



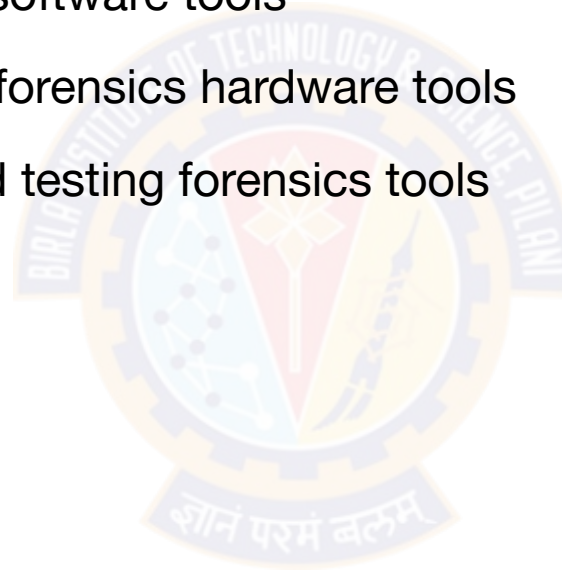
**BITS Pilani**  
Pilani | Dubai | Goa | Hyderabad

# Guide to Computer Forensics and Investigations Sixth Edition

## *Chapter 6* *Current Digital Forensics Tools*

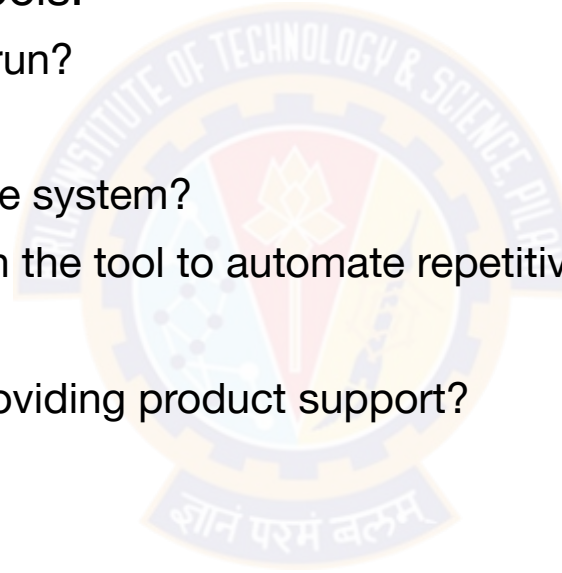
# Objectives

- Explain how to evaluate needs for digital forensics tools
- Describe available digital forensics software tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics tools



# Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible
- Questions to ask when evaluating tools:
  - On which OS does the forensics tool run?
  - Is the tool versatile?
  - Can the tool analyze more than one file system?
  - Can a scripting language be used with the tool to automate repetitive functions and tasks?
  - Does it have automated features?
  - What is the vendor's reputation for providing product support?



# Types of Digital Forensics Tools

- Hardware forensic tools
  - Range from simple, 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 Digital Forensics Tools (1 of 20)

- Follow guidelines set up by NIST's **Computer Forensics Tool Testing (CFTT)** program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRRs) should use validated tools
- Five major categories:
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting



# Tasks Performed by Digital Forensics Tools (2 of 20)

- **Acquisition**

- Making a copy of the original drive

- Acquisition subfunctions:

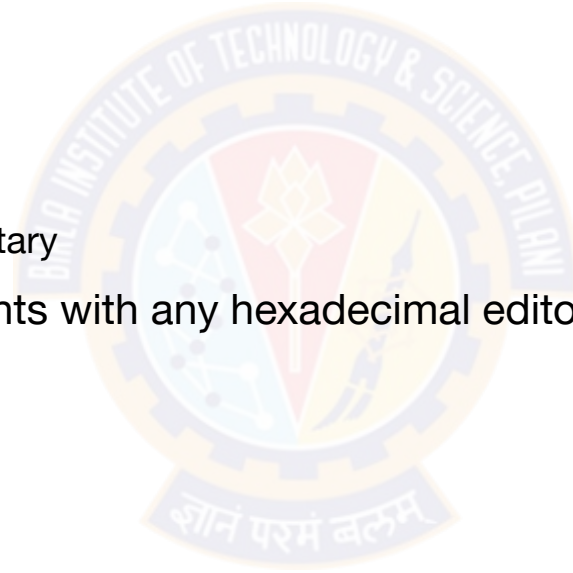
- Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote, live, and memory acquisitions



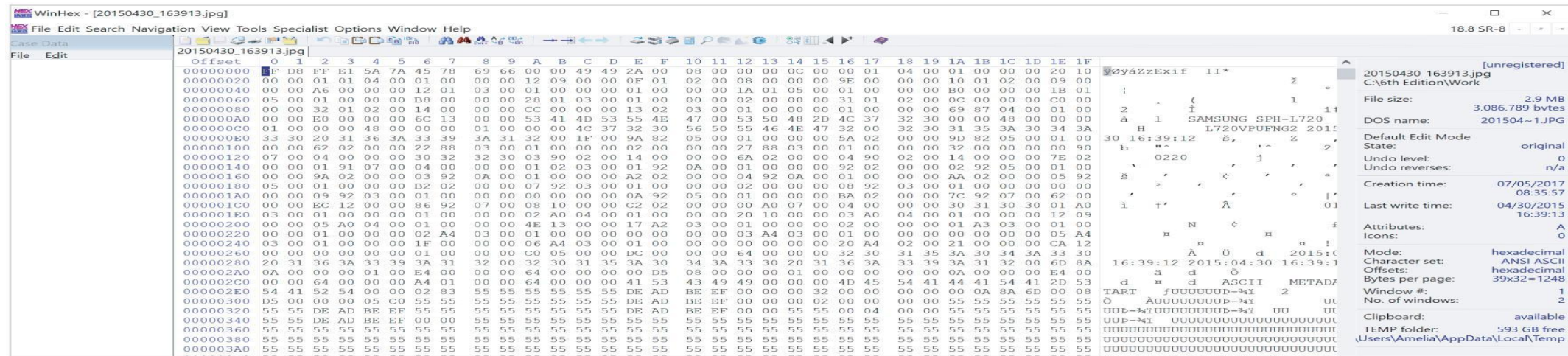


# Tasks Performed by Digital Forensics Tools (3 of 20)

- Acquisition (cont'd)
  - 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
  - You can view a raw image file's contents with any hexadecimal editor



# Tasks Performed by Digital Forensics Tools (4 of 20)



**Figure 6-1** Viewing data in WinHex

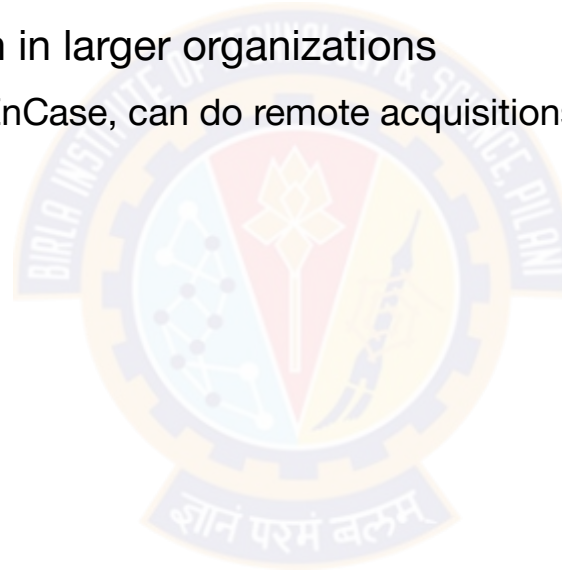
Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)





# Tasks Performed by Digital Forensics Tools (5 of 20)

- Acquisition (cont'd)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
    - Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensics drive images on a network



# Tasks Performed by Digital Forensics Tools (6 of 20)

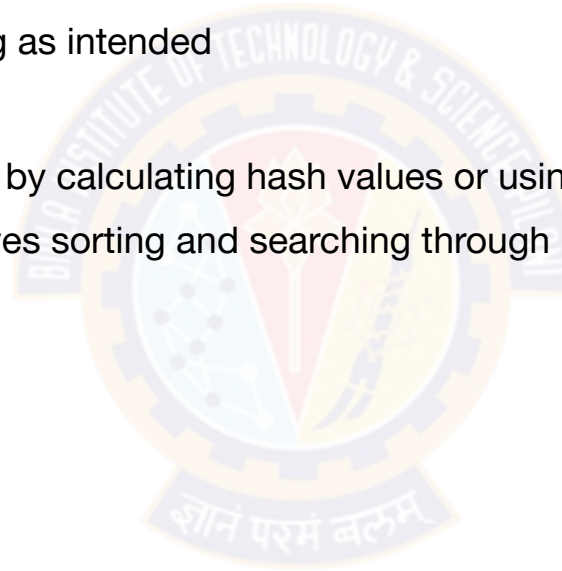
- Validation and Verification

- **Validation**

- A way to confirm that a tool is functioning as intended

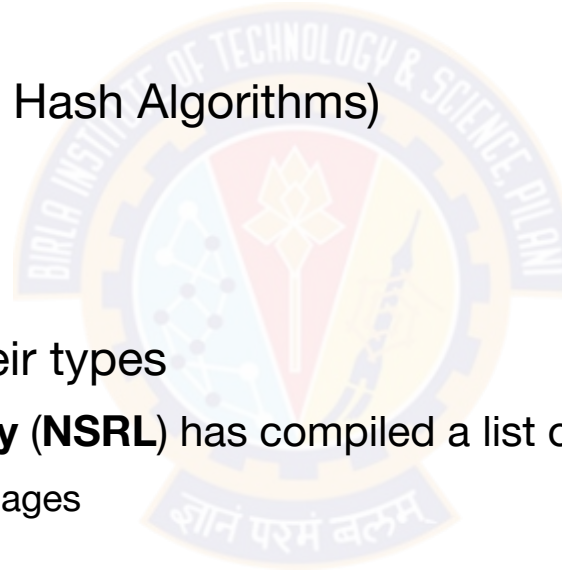
- **Verification**

- Proves that two sets of data are identical by calculating hash values or using another similar method
    - A related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data



# Tasks Performed by Digital Forensics Tools (7 of 20)

- Validation and verification (cont'd)
  - Subfunctions
    - Hashing
      - CRC-32, MD5, SHA-1 (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



# Tasks Performed by Digital Forensics Tools (8 of 20)

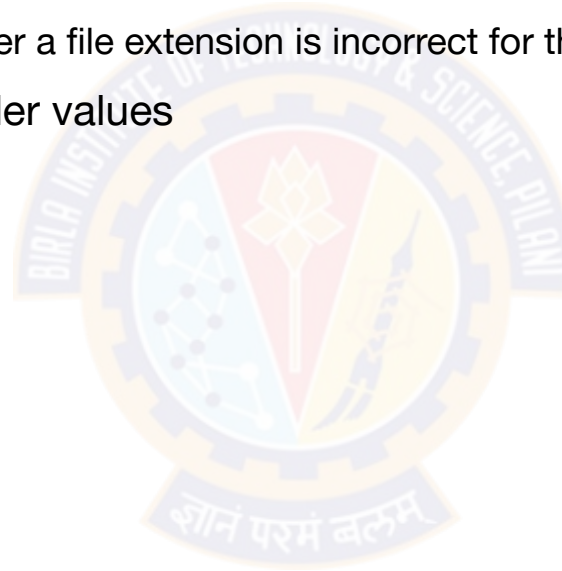


**Figure 6-2** The home page of the National Software Reference Library

Source: [www.nsrl.nist.gov](http://www.nsrl.nist.gov)

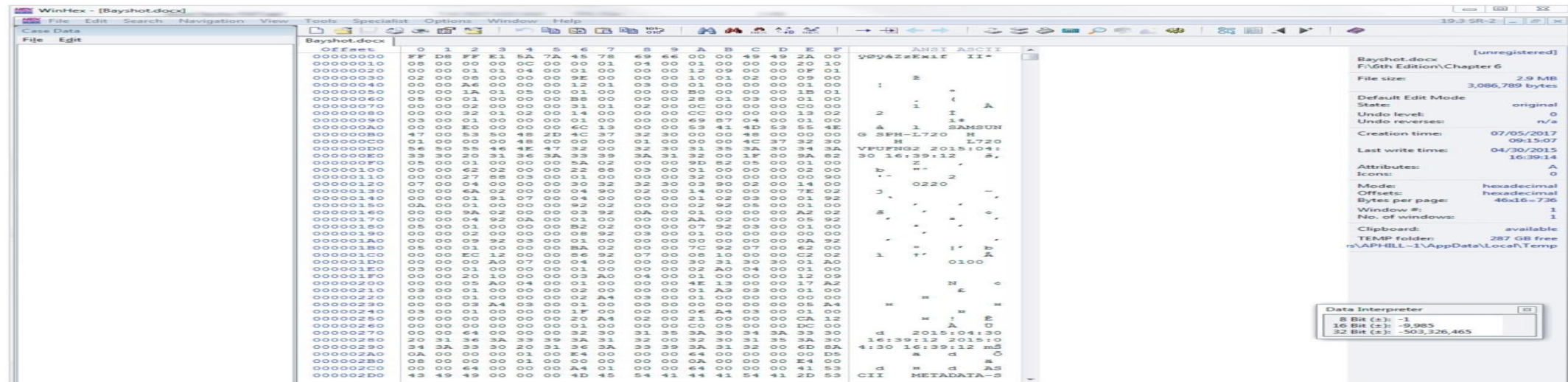
# Tasks Performed by Digital Forensics Tools (9 of 20)

- Validation and discrimination (cont'd)
  - 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





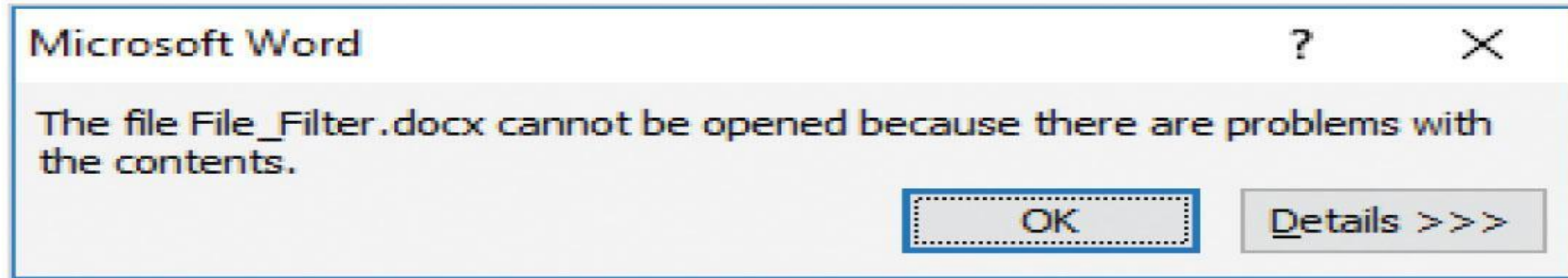
# Tasks Performed by Digital Forensics Tools (10 of 20)



**Figure 6-3** The file header indicates a .jpeg file

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

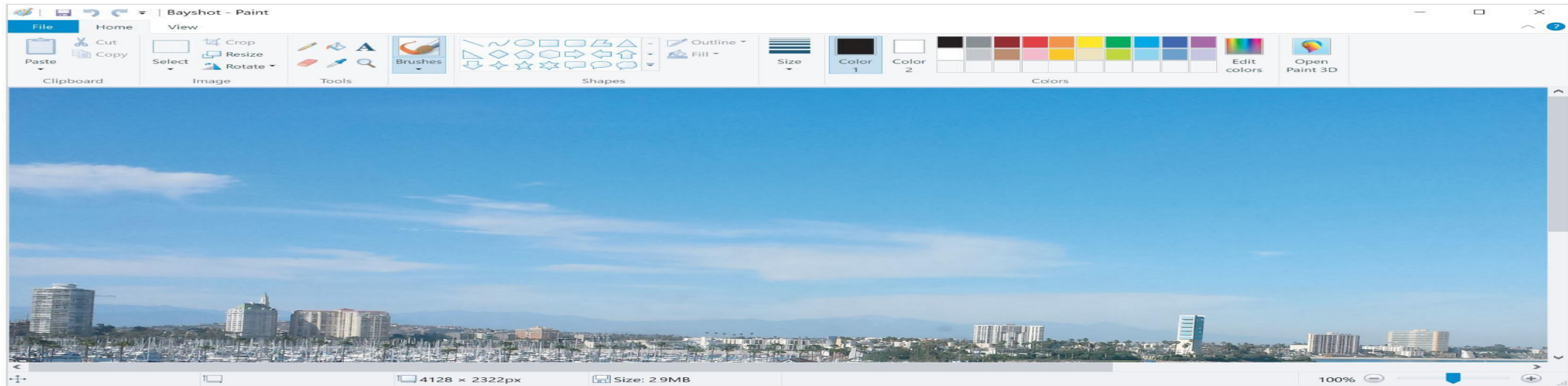
# Tasks Performed by Digital Forensics Tools (11 of 20)



**Figure 6-4** Error message displayed when trying to open a .jpeg file in Word



# Tasks Performed by Digital Forensics Tools (12 of 20)



**Figure 6-5** Bayshot .docx opened in Paint



# Tasks Performed by Digital Forensics Tools (13 of 20)

- **Extraction**

- Recovery task in a digital investigation
- Most challenging of all tasks to master
- Recovering data is the first step in analyzing an investigation's data



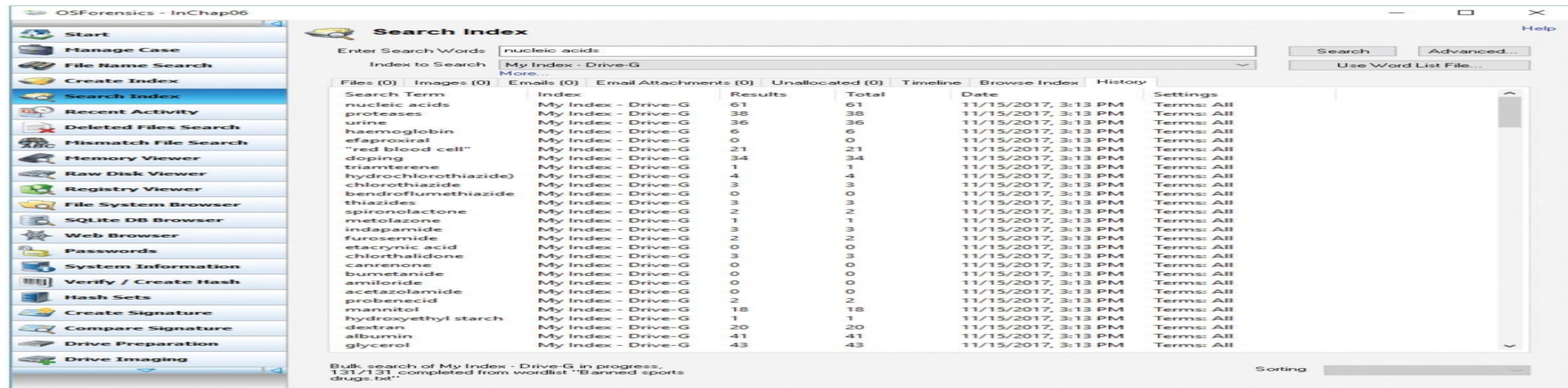
# Tasks Performed by Digital Forensics Tools (14 of 20)

- Extraction (cont'd)
  - Subfunctions of extraction
    - Data viewing
    - Keyword searching
    - Decompressing or uncompressing
    - Carving
    - Decrypting
    - Bookmarking or tagging
  - **Keyword search** speeds up analysis for investigators





# Tasks Performed by Digital Forensics Tools (15 of 20)

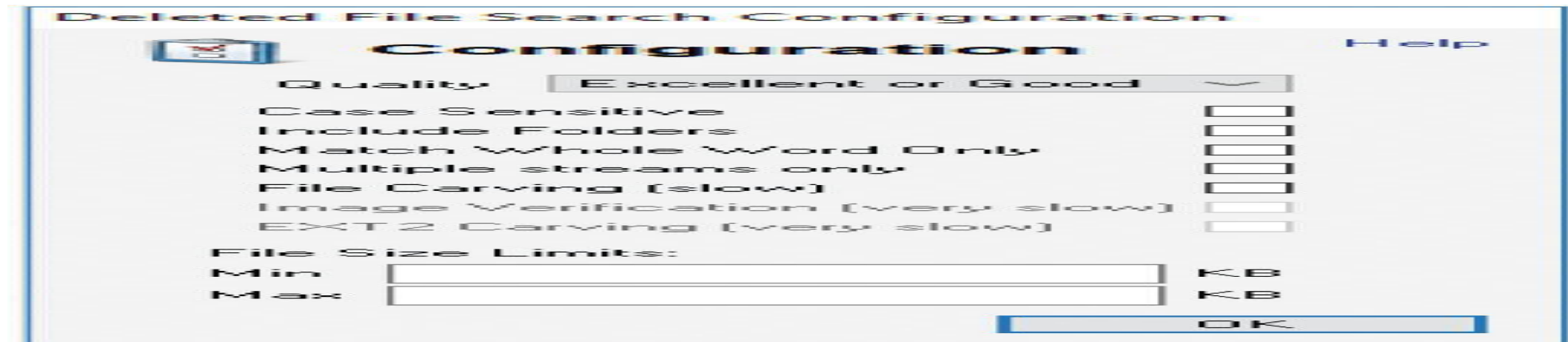


**Figure 6-6** Using a word list to search in OSForensics

Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)



# Tasks Performed by Digital Forensics Tools (16 of 20)



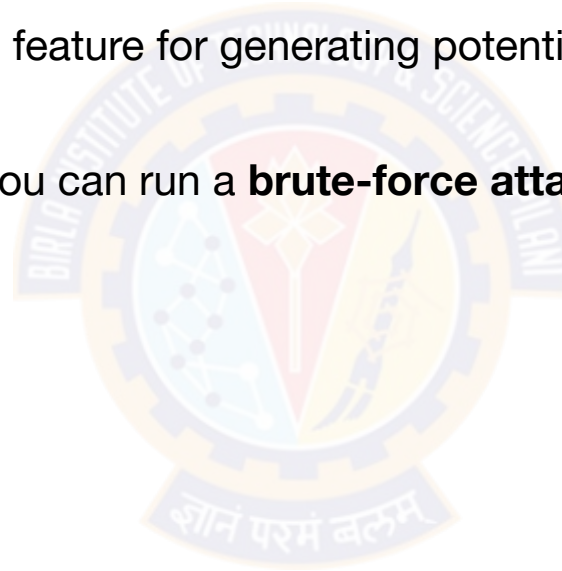
**Figure 6-7 Data-carving options in OS Forensics**

Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)



# Tasks Performed by Digital Forensics Tools (17 of 20)

- Extraction (cont'd)
  - 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**



# Tasks Performed by Digital Forensics Tools (18 of 20)

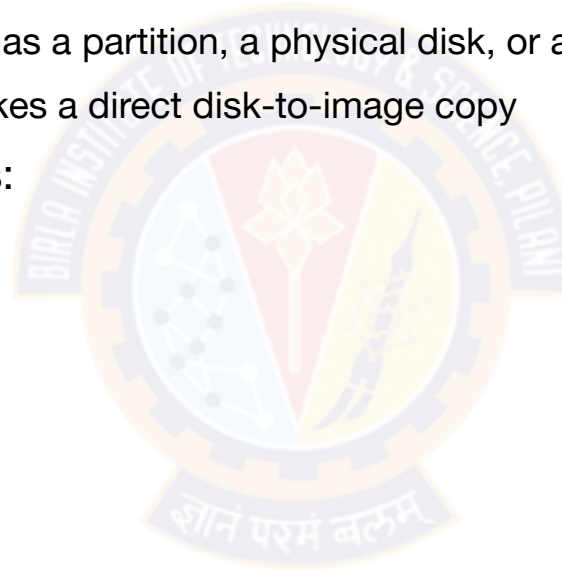
- **Reconstruction**

- Re-create a suspect drive to show what happened during a crime or an incident
- Methods of reconstruction
  - Disk-to-disk copy
  - Partition-to-partition copy
  - Image-to-disk copy
  - Image-to-partition copy
  - Disk-to-image copy
  - Rebuilding files from data runs and carving



# Tasks Performed by Digital Forensics Tools (19 of 20)

- Reconstruction (cont'd)
  - To re-create an image of a suspect drive
    - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
    - Simplest method is to use a tool that makes a direct disk-to-image copy
  - Examples of disk-to-image copy tools:
    - Linux dd command
    - ProDiscover
    - Voom Technologies Shadow Drive





# Tasks Performed by Digital Forensics Tools (20 of 20)

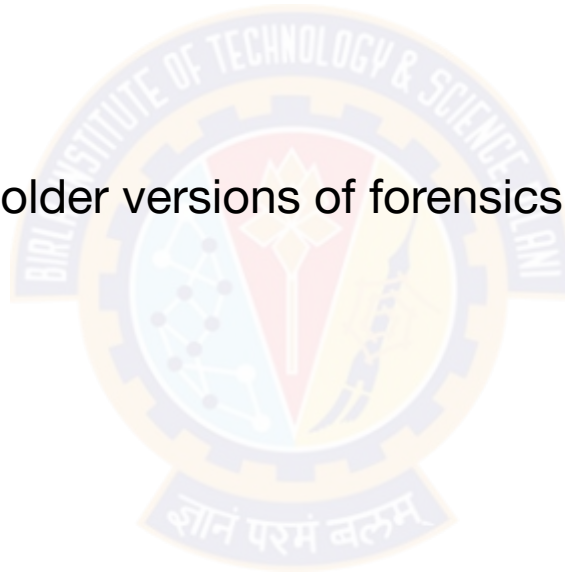
- **Reporting**

- To perform a forensics disk analysis and examination, you need to create a report
- Subfunctions of reporting
  - Bookmarking or tagging
  - Log reports
  - Timelines
  - Report generator
- Use this information when producing a final report for your investigation



# Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Future expandability
- Create a software library containing older versions of forensics utilities, OSs, and other programs



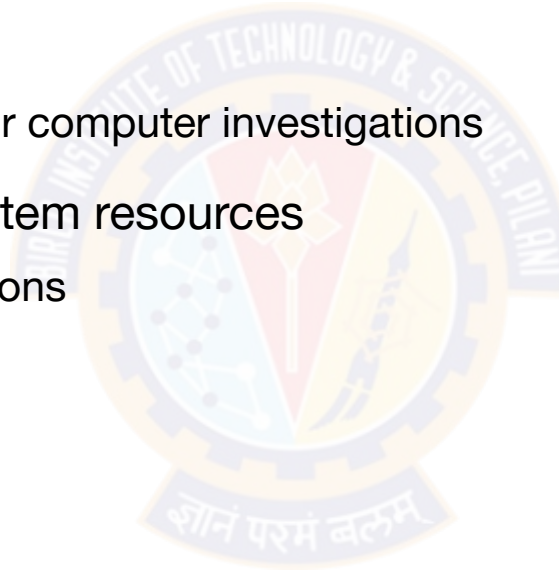
# Digital Forensics Software Tools

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



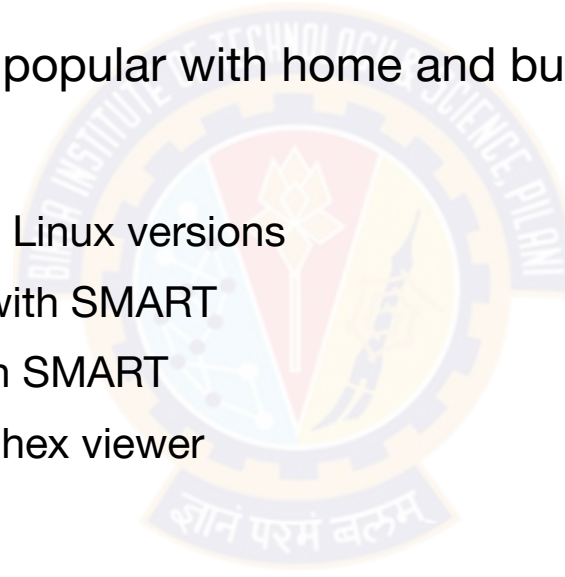
# Command-line Forensics Tools

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



# Linux Forensics Tools (1 of 3)

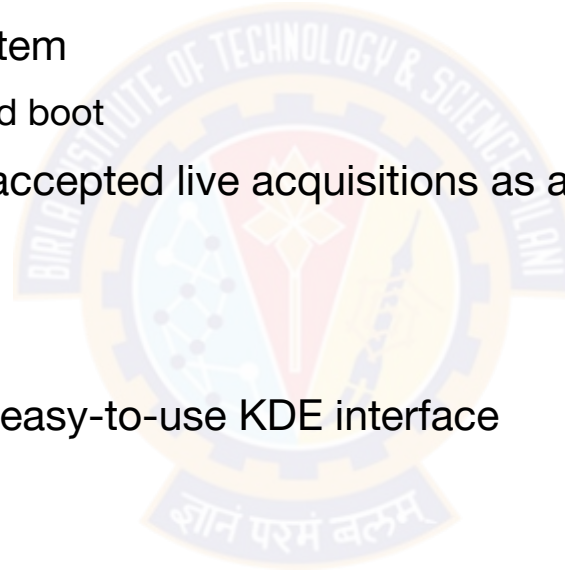
- UNIX has been mostly replaced by Linux
  - You might still encounter systems running UNIX
- Linux platforms have become more popular with home and business end users
- SMART
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer





# Linux Forensics Tools (2 of 3)

- Helix 3
  - One of the easiest suites to use
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot
  - \*\*Some international courts have not accepted live acquisitions as a valid forensics practice
- Kali Linux
  - Formerly known as BackTrack
  - Includes a variety of tools and has an easy-to-use KDE interface



# Linux Forensics Tools (3 of 3)

- Autopsy and SleuthKit
  - Sleuth Kit is a Linux forensics tool
  - Autopsy was the browser interface used to access Sleuth Kit's tools
  - Chapter 7 explains how to use these tools
- Forcepoint Threat Protection
  - Formerly known as Second Look
  - A Linux memory analysis tool
  - Could perform both onsite and remote memory acquisitions



# Other GUI Forensics Tools (1 of 2)

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs



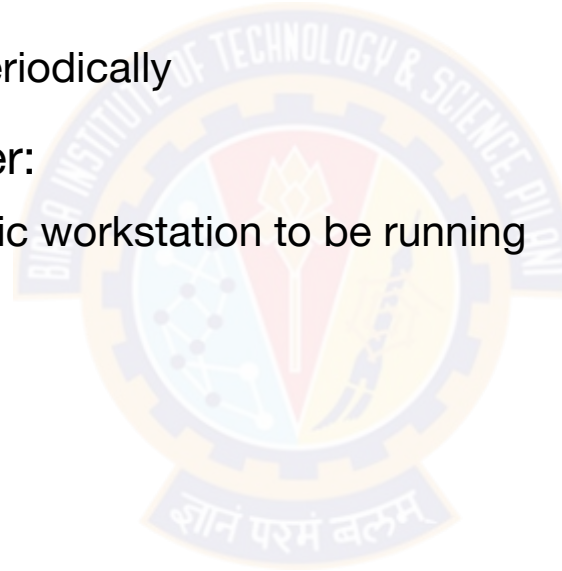
# Other GUI Forensics Tools (2 of 2)

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies
    - Investigators' may want to use only one tool
    - Should be familiar with more than one type of tool



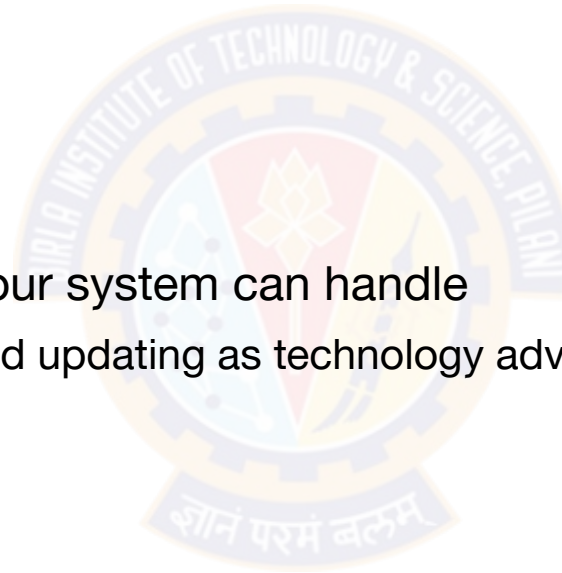
# Digital Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements periodically
- When planning your budget consider:
  - Amount of time you expect the forensic workstation to be running
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement



# Forensic Workstations (1 of 4)

- Carefully consider what you need
- Categories
  - Stationary workstation
  - Portable workstation
  - Lightweight workstation
- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances





# Forensic Workstations (2 of 4)

- Police agency labs
  - Need many options
  - Use several PC configurations
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization



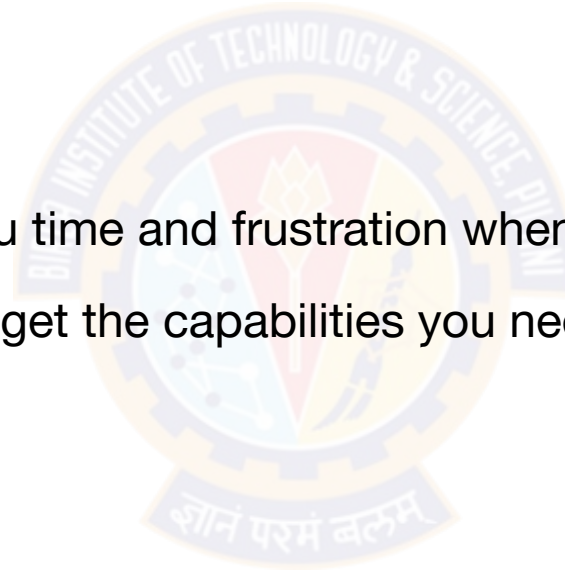
# Forensic Workstations (3 of 4)

- Building a forensic workstation is 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



# Forensic Workstations (4 of 4)

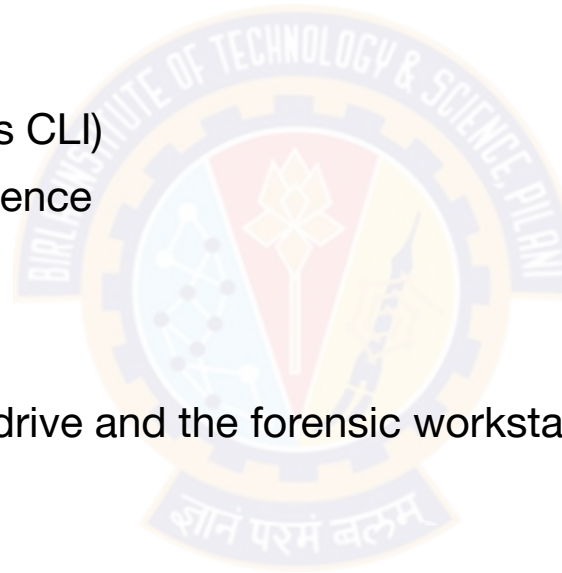
- Some vendors offer workstations designed for digital forensics
- Examples
  - F.R.E.D. unit from Digital Intelligence
  - Hardware mounts from ForensicPC
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation



# Using a Write-Blocker (1 of 2)

- **Write-blocker**

- Prevents data writes to a hard disk
- Software-enabled blockers
  - Typically run in a shell mode (Windows CLI)
  - Example: PDBlock from Digital Intelligence
- Hardware options
  - Ideal for GUI forensic tools
  - Act as a bridge between the suspect drive and the forensic workstation



# Using a Write-Blocker (2 of 2)

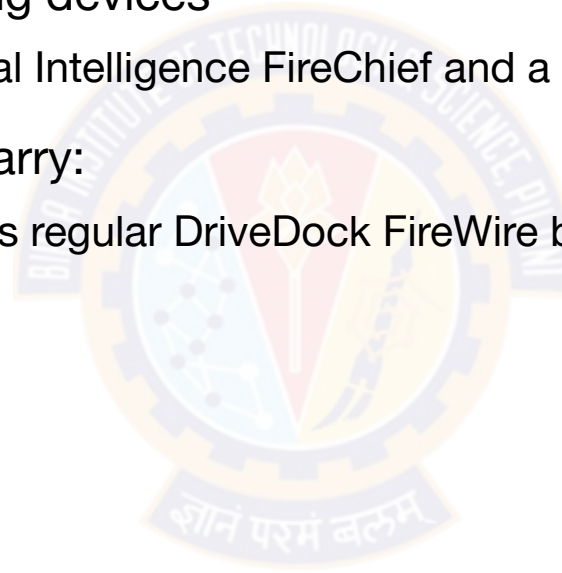
- You can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies
  - FireWire
  - USB 2.0 and 3.0
  - SATA, PATA, and SCSI controllers



# Recommendations for a Forensic Workstation

## (1 of 3)

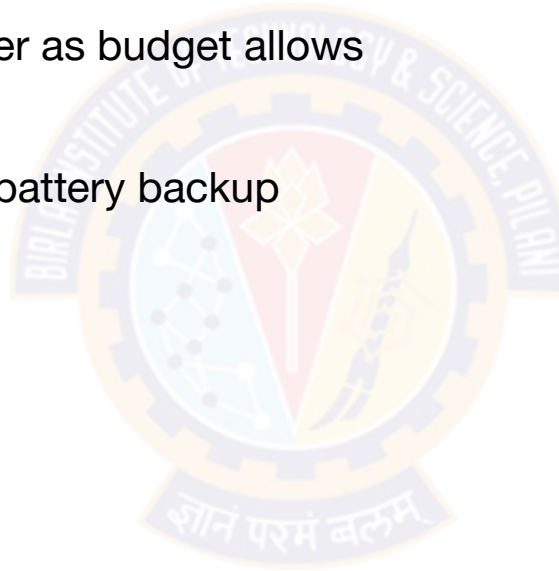
- Determine where data acquisitions will take place
- With Firewire and USB write-blocking devices
  - You can acquire data easily with Digital Intelligence FireChief and a laptop computer
- If you want to reduce hardware to carry:
  - WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon



# Recommendations for a Forensic Workstation

## (2 of 3)

- Recommendations when choosing stationary or lightweight workstation:
  - Full tower to allow for expansion devices
  - As much memory and processor power as budget allows
  - Different sizes of hard drives
  - 400-watt or better power supply with battery backup
  - External FireWire and USB ports
  - Assortment of drive adapter bridges

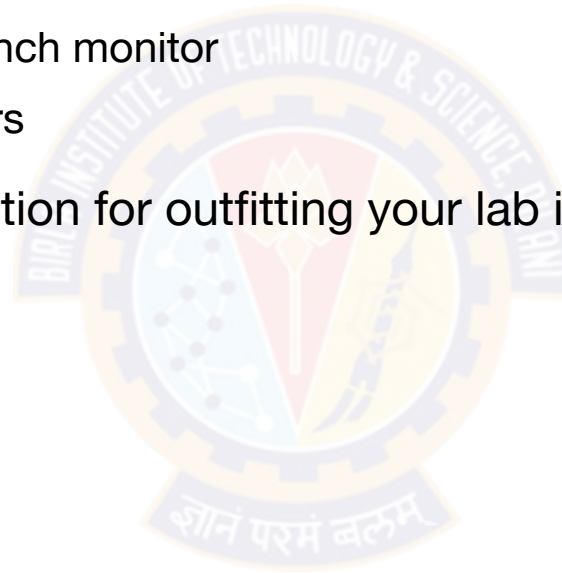




# Recommendations for a Forensic Workstation

## (3 of 3)

- Recommendations when choosing stationary or lightweight workstation (cont'd):
  - Ergonomic keyboard and mouse
  - A good video card with at least a 17-inch monitor
  - High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs



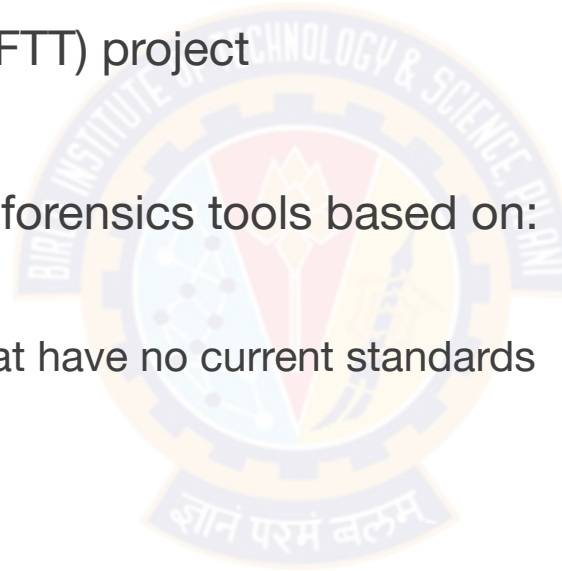
# Validating and Testing Forensic Software

- It is important to make sure the evidence you recover and analyze can be admitted in court
- You must test and validate your software to prevent damaging the evidence



# Using National Institute of Standards and Technology Tools (1 of 3)

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on forensics tools
- NIST has created criteria for testing forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards



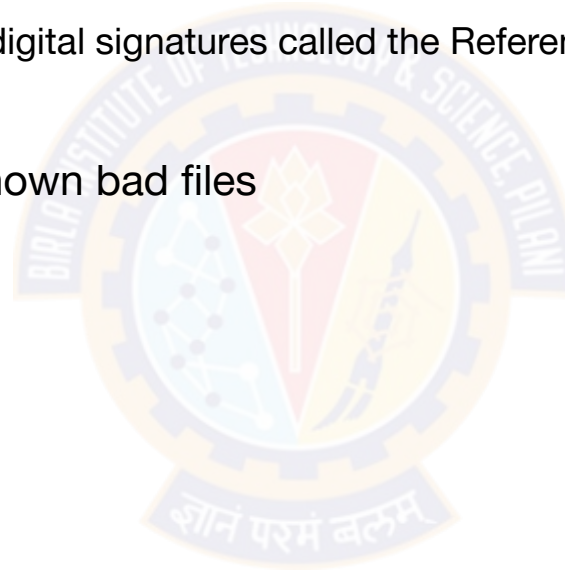
# Using National Institute of Standards and Technology Tools (2 of 3)

- Your lab must meet the following criteria
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- ISO 5725 - specifies results must be repeatable and reproducible



# Using National Institute of Standards and Technology Tools (3 of 3)

- NIST created the 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



# Using Validation Protocols (1 of 3)

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how forensics tools work
- One way to compare results and verify a new tool is by using a disk editor
  - Such as Hex Workshop or WinHex



# Using Validation Protocols (2 of 3)

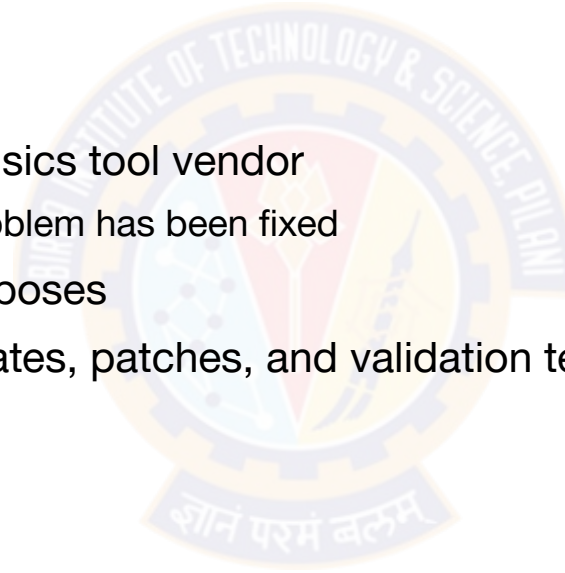
- Disk editors do not have a flashy interface, however they:
  - Are reliable tools
  - Can access raw data
- Digital Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools





# Using Validation Protocols (3 of 3)

- Digital Forensics Tool Upgrade Protocol
  - Test
    - New releases
    - OS patches and upgrades
  - If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools



# Summary (1 of 3)

- Consult your business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab



# Summary (2 of 3)

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - Command-line
  - GUI
- Forensics hardware
  - Customized equipment
  - Commercial options
  - Include workstations and write-blockers



# Summary (3 of 3)

- Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools
- Always run a validation test when upgrading your forensics tools





# Thank You!

Next chapter:  
Foundation for forensics

No.	Title of the Module
M1	Introduction to Cyber Crime, Digital Forensics and Incident Handling
M2	Foundation for Forensics
M3	Computer Crime and Identity Theft/Fraud
M4	Digital Forensic Process, Analysis and Validation
M5	Disk Structures (File Systems) and Data-hiding techniques
M6	Network and Cloud Forensics; Mobile Device and Security
M7	Digital Forensic Tools and Labs
M8	Organizations and Cyber Crime, Criminology and Organized Crime
M9	Investigating Internet Crime and E-Mail Crime
M10	Cyberspace Infrastructure and Enterprise Security
M11	Incident Detection and Characterization
M12	Incident Response and software Tools
M13	Incident Report Writing
M14	Emerging Cybercrime Trends, Recommendations and Practical Issues
M15	Miscellaneous Topics