Parul® University

# Cyber Security and Forensics - I
# 05201296

**Prof. Dipak L. Agrawal,** Assistant Professor
Faculty of IT & Computer Science

Parul®
University

DIGITAL LEARNING CONTENT

# CHAPTER-6

# Challenges in Cyber Forensics


# Topics

- Technical challenges - understanding the raw data and its structure
- Legal challenges in computer forensics and data privacy issues, Special tools and techniques - digital forensics tools, Special technique - data mining used in cyber forensics,
- Forensics auditing, Anti forensics.

# Technical Challenges

- With the vast development of the computer technologies within the last decade, usage of technology has been defined as both good and bad.
- One of the main problems is that as soon as a technology is developed to identify and investigate criminals, there is another technique that helps the criminals to hide themselves. This is a massive challenge forensics officers face today.


# Technical Challenges

- Encryption
- Steganography
- Data hiding in storage space
- Residual Data Wiping(अवशिष्ट)
- Tail Obfuscation (Obfuscation means to make something difficult to understand.)
- Attacking the tools
- Attacking the investigators
- Encryption

Parul®
University

DIGITAL LEARNING CONTENT

# Computer Forensics Tools

- Computer Forensics Tools
- 5.1.  Evaluating Computer Forensics Software Needs
- 5.2. Computer Forensics Software
- 5.3. Computer Hardware Tools
- 5.4. Validating and Testing Forensic Software

# 5.1 Evaluating Computer Forensics Software Needs

- Look for flexibility, and robustness
- OS
- File system
- Script capabilities
- Automated features
- Vendor's reputation
- Keep in mind what application files you will be analyzing


# Types of Computer Forensics Tools

- Hardware forensic tools
- Range from single-purpose components to complete computer systems and servers
- Software forensic tools
- Types
- Command-line applications
- GUI applications
- Commonly used to copy data from a suspect's disk drive to an image file


# Tasks Performed by Computer Forensics Tools

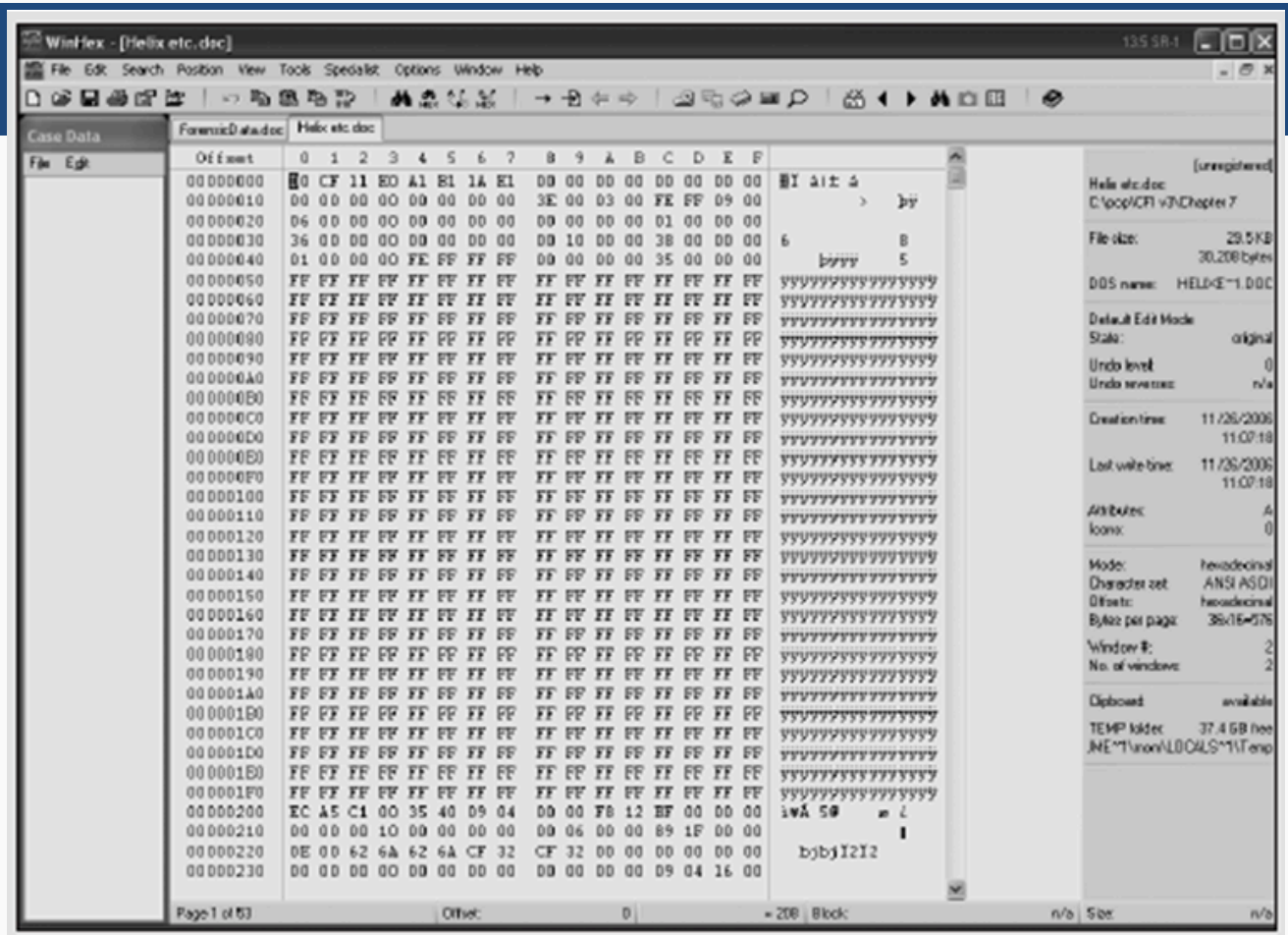
- Five major categories:
- Acquisition
- Validation
- Extraction
- Reconstruction
- Reporting


# Tasks Performed by Computer Forensics Tools (Cont.)

- Acquisition
- Making a copy of the original drive
- Acquisition sub functions:
- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification

# Tasks Performed by Computer Forensics Tools (Cont.)

- Acquisition
- Two types of data-copying methods are used in software acquisitions:
- Physical copying of the entire drive
- Logical copying of a disk partition
- The formats for disk acquisitions vary
- From raw data to vendor-specific proprietary compressed data
- You can view the contents of a raw image file with any hexadecimal editor



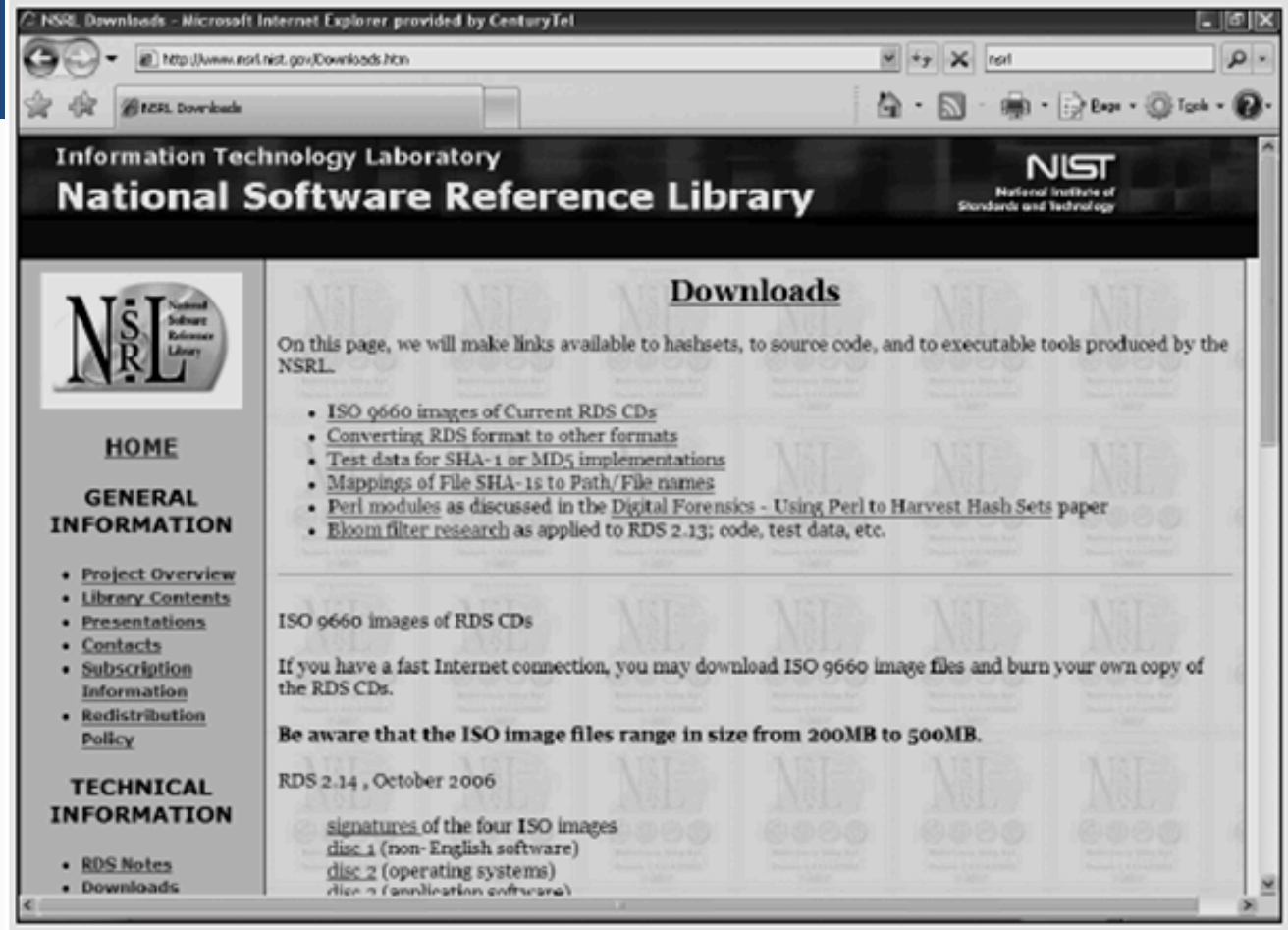

A sample hexadecimal editor

# Tasks Performed by Computer Forensics Tools (Cont.)

- Acquisition
- Creating smaller segmented files is a typical feature in vendor acquisition tools
- All computer forensics acquisition tools have a method for verification of the data-copying process
- That compares the original drive with the image
- Validation
- Ensuring the integrity of data being copied
- Involves sorting and searching through all investigation data


# Tasks Performed by Computer Forensics Tools (Cont.)

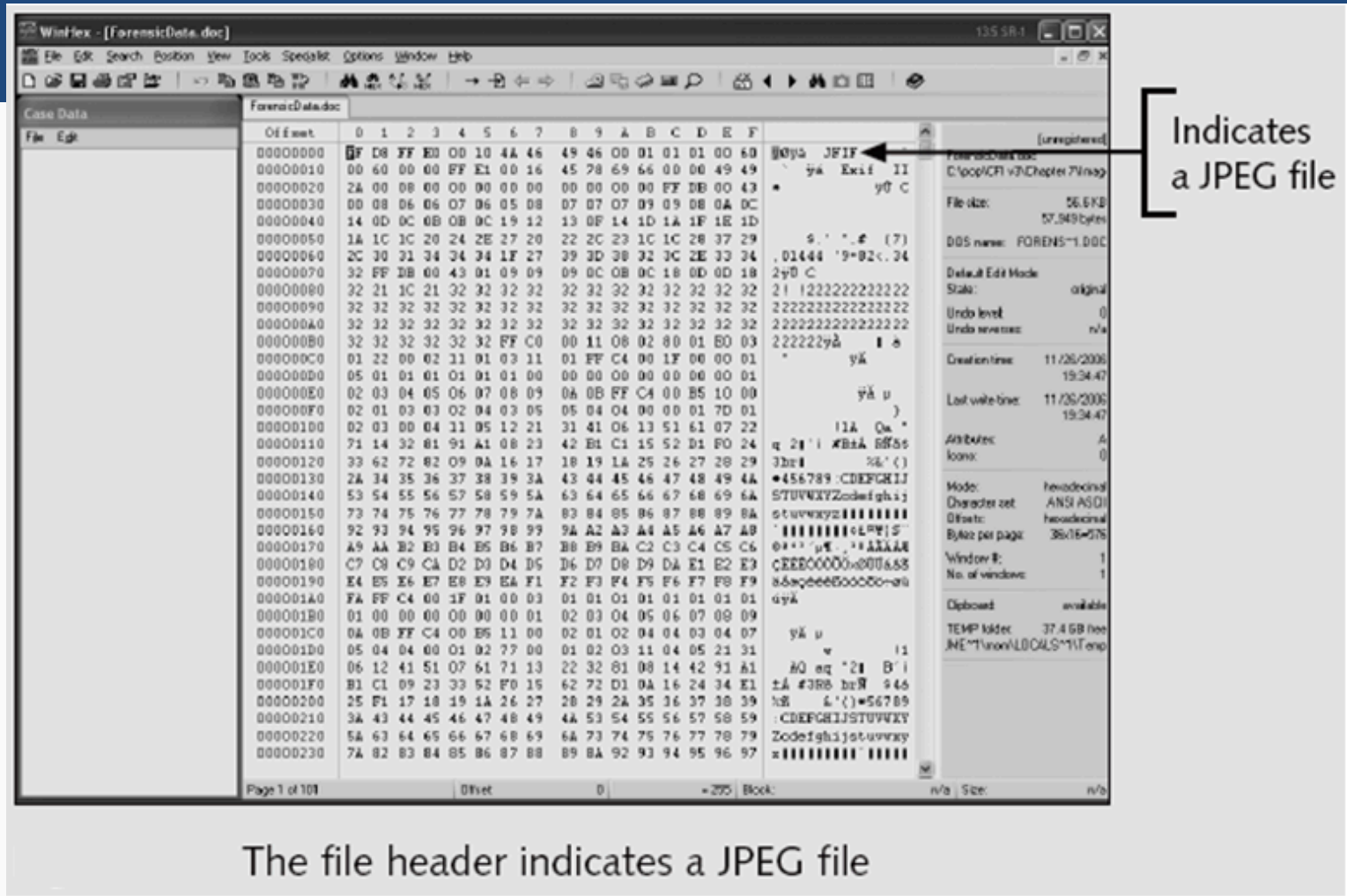
- Validation and discrimination
- Subfunctions
- Hashing
- CRC-32, MD5, Secure Hash Algorithms
- Filtering
- Based on hash value sets
- Analyzing file headers
- Discriminate files based on their types
- National Software Reference Library (NSRL) has compiled a list of known file hashes
- For a variety of OSs, applications, and images




The download page of the National Software Reference Library

# Tasks Performed by Computer Forensics Tools (Cont.)

- Validation and discrimination
- Many computer forensics programs include a list of common header values
- With this information, you can see whether a file extension is incorrect for the file type
- Most forensics tools can identify header values




The file header indicates a JPEG file


Error message displayed when trying to open a JPEG file in Word

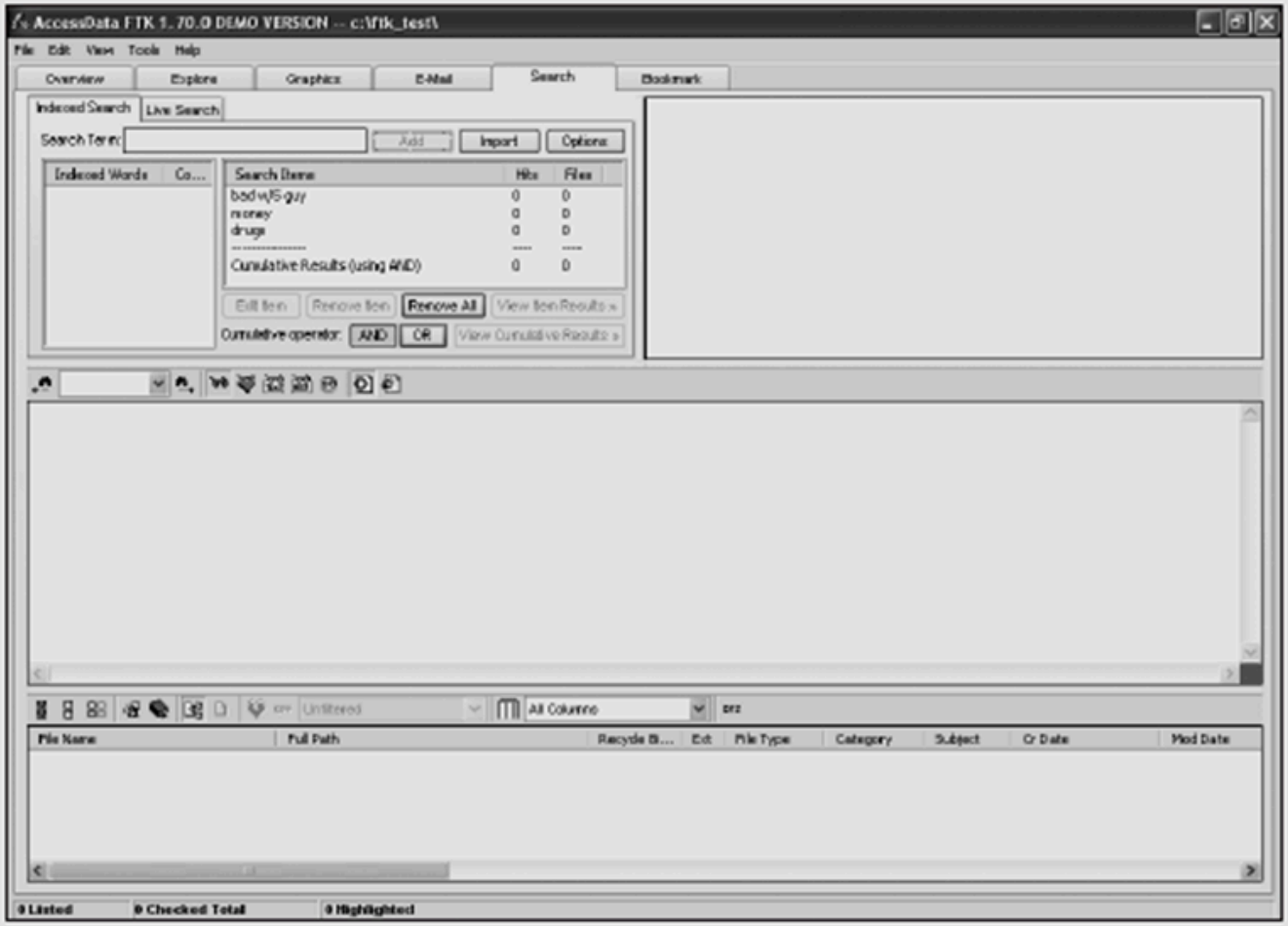

ForensicData.doc open in an image viewer

# Tasks Performed by Computer Forensics Tools (Cont.)

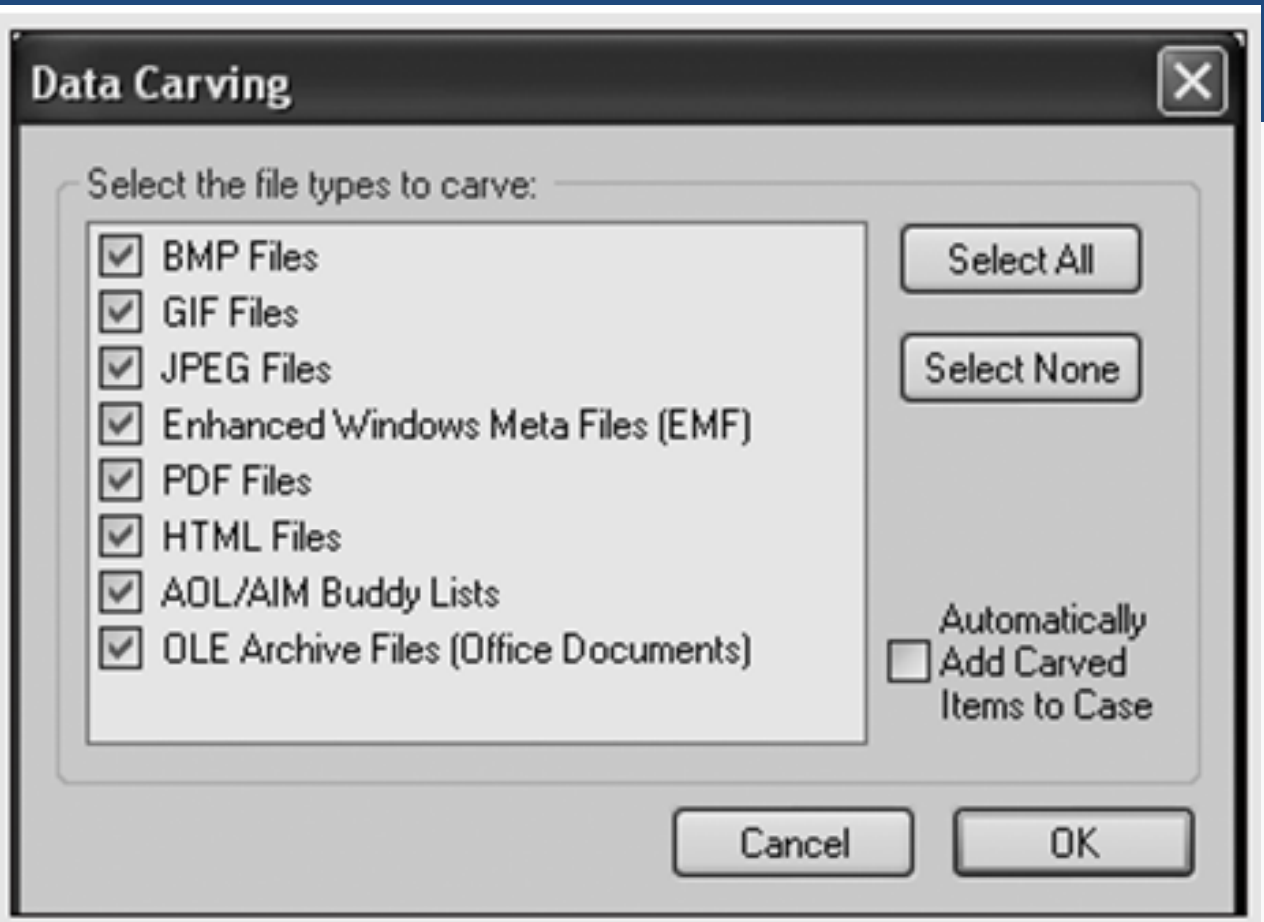
- Extraction
- Recovery task in a computing investigation
- Most demanding of all tasks to master
- Recovering data is the first step in analyzing an investigation's data
- Subfunctions
- Data viewing
- Keyword searching
- Decompressing
- Carving
- Decrypting
- Bookmarking
- Keyword search speeds up analysis for investigators

Parul®
University

DIGITAL LEARNING CONTENT




The Indexed Search feature in FTK




Data carving options in FTK


# 5.1.2 Tasks Performed by Computer Forensics Tools (Cont.)

- Extraction
- From an investigation perspective, encrypted files and systems are a problem
- Many password recovery tools have a feature for generating potential password lists
- For a password dictionary attack
- If a password dictionary attack fails, you can run a brute-force attack


# 5.1.2 Tasks Performed by Computer Forensics Tools (Cont.)

- Reconstruction
- Re-create a suspect drive to show what happened during a crime or an incident
- Subfunctions
- Disk-to-disk copy
- Image-to-disk copy
- Partition-to-partition copy
- Image-to-partition copy

Some tools that perform an image-to-disk copy:

- SafeBack
- SnapBack
- EnCase, FTK Imager, ProDiscover

# 5.1.2 Tasks Performed by Computer Forensics Tools (Cont.)

- Reporting
- To complete a forensics disk analysis and examination, you need to create a report
- Subfunctions
- Log reports
- Report generator
- Use this information when producing a final report for your investigation

# 5.1.3 Tool Comparisons

Comparison of forensics tool functions

| Function | ProDiscover Basic | AccessData Ultimate Toolkit | Guidance Software EnCase |
|---|---|---|---|
| **Acquisition** | | | |
| Physical data copy | √ | √ | √ |
| Logical data copy | √ | √ | √ |
| Data acquisition formats | √ | √ | √ |
| Command-line process | | | √ |
| GUI process | √ | √ | √ |
| Remote acquisition | | | √* |
| Verification | √ | √ | √ |
| **Validation and discrimination** | | | |
| Hashing | √ | √** | √** |
| Filtering | | √ | √ |
| Analyzing file headers | | √ | √ |
| **Extraction** | | | |
| Data viewing | √ | √*** | √*** |
| Keyword searching | √ | √ | √ |
| Decompressing | | √ | √ |
| Carving | | √ | √ |
| Decrypting | | √ | |
| Bookmarking | √ | √ | √ |
| **Reconstruction** | | | |
| Disk-to-disk copy | √ | √ | √ |
| Image-to-disk copy | √ | √ | √ |
| Partition-to-partition copy | √ | | √ |
| Image-to-partition copy | √ | | √ |
| **Reporting** | | | |
| Log reports | | √ | √ |
| Report generator | √ | √ | |


# 5.1.4 Other Considerations for Tools

- Considerations
- Flexibility
- Reliability
- Expandability
- Keep a library with older version of your tools
- Create a software library containing older versions of forensics utilities, OSs, and other programs


# 5.2 Computer Forensics Software

- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

5.2.1 Command-line Forensic Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
- One of the first MS-DOS tools used for computer investigations
- Advantage
- Command-line tools require few system resources
- Designed to run in minimal configurations


# 5.2 Computer Forensics Software

5.2.2 UNIX/Linux Command-line Forensic Tools

- *nix platforms have long been the primary command-line OSs

SMART

- Designed to be installed on numerous Linux versions
- Can analyze a variety of file systems with SMART
- Many plug-in utilities are included with SMART
- Another useful option in SMART is its hex viewer


# 5.2 Computer Forensics Software

## 5.2.2 UNIX/Linux Command-line Forensic Tools

Helix

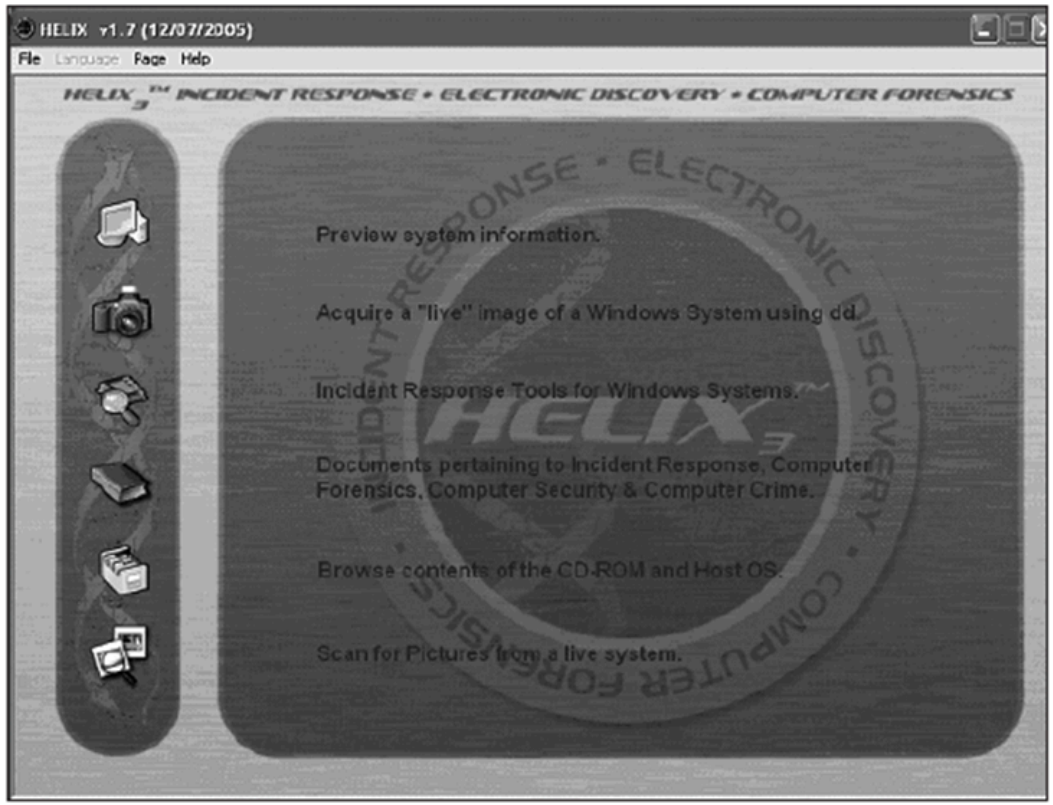
- One of the easiest suites to begin with
- You can load it on a live Windows system
- Loads as a bootable Linux OS from a cold boot

Autopsy and SleuthKit

- Sleuth Kit is a Linux forensics tool
- Autopsy is the GUI/browser interface used to access Sleuth Kit's tools

# 5.2 Computer Forensics Software

## 5.2.2 UNIX/Linux Command-line Forensic Tools




The Helix menu

## 5.2.2 UNIX/Linux Command-line Forensic Tools

Knoppix-STD

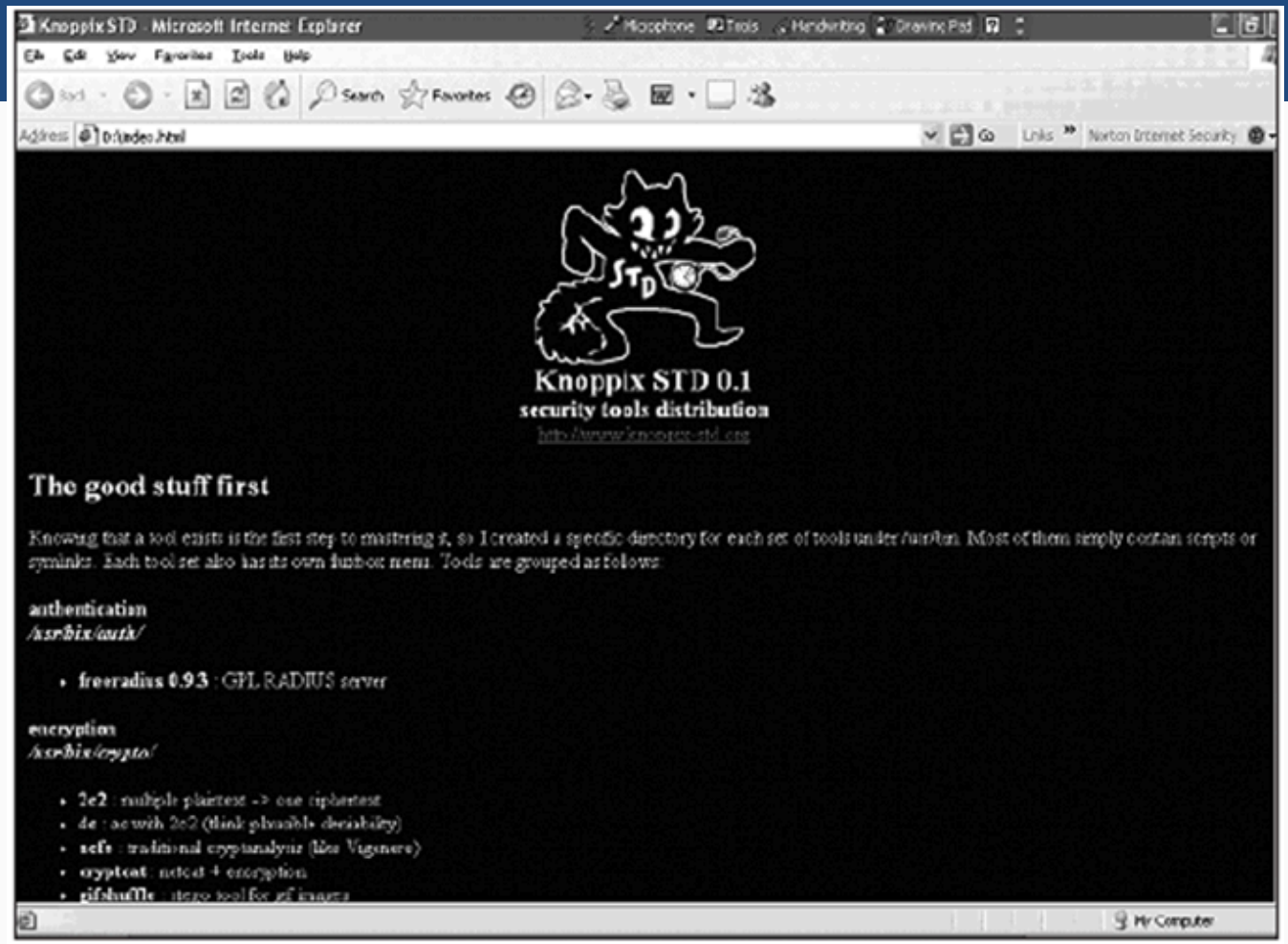
Knoppix Security Tools Distribution (STD)

A collection of tools for configuring security measures, including computer and network forensics

Knoppix-STD is forensically sound

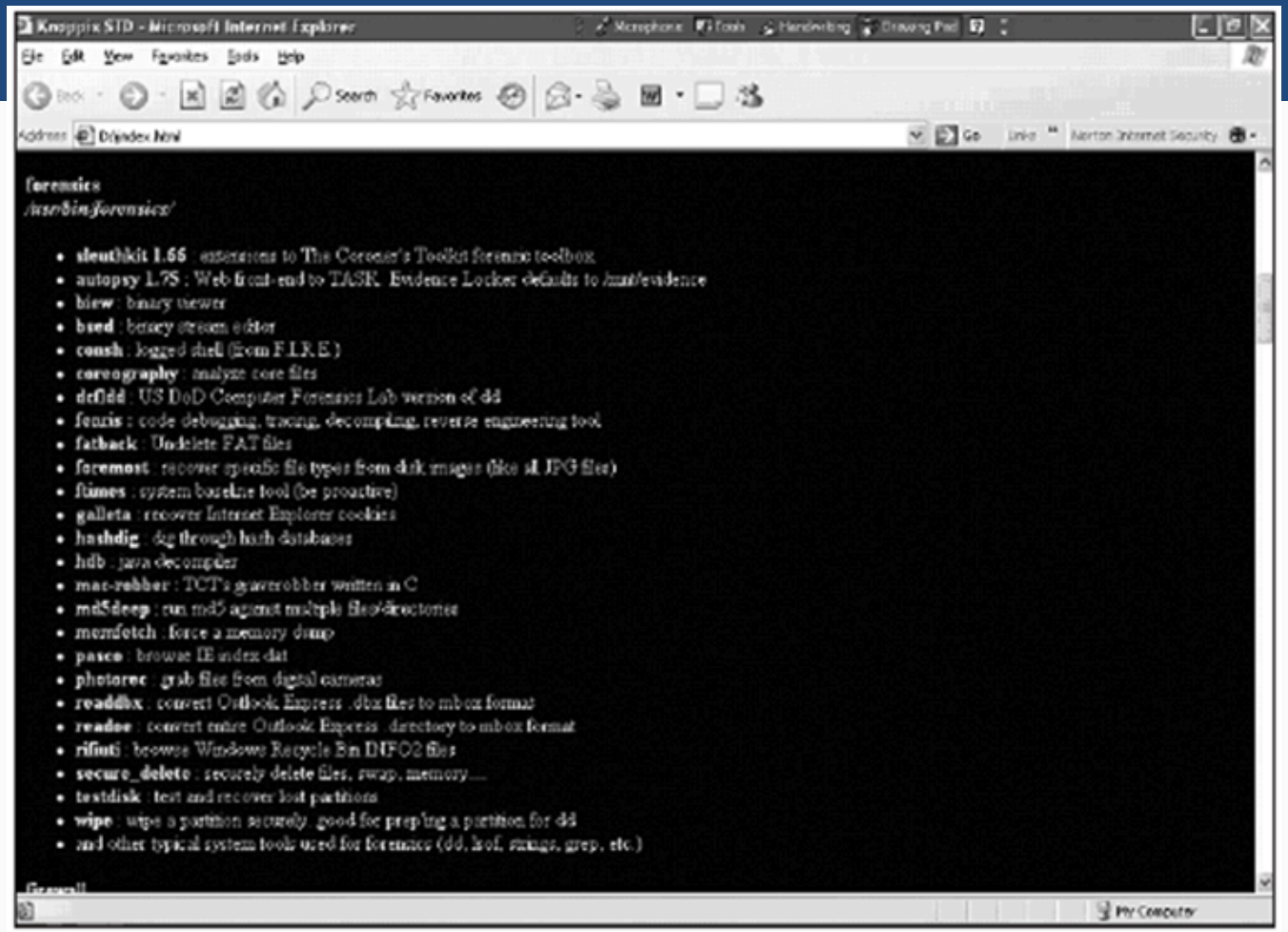
Doesn’t allow you to alter or damage the system you’re analyzing

Knoppix-STD is a Linux bootable CD




The Knoppix-STD information window in Windows

# 5.2.2 UNIX/Linux Command-line Forensic Tools (Cont.)




A list of forensics tools available in Knoppix-STD


# 5.2.3 GUI Forensic Tools

- Simplify computer forensics investigations
- Help training beginning investigators
- Most of them come into suites of tools
- Advantages
- Ease of use
- Multitasking
- No need for learning older Oss
- Disadvantages
- Excessive resource requirements
- Produce inconsistent results
- Create tool dependencies

Parul®
University

DIGITAL LEARNING CONTENT

# 5.3 Computer Hardware Tools

Technology changes rapidly

Hardware eventually fails

- Schedule equipment replacements

When planning your budget consider:

- Failures
- Consultant and vendor fees
- Anticipate equipment replacement


# 5.3 Computer Hardware Tools

5.3.1 Forensic Workstations

Carefully consider what you need

Categories

Stationary

Portable

Lightweight

Balance what you need and what your system can handle

Police agency labs

Need many options

Use several PC configurations

Private corporation labs

Handle only system types used in the organization

Keep a hardware library in addition to your software library


# 5.3 Computer Hardware Tools

5.3.1 Forensic Workstations (Cont.)

Not as difficult as it sounds

Advantages

Customized to your needs

Save money

Disadvantages

Hard to find support for problems

Can become expensive if careless

Also need to identify what you intend to analyze

# 5.3 Computer Hardware Tools

5.3.1 Forensic Workstations (Cont.)

You can buy one from a vendor as an alternative

Examples

F.R.E.D.

F.I.R.E. IDE

Having vendor support can save you time and frustration when you have problems

Can mix and match components to get the capabilities you need for your forensic workstation


# 5.3 Computer Hardware Tools

5.3.2 Using a Write Broker

Write-blocker

Prevents data writes to a hard disk

Software-enabled blockers

Software write-blockers are OS dependant

Example: PDBlock from Digital Intelligence

Hardware options

Ideal for GUI forensic tools

Act as a bridge between the suspect drive and the forensic workstation


# 5.3 Computer Hardware Tools

5.3.2 Using a Write Broker (Cont.)

Can navigate to the blocked drive with any application

Discards the written data

For the OS the data copy is successful

Connecting technologies

FireWire

USB 2.0

SCSI controllers

Parul®
University

DIGITAL LEARNING CONTENT

# 5.3 Computer Hardware Tools

5.3.3 Recommendations for a Forensic Workstation

Determine where data acquisitions will take place

Data acquisition techniques

USB 2.0

FireWire

Expansion devices requirements

Power supply with battery backup

Extra power and data cables


# 5.3 Computer Hardware Tools

5.3.3 Recommendations for a Forensic Workstation (Cont.)

External FireWire and USB 2.0 ports

Assortment of drive adapter bridges

Ergonomic considerations

Keyboard and mouse

A good video card with at least a 17-inch monitor

High-end video card and monitor

If you have a limited budget, one option for outfitting your lab is to use high-end game PCs


# 5.4 Validating and Testing Forensic Software

Make sure the evidence you recover and analyze can be admitted in court

Test and validate your software to prevent damaging the evidence

5.4.1 Using National Institute of Standards and Technology (NIST) Tools

Computer Forensics Tool Testing (CFTT) program

Manages research on computer forensics tools

NIST has created criteria for testing computer forensics tools based on:

Standard testing methods

ISO 17025 criteria for testing items that have no current standards

ISO 5725

# 5.4 Validating and Testing Forensic Software

5.4.1 Using National Institute of Standards and Technology (NIST) Tools (Cont.)

Your lab must meet the following criteria

Establish categories for computer forensics tools

Identify computer forensics category requirements

Develop test assertions

Identify test cases

Establish a test method

Report test results

Also evaluates drive-imaging tools using

Forensic Software Testing Support Tools (FS-TST)


# 5.4 Validating and Testing Forensic Software

5.4.1 Using National Institute of Standards and Technology (NIST) Tools (Cont.)

National Software Reference Library (NSRL) project

Collects all known hash values for commercial software applications and OS files

Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)

Helps filtering known information

Can use RDS to locate and identify known bad files


# 5.4 Validating and Testing Forensic Software

## 5.4.2 Using Validation Protocols

Always verify your results

Use at least two tools

Retrieving and examination

Verification

Understand how tools work

One way to compare results and verify a new tool is by using a disk editor

Such as Hex Workshop or WinHex


# 5.4 Validating and Testing Forensic Software

## 5.4.2 Using Validation Protocols (Cont.)

Disk editors

Do not have a flashy interface

Reliable tools

Can access raw data

Computer Forensics Examination Protocol

Perform the investigation with a GUI tool

Verify your results with a disk editor

Compare hash values obtained with both tools


# Summary

Create a business plan to get the best hardware and software

Computer forensics tools functions

Acquisition

Validation and discrimination

Extraction

Reconstruction

Reporting

Maintain a software library on your lab

Computer Forensics tools types

Software

Hardware


# Summary (Cont.)

Forensics software

Command-line

GUI

Forensics hardware

Customized equipment

Commercial options

Include workstations and write-blockers

Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools

Always test your forensics tools

# What Is a Forensic Audit?

- While a forensic audit may sound like something exciting you hear about on crime dramas like Law and Order or CSI, the truth is a little more mundane. A forensic audit is the process of reviewing a person's or companies financial statements to determine if they are accurate and lawful. Forensic accounting is most commonly associated with the IRS and tax audits, but it may also be commissioned by private companies to establish a complete view of a single entity's finances.

# When Are Forensic Audits Used?

- Forensic audits are used wherever an entity's finances present a legal concern. For instance, it is used in cases of suspected embezzlement or fraud, to determine tax liability, to investigate a spouse during divorce proceedings or to investigate allegations of bribery, among other reasons.
- Forensic audits are performed by a class of professionals with skillsets in both criminology and accounting who specialize in following a money trail, keeping track of fraudulent and actual balance sheets and checking for inaccuracies in overall and detailed reports of income or expenditures.


# When Are Forensic Audits Used?

- Anti-forensics has only recently been recognized as a legitimate field of study. Within this field of study, numerous definitions of anti-forensics abound. One of the more widely known and accepted definitions comes from Dr.Marc Rogers of Purdue University. Dr. Rogers uses a more traditional “crime scene” approach when defining anti-forensics. “Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.”
- A more abbreviated definition is given by Scott Berinato in his article entitled, The Rise of Anti-Forensics. “Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you.

# When Are Forensic Audits Used?

- Sub-categories
- Anti-forensics methods are often broken down into several sub-categories to make classification of the various tools and techniques simpler.
- Purpose and goals
- Within the field of digital forensics there is much debate over the purpose and goals of anti-forensic methods. The common conception [who?] is that anti-forensic tools are purely malicious in intent and design.
- Data hiding: It is the process of making data difficult to find while also keeping it accessible for future use. “Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves.”


# When Are Forensic Audits Used?

- Encryption
- One of the more commonly used techniques to defeat computer forensics is data encryption. In a presentation he gave on encryption and anti-forensic methodologies the Vice President of Secure Computing, Paul Henry, referred to encryption as a “forensic expert's nightmare”.
- The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key. Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.

# Steganography

- Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. “Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph).”
- **Other forms of data hiding**
- Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places can include “memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions.”
- One of the more well-known tools that is often used for data hiding is called Slacker (part of the Metasploit framework). Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software.

# DIGITAL LEARNING CONTENT


Parul® University

www.paruluniversity.ac.in