

Conducting Computer Forensics in Education

***Presented By
Rob Lipton, Ph.D.
IT-ETS Technical Project Administrator
Berks County Intermediate Unit***



Submitted by:
Anthony
Rieder,
Butler County
Area
Vocational-
Technical

School

Objectives

- Understand computer forensics
- Prepare for computer investigations
- Conducting an investigation
- Understand computer forensics workstations and software
- Understand how to identify needs for computer forensics tools

Understanding Computer Forensics

Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases

Computer Forensics Versus Other Related Disciplines

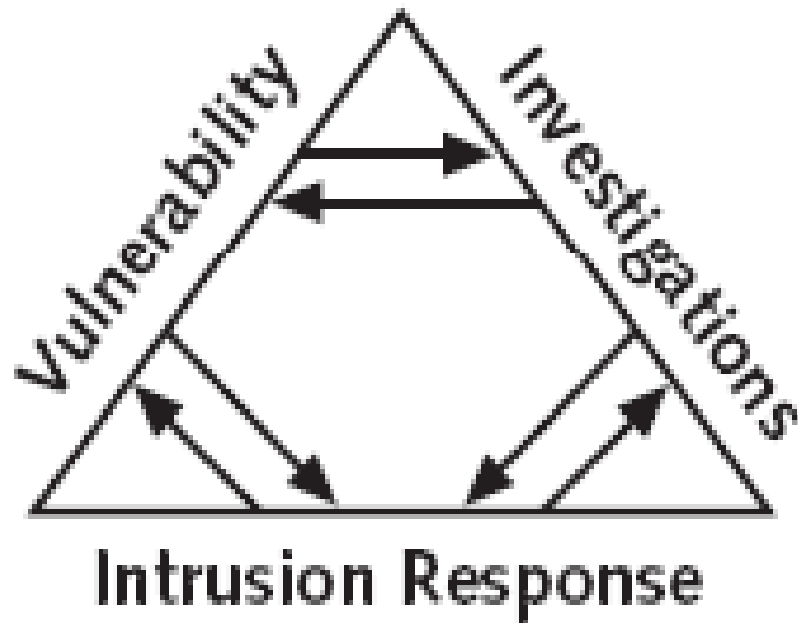


Figure 1-1 The investigations triad

Guide to Computer Forensics and Investigations, 2e
Course Technologies 2007

Computer Forensics

- ***includes:***
 - Securely collecting computer data
 - Examining suspect data to determine details such as origin and content
 - Presenting computer-based information to courts
 - Applying board policies and laws to computer practice

Involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in an administrative hearing or court

A Brief History of Computer Forensics

- **Well-known crimes— one-half cent**
- By the early 1990s, specialized tools for computer forensics were available
 - EnCase
 - Forensic Tool Kit (FTK)
 - Resources for Forensic Software and Hardware



Acquiring Certification and Training

Update your skills through appropriate training

- International Association of Computer Investigative Specialists (IACIS)
 - Certified Electronic Evidence Collection Specialist (CEECS)
 - Certified Forensic Computer Examiners (CFCEs)
- High-Tech Crime Network (HTCN)
 - Certified Computer Crime Investigator,
 - Certified Computer Forensic Technician,
- EnCase Certified Examiner (EnCE) Certification



Using National Institute of Standards and Technology Tools

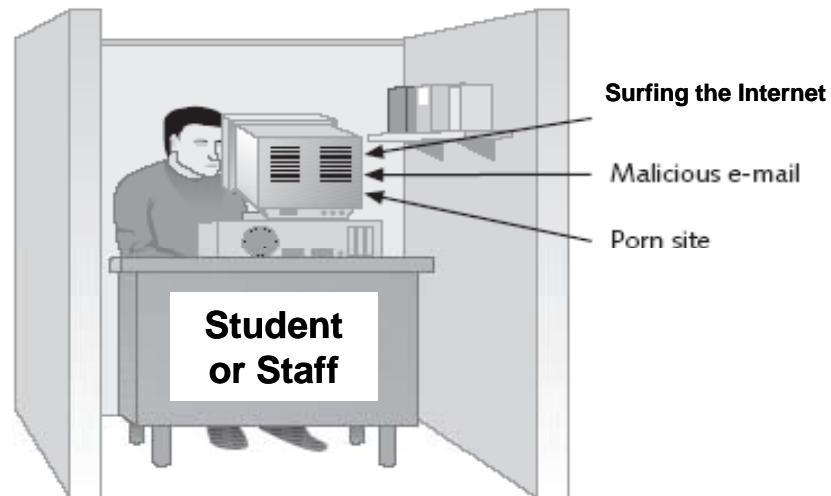
- Computer Forensics Tool Testing (CFTT) program
 - Based on standard testing methods
 - ISO 17025 criteria
 - ISO 5725
- Also evaluate disk imaging tools
 - Forensic Software Testing Support Tools (FS-TSTs)
- National Software Reference Library (NSRL) project
 - Collects all known hash values for commercial software applications and OS files
 - Helps filtering known information
- **Great Training Resource**
<http://www.forensics.nl/presentations>

Preparing a Computer Investigation



Preparing For Computer Investigations

- **Public investigations**
 - Government agencies responsible for criminal investigations and prosecution
- **School investigations**
 - School's IT Staff



abuse of computer privileges

Basic's of an Investigation

- Understand violations of policies & laws
 - School district, city, county, state, and federal laws on computer-related crimes
 - PA Statute Fraud 18: 3933(a)(1)*
 - PA Statute Misuse of Computer System Information 18: 3933(a)(3)*
 - PA Statute Unauthorized use or alteration of data 18: 3933(a)(2)
- Know how to build an administrative case
 - Include details use by authorities for criminal prosecution

Until 1993, laws defining computer crimes did not exist

Following the Legal Process

- A criminal or **administrative** case follows three stages:
 - Complaint
 - Someone files a complaint
 - Investigation
 - A specialist (*Tech Director*) investigates the complaint
 - Prosecution
 - Prosecutor (*Administrative Panel*) collects evidence and builds a case

Search Warrant Case Law

Commonwealth V. Copenhefer
553 PA 285, 719 A.2d 242

The Fourth Amendment to the U.S. Constitution protects everyone's rights to be secure in their person, residence, and property from search and seizure

Preparing a Computer Investigation

- Gather evidence to prove a suspect committed a crime or violated a civil policy
- Collect evidence that can be offered in court or at an inquiry
 - Investigate the suspect's computer
 - Preserve the evidence on a different computer
- Follow an accepted procedure to prepare a case
- *Chain of custody*
 - Route the evidence takes from the time you find it until the case is closed or goes to court

Identifying the Case Requirements

- Identify requirements, such as:
 - *Nature of the case*
 - *Suspect's name*
 - *Suspect's activity*
 - *Suspect's hardware and software specifications*

Reviewing a Case

- **Tasks for planning your investigation**
 - Identify the case requirements
 - Plan your investigation
 - Conduct the investigation
 - Complete the case report
 - Critique the case

Planning Your Investigation

- List what you can assume or know
 - Several incidents **may** or **may not** be related
 - Suspect's computer can contain information about the case
 - Whether someone else has used suspect's computer
- Make an image of suspect's computer disk drive
- Analyze – **Make a forensic copy**

Planning your Investigation

A basic investigation plan:

- Prepare a forensics workstation
- Obtain the evidence from the secure container
- Make a forensic copy of the evidence
- Return the evidence to the secure container
- Process the copied evidence with computer forensics tools
- Don't forget to create an evidence custody form
 - helps you document what has been done with the original evidence and its forensics copies

Taking a Systematic Approach

● **What you Should Do**

- Make an initial assessment about the type of case you are investigating
- Determine a preliminary design or approach to the case
- Create a detailed design
- Determine the resources you need
- Obtain and copy an evidence disk drive
- **Analyze and recover the digital evidence**
- Investigate the data you recovered
- Complete the case report
- Critique the case

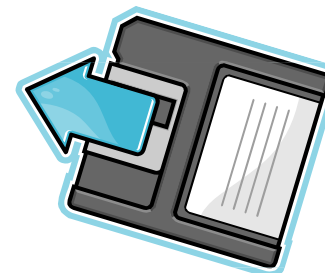
Preparing for a Computer Related Search

● **Steps**

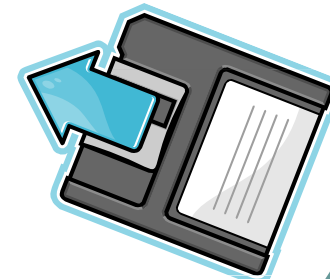
- *Determining who is in charge*
- *Using additional technical expertise*
- *Determining the tools you need*
- *Preparing the investigation team*

Conducting an Investigation

- Copy the evidence using a variety of methods
 - No single method retrieves all data
- More methods used is better



Slow response can cause digital evidence lost

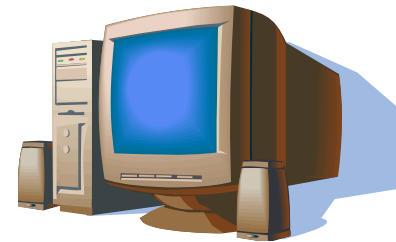


Securing a Computer Incident

- Preserve the evidence
- Keep information confidential
- Define a secure perimeter
 - Use yellow barrier tape
 - Legal authority
- Professional curiosity
 - Can destroy evidence

Identifying the Type of Computing System

- **Identify:**
 - Size of the disk drive
 - Number of computers at the crime scene
 - OS Type(s)
 - Specific details about the hardware
- **Easier to do in a controlled environment**



Determining Whether You Can Seize a Computer

- **Ideal situation**

- Seize computers and take them to your lab

- **Not always possible**

- Need a warrant
- Consider using portable resources

Seizing Digital Evidence at the Scene

- Law enforcement seizes evidence using a warrant
 - Review U.S. DoJ standards for seizing digital data
- Civil investigations follow same rules
 - Requires less documentation



**Consult with your school solicitor
for guidelines**

Securing your Evidence

- Use evidence bags to secure and catalog the evidence
- Use computer safe products
 - Antistatic bags
 - Antistatic pads
- Use well-padded containers
- Use evidence tape to seal all openings
 - Floppy disk or CD drives
 - Power supply electrical cord
- Write your initials on tape to prove that evidence has not been tampered
- Consider computer-specific temperature and humidity ranges

Using Additional Technical Expertise

- Look for specialists
 - OSs
 - RAID servers
 - Databases
- Educate specialists in proper investigative techniques
 - Prevent evidence damage

Processing Data Centers with an Array of RAIDs

- Sparse evidence file recovery
 - Extracts only data related to evidence for your case from allocated files
 - Minimizes how much data you need to analyze
 - *Doesn't recover residual data in free or slack space*
 - If you have a computer forensics tool that accesses the unallocated space on a RAID system, work it on a test system first to make sure it doesn't corrupt the RAID computer
 - **Terabyte of Music is enough storage for 20 years of continuous music**

Retrieving Evidence Data Using a Remote Network Connection

- Bit-stream image copies can also be retrieved from a workstation's network connection
- **Software:**
 - SnapBack
 - EnCase
 - R-Tools
- Can be a time-consuming process even with a 1000-Mb connection
- It takes less using a NIC-to-NIC connection
- Different than Network Forensics

Processing a Major Incident



Processing a Major Incident

- Guidelines

- Sketch the incident or crime scene
- ***Check computers as soon as possible***
- Save data from current applications
- Make notes of everything when copying data from suspect's computer
- Close applications and shutdown the computer

Processing a Major Incident

● **Guidelines**

- Look for information related to the investigation
 - Passwords, passphrases, PINs, bank accounts
- Collect documentation and media related to the investigation
 - Hardware, software, backup media

Processing a Major Incident

- Guidelines
 - Keep a journal
 - Secure the scene
 - Be professional and courteous with onlookers
 - Remove people who are not part of the investigation
 - Video record the computer area
 - **Pay attention to details**

Using a Technical Advisor at an Incident

- **Technical specialists**

- Responsibilities:

- Know aspects of the seized system
- Is direct investigator handling sensitive material
- Help securing the scene
- Help document the planning strategy
- Conduct ad hoc trainings
- Document activities

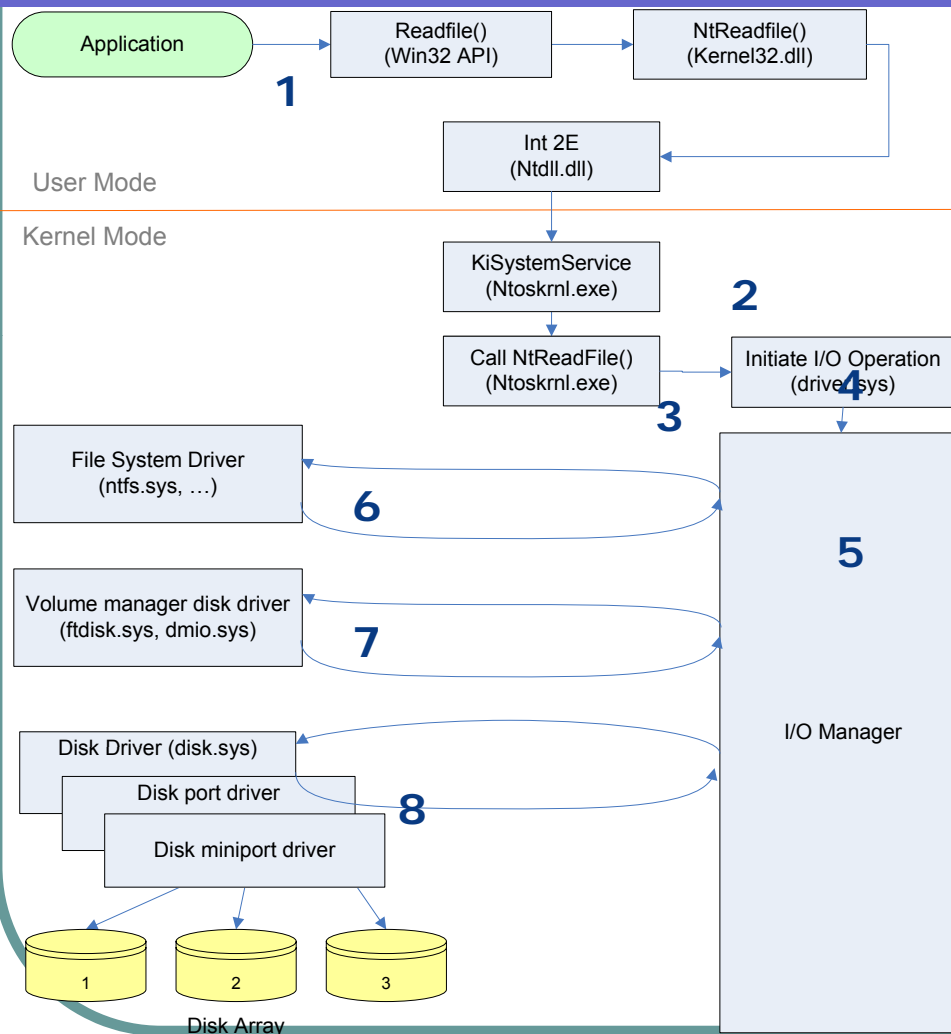
Understanding Data-Recovery Workstations and Software



Understanding Data-Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- Computer forensics workstation
 - Specially configured personal computer
- To avoid altering the evidence, use:
 - Forensics boot floppy disk
 - Write-blockers devices

What Happens When You Read a File?



1. Readfile() called on File1.txt offset 0
2. Transition to Kernel mode
3. NtReadFile() processed
4. I/O Subsystem called
5. I/O Request Packet (IRP) generated
6. Data at File1.txt offset 0 requested from ntfs.sys
7. Data at D: offset 2138231 requested from dmio.sys
8. Data at disk 2 offset 139488571 requested from disk.sys

Copying the Evidence Disk

- A forensic copy is an exact duplicate of the original data
- Create a forensic copy using:
 - MS-DOS
 - Specialized tool such as Digital Intelligence's Image
 - First, create a bit-stream image
 - Then, copy the image to a target disk

Assembling the Tools for a Forensic Boot Floppy Disk

● **Tools:**

- Disk editor such as Norton Disk Edit or Hex Workshop
- Floppy disk
- MS-DOS **OS**
- Computer that can boot to a true MS-DOS level
- Forensics acquisition tool
- Write-block tool



Creating a Forensic Boot Floppy Disk

- **Goal** is not to alter the original data on a disk
- Preferred way to preserve the original data is to never examine it
 - Make forensic copies
 - Create a special boot floppy disk that prevents OS from altering the data when the computer starts up
 - Windows 9x can also alter other files, especially if DriveSpace is implemented on a file allocation table (FAT) 16 disk

Understanding Bit-stream Copies

- Bit-by-bit copy of the original storage medium
- Exact copy of the original disk
- Different from a simple backup copy
 - Backup software only copy known files
 - Backup software cannot copy deleted files or e-mail messages, or recover file fragments
- A bit-stream image file contains the bit-stream copy of all data on a disk or partition
- Preferable to copy the image file to a target disk that matches the original disk's manufacturer, size, and model

Assembling the Tools for a Forensic Boot Floppy Disk

- **Steps:**

- Make the floppy disk bootable
- Update the OS files to remove any reference to the hard disk (using Hex Workshop or Norton Disk Edit)
 - Modify the command.com file on the floppy disk
 - Modify the io.sys file on the floppy disk
- Add computer forensic tools
- Test your floppy disk
- Create several backup copies

Using a Write-Blocker

- Prevents data writes to a hard disk
- Software options:
 - Software write-blockers are OS-dependent
 - PDBlock
- Hardware options
 - Ideal for GUI forensic tools
 - Act as a bridge between the disk and the workstation

Using a Write-Blocker

- Discards the written data
- For the OS, the data copy is successful
- Connecting technologies
 - FireWire
 - USB 2.0
 - SCSI controllers

Determining the Tools You Need

- Prepare your tools using incident and crime scene information
- Initial-response field kit
 - Lightweight
 - Easy to transport
- Extensive-response field kit
 - Includes all tools you can afford

Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for high-end analysis tasks

Recommendations for a Forensic Workstation

- Data acquisition techniques:
 - USB 2.0
 - FireWire
- Expansion devices requirements
- Power supply with battery backup
- Extra power and data cables
- External FireWire and USB 2.0 ports

Stocking Hardware Peripherals

- Any lab should have in stock:
 - IDE cables
 - Small Computer System Interface (SCSI) cards, preferably ultra-wide
 - Graphics cards, both PCI and AGP types
 - Power cords
 - Hard disk drives
 - At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA adapter
 - Computer hand tools

Determining the Tools You Need

Number Needed	Tools
1	Small computer tool kit
1	Large-capacity disk drive
1	IDE ribbon cable, 36 inches or longer (ATA-33 or ATA-100)
1	Forensic boot floppy disk containing your preferred acquisition utility
1	Laptop IDE 40- to 44-pin adapter
1	Laptop personal computer (PC)
1	FireWire or USB dual write-protect external bay IDE disk drive box
1	Flashlight
1	Digital camera or photographic camera with film and flash
10	Evidence log forms
1	Notebook or dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marking pen
10	Floppy disks

Determining the Tools You Need

Tools in an Extensive-Response Field Kit

Number Needed	Tools
Varies	Assorted technical manuals ranging from (OS) references to forensic analysis guides
1	Initial-response field kit
1	Portable PC with SCSI card for DLT tape drive or suspect's SCSI drive
1	DLT or Super-DLT portable tape drive
10	DLT or Super-DLT tape cartridges
1	DLT or Super-DLT tape cleaning cartridge
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Gloves (leather) and disposable latex gloves (assorted sizes)
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from suspect's interior CPU cabinet
1	Iomega 250 MB Zip drive
1	Iomega 750 MB Zip drive
1	Iomega 2 GB Jaz drive
10	Iomega 100 MB Zip cartridges
10	Iomega 250 MB Zip cartridges
10	Iomega 750 MB Zip cartridges
10	Iomega 1 GB Jaz cartridges
10	Iomega 2 GB Jaz cartridges
5	Additional assorted hard disk drives for data acquisition

Maintaining Operating Systems and Application Software Inventories

- Maintain licensed copies of software, like:
 - Microsoft Office XP, 2003, 2000, 97, and 95
 - Quicken
 - Programming languages
 - Specialized viewers
 - Corel Office Suite
 - StarOffice/OpenOffice
 - Peachtree accounting applications

Using Laptop Forensic Workstations

- Create a mobile forensic workstation using a laptop PC
 - FireWire port
 - USB 2.0 port
 - PCMCIA SATA hard disk
- Laptops are still limited as forensic workstations, but are improving

Types of Computer Forensics Tools



Types of Computer Forensics Tools

- **Hardware forensic tools**
 - Single-purpose components
 - Complete computer systems and servers
- **Software forensic tools**
 - Command-line applications
 - GUI applications

Computer Hardware Tools

- Provide analysis capabilities
- Hardware eventually fails
 - Schedule equipment replacements
 - When planning your budget
 - Failures
 - Consultant and vendor fees
 - Anticipate equipment replacement

Computer Forensics Software Needs

- Look for versatility, flexibility, and robustness
 - OS
 - File system
 - Script capabilities
 - Automated features
 - Vendor's reputation
- Keep in mind what applications you analyze

GUI Forensic Tools

- Simplify computer forensics investigations
- Help training beginning investigators
- Most of them come into suites of tools

Tasks Performed by Computer Forensics Tools

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

Acquisition

- Acquisition categories:
 - Physical data copy
 - Logical data copy
 - Data acquisition format
 - Command-line acquisition
 - GUI acquisition
 - Remote acquisition
 - Verification



Validation and Discrimination

- Hashing
 - Cyclic redundancy check (CRC)-32, MD5, Secure Hash Algorithms (SHAs)
- Filtering
 - Based on hash value sets
- Analyzing file headers
 - Discriminate files based on their types

Extraction

- Major techniques include:
 - Data viewing
 - How data is viewed depends on the tool used
 - Keyword searching
 - Recovers key data facts
 - Decompressing
 - Archive and cabinet files

Extraction

- Major techniques include:
 - Carving
 - Reconstruct fragments of deleted files
 - Decrypting
 - Password dictionary attacks
 - Brute-force attacks
 - Bookmarking
 - First find evidence, then bookmark it

Reconstruction

- Re-create a suspect's disk drive
 - Techniques
 - Disk-to-disk copy
 - Image-to-disk copy
 - Partition-to-partition copy
 - Image-to-partition copy

Reporting

- **Configure your forensic tools to:**
 - Log activities
 - Generate reports
- **Use this information when producing a final report for your investigation**

Tool Comparisons

Forensic Tool Functions and Subfunctions Comparison

VENDOR TOOL	AccessData Ultimate Toolkit	Guidance Software EnCase	Digital Intelligence DriveSpy
FUNCTION			
Acquisition			
Physical data copy	√	√	
Logical data copy	√	√	√
Data acquisition formats	√	√	
Command-line process		√	√
GUI process	√	√	√
Remote acquisition		√*	
Verification	√	√	√
Validation and Discrimination			
Hashing	√**	√**	√
Filtering	√	√	√

Tool Comparisons

Forensic Tool Functions and Subfunctions Comparison (continued)

VENDOR TOOL	AccessData Ultimate Toolkit	Guidance Software EnCase	Digital Intelligence DriveSpy
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	√		

*Must purchase Enterprise Edition for this feature

**Both MD5 and SHA-1

***Supported file formats vary

Other Considerations for Tools

- Flexibility
- Reliability
- Expandability
- **Keep a library with older version of your tools**



Questions



Computer forensic tools

SABRE Security 2004: <http://www.sabre-security.com/products/bindiff.html>

ByteBack III: <http://www.toolsthatwork.com/byte.shtml>

History Reader for IE 5.x and 6.x:

<http://www.wbaudisch.de/HistoryReader.htm>

CD/DVD Diagnostic: <http://www.cdrom-prod.com/cddvddiagnostic.htm>

dtSearch: <http://patriot.net/~carvdawg/scripts/hasher.pl>

hackman: <http://www.technologismiki.com/hackman/>

Hex Workshop: <http://www.hexworkshop.com/features.html>

KaZAlyser: <http://www.sandersonforensics.co.uk/kazalyser.htm>

Passware Kit: <http://www.lostpassword.com/kit.htm>

Secret Explorer: <http://lastbit.com/wse/default.asp>

E-mail Examiner: <http://www.paraben-forensics.com/examiner.html>

pda seizure: <http://www.paraben-forensics.com/pda.html>