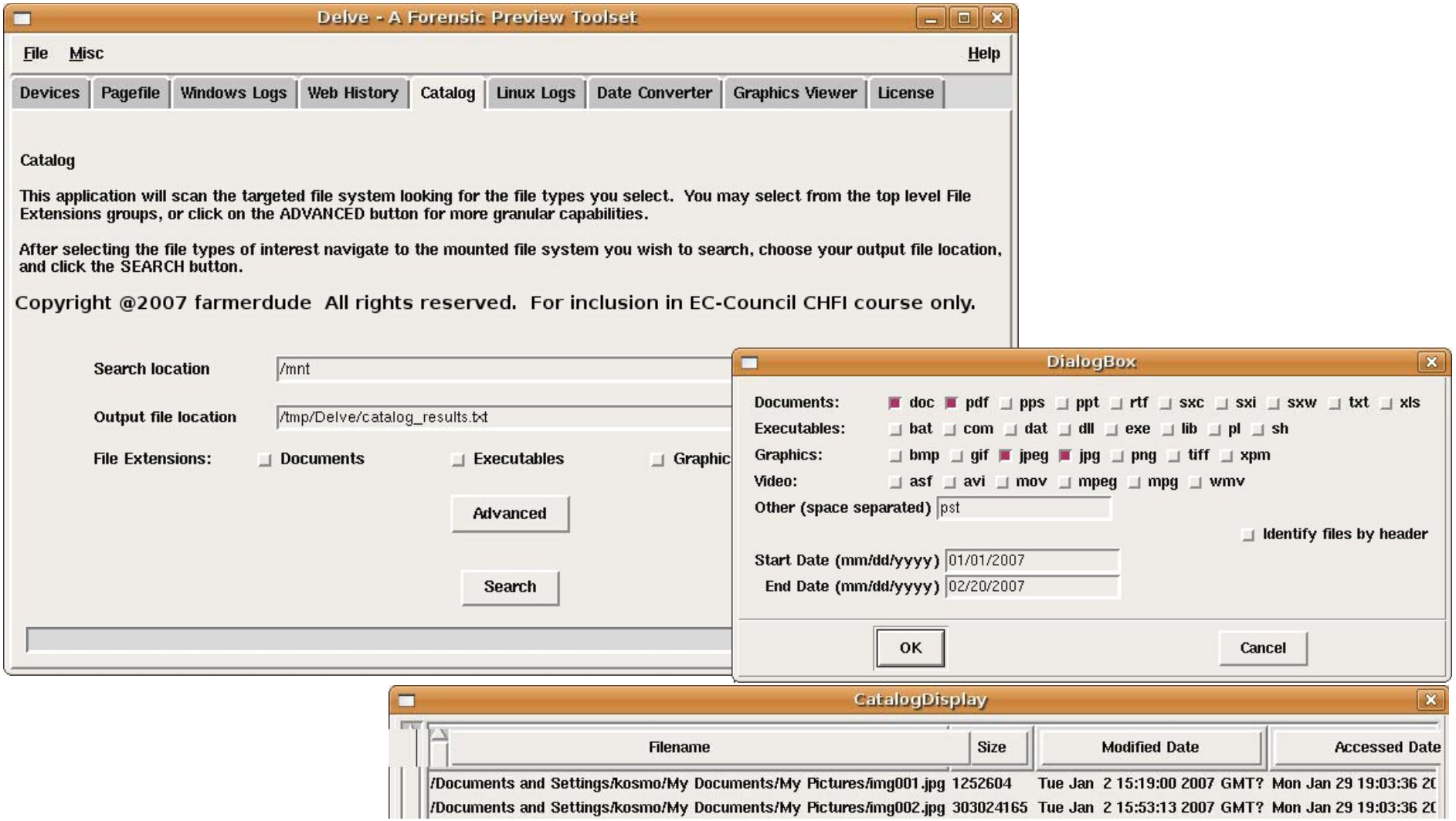
Screenshots



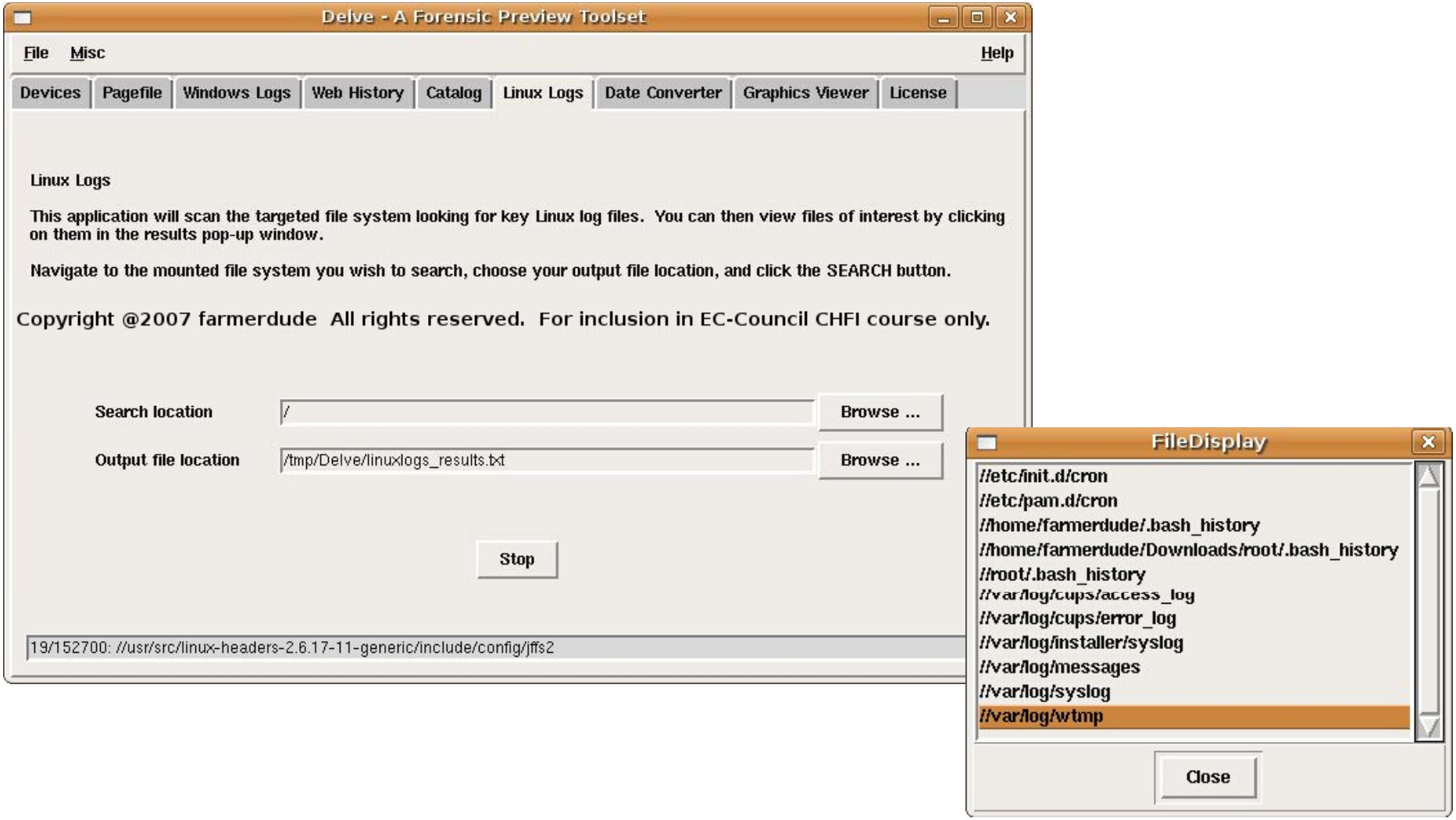
Screenshots



Screenshots

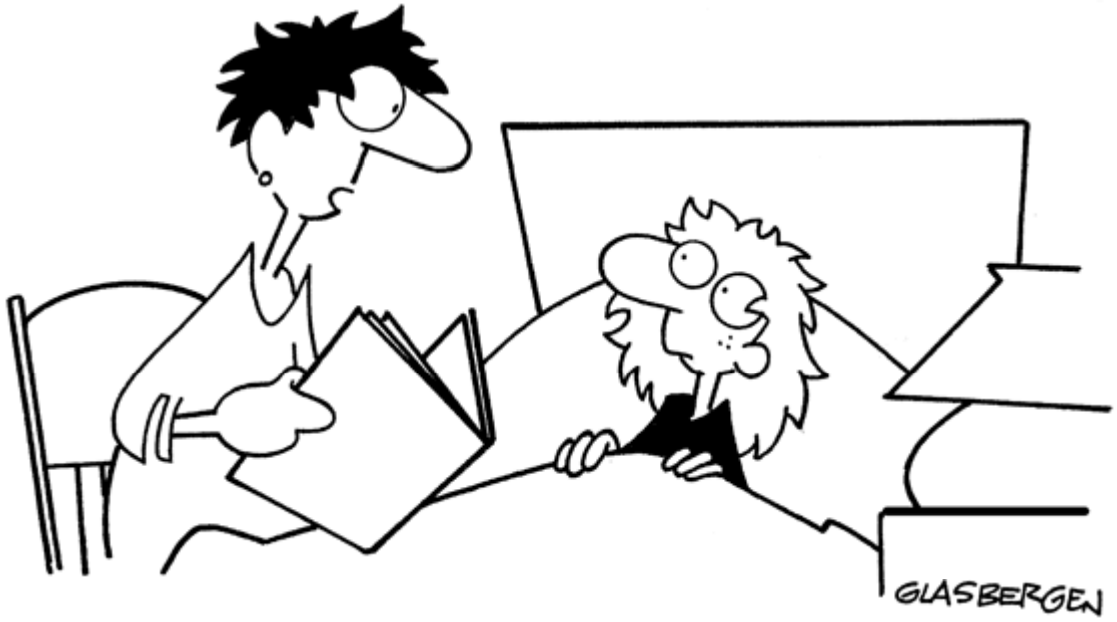


Screenshots

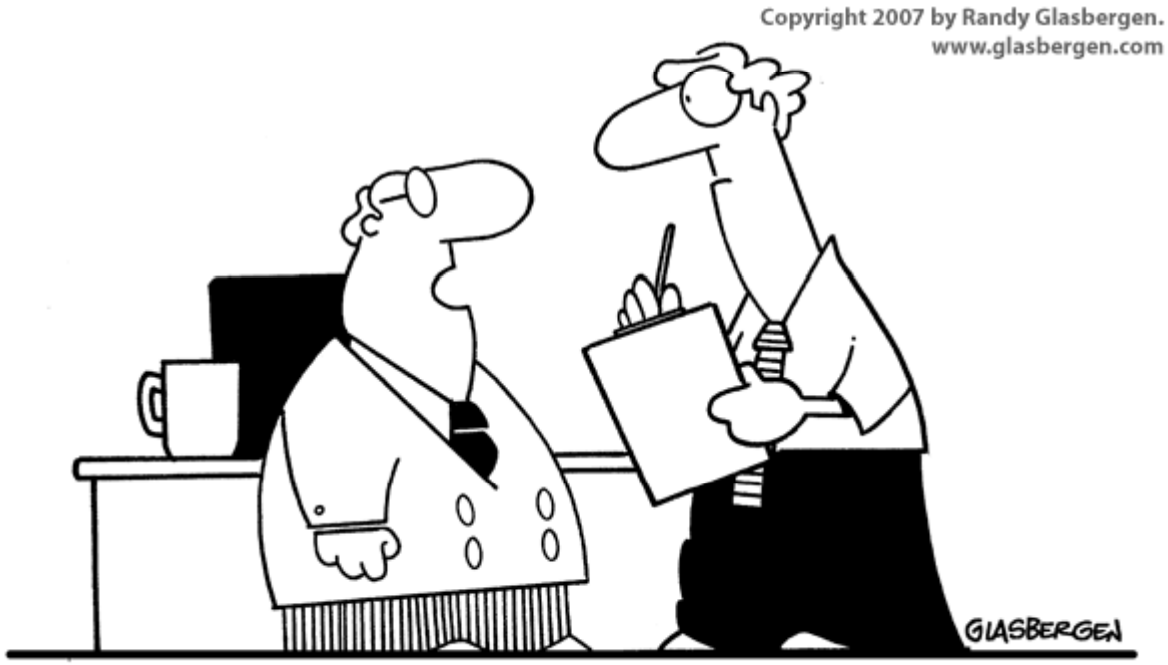


Summary

- Linux imparts greater control, flexibility, and power as a forensics tool.
- Linux has a number of simple utilities that make imaging and basic analysis of suspect disks and drives easier.
- Linux cannot identify the last sector on hard drives with odd number of sectors.
- There are several popular Linux tool kits that provide GUI as well for convenience.



"Cinderella got married and lived happily ever after until she got back from her honeymoon and stepped on the scales."



**"How can anyone say we're not a green company?
We've been dumping green stuff in the river for years!"**