The Forensic Process Examined:
Creating cases for classroom use

Yvonne LeClaire
Lewis University
MSIS 68-595

Table of Contents

Introduction

Computer forensics can be defined as "obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases." [1] While computer forensics may seem to be a fairly mainstream idea, the field of study can hardly be called new. Computer forensics had its somewhat formal beginnings in 1984 with the creation of the FBI's Magnetic Media Program, now known as CART (Computer Analysis and Response Team). CART provides assistance to the FBI and other law enforcement agencies in the search and seizure of computers during investigations. [2]

The Federal Rules of Evidence has controlled the use of digital evidence since 1970.[3] The rules differ depending on the type of case and the type of digital evidence obtained. This paper will not deal with the legal specifics of each type of case. I will leave that to the lawyers. In part, this paper will deal with the specifics of collecting and analyzing digital evidence, assuming that all the required paperwork and warrants are in order at the time of collection.

There are a number of different forensic tools that can be used to analyze digital data, some of the more common being Access Data's FTK, Guidance Software's EnCase, and the open source suite SANS Investigative Forensic Toolkit. The focus here will be on Access Data's suite of tools.

The purpose of this project is to show what Access Data has to offer and how the various tools can be used to recover and analyze digital data. Procedure for the collection of electronic evidence will also be discussed. Additionally, discussion will include some actual cases in which computer forensics was successfully used to recover evidence, aiding in the eventual conviction of the suspect(s).

The goal for this project is to come up with several evidence-filled hard drive images for use in the classroom. The images will be used for forensic case creation, analysis and reporting. This will be done by fabricating evidence on several computers. Subsequently, in some instances evasive action will be taken. These actions will include hiding, deleting, or encrypting some of the data. Finally, the hard drives will be imaged and analyzed using various tools in Access Data's suite in order to see what evidence can be uncovered, even after the evasive attempts.

Digital Evidence

According to the U.S. Department of Justice:

"Digital Evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device." Digital evidence:

- Is latent, like fingerprints or DNA evidence, often requiring special software, equipment and skill sets to make it visible.
- Crosses jurisdictional borders quickly and easily, which may affect its admissibility.
- Is easily altered, damaged or destroyed. Proper documentation, collection, handling and preservation are essential.
- Can be time sensitive. This is especially true of temporary files or items that have been deleted. While they may still exist in storage, continued use of the device may result in crucial evidentiary data being partially or completely overwritten and potentially unrecoverable.

Where can one find digital evidence? Depending on the type of crime and the number of people involved, the number of devices and their location can vary widely. Recognizing possible sources of digital evidence can be difficult in today's world. Storage devices can be disguised as common household items, such as a pen or pocket knife. Also, the size of electronic devices and their associated storage media seem to be decreasing all the time. Even devices that are not designed specifically for storage can hold a wealth of information for someone trained in digital forensics. Items that first responders should be aware of include the following:

Computers

- Desktop – While the tower is still the most common desktop design, there are also a number of non-traditional designs on the market.
- Laptop
  - Notebook
  - Tablet
  - Netbook
- Server
  - Mini-computer/mid-range server
  - Mainframe/large server
  - Rack-mounted

Storage Devices

- Hard Drives
  - Internal
  - External

- Removable Media
    - Flash drive/thumb drive/USB stick – These can be more difficult to identify because they are commonly disguised as or are a part of common objects, such as:
        - Keychain fob
        - Necklace
        - Pen
        - Pocket knife
        - Watch
        - Toys/knick-knacks
        - Comb
        - Cigarette Lighter
        - Eraser
        - Eyeglasses/sunglasses
        - Bullet
        - Toothbrush
        - Bicycle lock
    - CD/DVD
    - Floppy disk/zip disk
    - Memory cards – ranging is size from the micro SD card (approximately 1/4" x 1/2") to the Compact Flash card (approximately 1 ½" x 1 ¾ ")
    - Tapes – video, audio, data

Handheld Devices

- Digital camera
- Video camera
- Mp3 player
- Voice recorder

  * The four previous items may be difficult to identify because, like the flash drive, they are sometimes disguised as common items.
- Calculator
- Mobile/Smart phone
- Pager
- PDA
- Gaming devices (Nintendo DS, PSP)
- GPS
- e-book reader

Peripheral Devices – Generally speaking, the following items are not designed as storage devices; however, there may be information stored on them that can be used as evidence. In some instances, their presence alone is potential evidence.

- Web cam
- Memory/Sim card reader
- Thumb print reader
- USB hub

- VoIP device
- Printer
- Microphone
- Scanner
- External disk/tape drives
- Monitor
- Mouse
- Keyboard

Network Devices

- Network hub
- Wireless access point
- Modem
- Internal/external wireless card
- Wireless/Bluetooth device
- Antenna
- Network switch
- Router

Miscellaneous Possible Sources

- Fax machine
- Satellite/cable receiver and access cards
- Video game systems
- Surveillance equipment
- Digital video recorders
- Telephone
- Answering machine
- Hard drive duplicator
- Caller ID units
- VCR

The importance of having skilled individuals at the site of evidence collection cannot be stressed enough. First responders should take the proper precautions to prevent the possible loss of evidence. Simple acts such as powering a system on or off, loss of battery power, remote device activation, touching the keyboard or mouse, unplugging a device or cable, may all cause loss of data.[4]

Determining the Course of Action

In addition to becoming familiar with the devices which may contain digital evidence, it is also of value to ask certain questions concerning the case in order to better determine what types of evidence are likely to be found. More importantly, if a situation exists where one course of action must be chosen over another, one must be able to decide which would be more detrimental given the probable location and type of evidence. For example, if a technician had to choose between imaging a live computer or shutting it down and imaging it at the lab, which course of action would be better?

Assume the case was one in which a murder was committed six months ago. A recent tip led authorities to the location to seize the suspect's computer to search for an alleged email sent the day of the murder. In this case, it might be safe to say that the computer could be powered down without the loss of any critical data. However, consider a case in which authorities broke down the door of an alleged drug dealer. At the time of the raid, the suspect was on his computer and actively accessing suspicious documents. It might be a safer bet to image the live drive. An active drug dealer who keeps his records on the computer might be more likely to use a program or utility that encrypts his hard drive at shut down. A murderer who sent a random email six months ago and believed he was not a suspect might not take such precautions.

Computers (or other electronic devices) can have different roles in a crime. Questions that should be asked in order to help determine the best course of action in a particular case are:

To simplify, the following questions are asked using the term 'computer system.' This term can be replaced with any device which may contain electronic evidence.

- Is the computer system contraband of a crime, or criminally possessed? For example, was the computer itself, or any of the software on it, stolen? More indirectly, if a person stole a credit card and used that card to purchase some of the software on their computer, the software is still considered contraband of the crime, even though it wasn't technically "stolen" from the store itself.[5]

  In a case where the computer is contraband of a crime, digital evidence may have little or no part in the investigation. If the warrant under which the computer was seized merely covered stolen computer equipment, forensic analysis of the computer may not even be allowed.

- Is the computer system an instrument of the offense? In other words, was the system used, even in part, to commit the offense? For example, was the computer used to create counterfeit car titles in an auto theft ring in which the cars were stolen and then re-sold with the forged documents? Sometimes the connection is a stretch. In U.S. v Campbell, No. 92-1104, the court ruled that computer equipment was properly seized and was forfeit during the search of a property for marijuana. During the search, a printout detailing the growing characteristics of marijuana was found. The file that the printout originated from was found on the computer. It was ruled that instructions for growing marijuana constituted use of the computer in manufacturing a controlled substance, making it forfeitable under the law.[6]

- Is the computer system only incidental to the offense? More simply put, is it used to store evidence of the offense?[7] For example, if a car thief kept detailed records on his computer concerning all the car that he stole, the computer is incidental to the offense.

- Is the computer system both an instrument of the offense and a storage device for evidence?[8] For example, combining two of the above scenarios; a suspect used

his computer to both create counterfeit car titles and keep detailed records of the cars he stole and resold.

Depending on the case, the role that the same computer plays in a crime can differ. Referring to a previous example, the suspect was charged with manufacturing a controlled substance. Since the file on the computer aided him in committing the crime, the computer was a tool of the offense. However, consider the suspect was instead charged with possession of a controlled substance. He claimed that marijuana found in his home did not belong to him, nor did he even know what it looked like. The file on the computer could possibly be used as evidence to show that he was lying concerning his ignorance in the matter.

Whether one is a first responder or a forensic technician in the lab, answering the previous questions will aid in determining the best course of action in a particular case. As a first responder, it will help determine what items should be seized and whether or not a live imaging is in order. As a technician in the lab, it may be helpful in determining the type of evidence that might be found and the places that evidence is likely to exist on the system. This would most certainly narrow the scope of the examination, resulting in a more efficient search and quicker results. With the growing size of computer storage and the number of files present on even one small computer system, this is an important concern.

Uses for Digital Evidence

As shown, digital evidence can take many forms and play many roles in an investigation but, what is its true value? The following examples help to illustrate:

"In 2005, digital evidence from a floppy drive led investigators to the BTK serial killer, a criminal who had eluded police capture since 1974 and claimed at least 10 victims. Digital evidence from a mobile phone led international police to the terrorists responsible for the Madrid train bombings, which resulted in the deaths of at least 190 people in 2004. Digital evidence collected from computer networks at university and military sites in the 1980s led to the discovery of international espionage supported by a foreign government hostile to the United States."[9]
The question of the value of digital evidence can best be answered by discussing, more specifically, some of the ways it can be used in an investigation.

Direct Relation
Most apparently, digital evidence can directly relate to an offense. An example of this would be finding pornographic pictures or videos of children on the computer of someone under investigation for possession of child pornography. If the examiner finds that the computer was also used to upload the pictures to a website or to send them to someone in an email, the suspect can possibly be charged with distribution of child pornography as well.

Assume that further analysis shows that the video footage came from a specific video camera which was also recovered from the suspect's home. Forensic examination of the video camera reveals additional pornographic footage in which the suspect was present as well as the children. The footage was deleted in an attempt to destroy evidence but was recovered by the technician nevertheless. The suspect's charges might well be amended to include child molestation at this point. The value of digital evidence is apparent in a case such as this.

In less concrete but still valuable examples of digital evidence directly relating to a crime; law enforcement officials may be investigating a string of car thefts. A flash drive found at the home of a suspect reveals pictures of a number of the cars that were stolen. When investigating a woman accused of harassment by her ex-boyfriend, technicians find threatening emails and a digital journal containing a detailed schedule of her ex-boyfriend's activities for the previous three-month period. While this evidence by itself may not assure a conviction, it may be combined with other evidence to get a better look at the whole picture.

Show Intent

Digital evidence is often used to show intent or premeditation. "Many digital devices efficiently track user activity; it is also possible to recover deleted files, both of which may affect a criminal investigation."[10] The fact that a file exists on a computer may point to a suspect's guilt. However, the manual deletion of the file may be an even stronger indicator of that guilt. For example, a man was accused of accidentally killing his wife when an argument over her infidelity turned violent. Upon examination of his computer, deleted Internet files were found containing the search terms "perfect murder," "quick ways to kill someone," and "getting away with murder."[11] The search terms themselves are strong indicators that premeditation was involved. The fact that he deleted those searches with the hope of avoiding detection strengthens that theory even more. The potential difference is huge: manslaughter (accident) or murder (premeditation)?

Support or Refute Testimony

Quite often digital evidence is used to support the testimony of a witness who might otherwise seem less than credible. For example, assume a teenager is accused of being involved in a hit-and-run accident. He claims he was at home, twenty miles away, at the time of the accident. Text messages retrieved from his cell phone prove that he was, in fact, at home and in the middle of an hour-long texting session with his girlfriend.

Digital evidence can also be used to refute the testimony of a more credible witness or suspect. A surgeon, involved in a malpractice suit for unnecessary limb removal, claims that the hospital lab was at fault due to incorrect biopsy analysis. Analysis of the lab's log files show that the surgeon began the amputation before the lab had even posted the results of the biopsy. [12]

The same evidence used to support the testimony of one witness can be used to refute the testimony of another. For instance, a known drug dealer may testify that he saw an elected official enter a hotel with a woman who was found murdered later that same day.

The official may deny the charges, stating that he's never seen the woman before. Pictures from the dealer's cell phone clearly show the official entering the hotel with the woman. The dealer states that he snapped the pictures with the intention of blackmailing the married official at a later date. Whatever your view of politicians, in general, the politician would normally be seen as a more credible witness than the drug dealer. However, the digital evidence suggests the opposite in this case.

Expand or Narrow an Investigation
Sometimes, digital evidence may reveal that there is more (or less) to an investigation than originally thought. For example, while investigating possible theft of company secrets, the analysis of a suspect's computer might reveal that the theft is not limited to one employee. There may be evidence that secret documents are being transferred between a group of people both inside and outside the company. Conversely, where an entire group of people are suspected, evidence may show that a fewer number are actually involved.

Narrowing the Scope

Examining a computer for digital evidence can prove to be an enormous task. As a forensic examiner, it is important to know the type of investigation you're dealing with, in order to fine-tune the scope of the investigation. While traveling down one path, the examiner may find others that require exploration. However, it is important to have a starting point for the sake of efficiency. Where does one start?

Starting Points – As provided by the Department of Justice, the following are some of the more common starting points for forensic examination by case type.

- Death investigation
    - Email
    - Images
    - Financial documents
    - Internet searches/activities
    - Medical records
    - Journal/diary
    - Legal documents and wills

  Any specific details concerning the case may be helpful in narrowing the scope as well. For instance, if it was suspected that a man murdered his spouse due to infidelity, a search for the first four items might be beneficial, whereas medical records would be less likely to be of any evidentiary value. However, if the possible motive for murder was financial distress due to prolonged illness of the spouse, medical records may be more pertinent than something such as images.

- Child Exploitation/Abuse
    - Images
    - Email
    - Chat logs

- Internet activity logs
- Digital camera/video software
- Graphic/video editing software
- Games

Some evidence is more obvious than others. For example, it is difficult to say that child pornography is anything other than what it is. However, a seemingly harmless logged chat between two children planning to meet up after school becomes a different matter entirely when it is known that no children live in or even visit the home the computer was seized from.

- Domestic Violence
  - Address books
  - Journal/Diary
  - Email
  - Financial records
  - Medical records

While some of the items, such as financial records, may not contain direct evidence of the crime, they can definitely point to motive.

- Stalking
  - Address books
  - Email
  - Journal/Diaries
  - Images
  - Internet activity logs
  - Telephone records
  - Victim background research
  - Legal documents

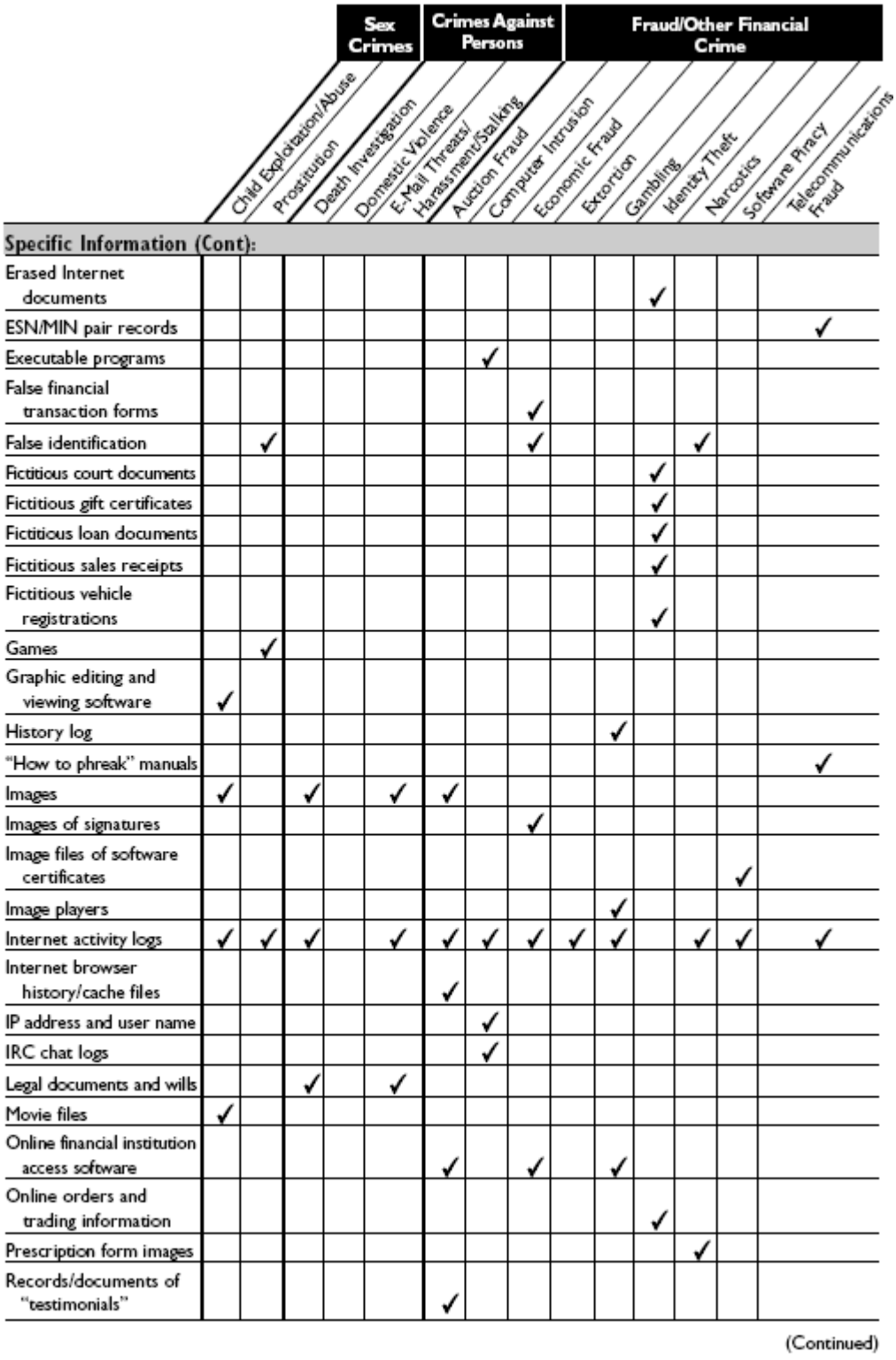
Without a doubt, these starting points are invaluable for increasing the efficiency of any investigation. See figures 1a, 1b, and 1c for a more complete matrix listing of crimes and the likely types of digital evidence connected to each.[13]

At the Scene - Procedure

We have looked at the different devices that can provide investigators with digital evidence, the ways in which they can provide it, and the forms that it can take. In order for it to be useful in a court of law, it is of the utmost importance that procedure be followed concerning the collection, transportation, and storage of any devices that may contain digital evidence. As stated, this paper will not deal with the legalities of whether or not something "can" be taken. The following procedure assumes that all the required paperwork and warrants are in order.

	Sex Crimes					Crimes Against Persons			Fraud/Other Financial Crime						
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunications Fraud
General Information:														
Databases		✓				✓		✓		✓		✓		
E-Mail/notes/letters	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financial/asset records		✓	✓	✓	✓	✓		✓		✓		✓		✓
Medical records		✓	✓	✓										
Telephone records			✓	✓	✓	✓								✓
Specific Information:														
Account data						✓								
Accounting/bookkeeping software						✓								
Address books		✓	✓	✓	✓	✓	✓	✓		✓		✓		
Backdrops											✓			
Biographies			✓											
Birth certificates											✓			
Calendar		✓				✓		✓		✓		✓		
Chat logs	✓					✓							✓	
Check, currency, and money order images								✓			✓			
Check cashing cards											✓			
Cloning software														✓
Configuration files							✓							
Counterfeit money											✓			
Credit card generators											✓			
Credit card numbers											✓			
Credit card reader/writer											✓			
Credit card skimmers								✓						
Customer database/ records		✓								✓				✓
Customer information/ credit card data						✓		✓		✓				
Date and time stamps	✓								✓					
Diaries			✓	✓	✓									
Digital cameras/software/ images	✓					✓					✓			
Driver's license											✓			
Drug recipes												✓		
Electronic money										✓				
Electronic signatures											✓			

Figure 1a – Source: U.S. Department of Justice



	Sex Crimes					Crimes Against Persons			Fraud/Other Financial Crime					
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunications Fraud
Specific Information (Cont):														
Erased Internet documents											✓			
ESN/MIN pair records														✓
Executable programs							✓							
False financial transaction forms								✓						
False identification		✓						✓				✓		
Fictitious court documents											✓			
Fictitious gift certificates											✓			
Fictitious loan documents											✓			
Fictitious sales receipts											✓			
Fictitious vehicle registrations											✓			
Games		✓												
Graphic editing and viewing software	✓													
History log										✓				
"How to phreak" manuals														✓
Images	✓		✓		✓	✓								
Images of signatures								✓						
Image files of software certificates													✓	
Image players										✓				
Internet activity logs	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓
Internet browser history/cache files						✓								
IP address and user name							✓							
IRC chat logs							✓							
Legal documents and wills			✓		✓									
Movie files	✓													
Online financial institution access software						✓		✓		✓				
Online orders and trading information											✓			
Prescription form images												✓		
Records/documents of "testimonials"						✓								

(Continued)

Figure 1b – Source: U.S. Department of Justice

Specific Information (Cont):	Sex Crimes		Crimes Against Persons			Fraud/Other Financial Crime							
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy Telecommunications Fraud
Scanners/scanned signatures										✓			
Serial numbers												✓	
Social security cards										✓			
Software cracking information and utilities												✓	
Source code							✓						
Sports betting statistics									✓				
Stock transfer documents										✓			
System files and file slack										✓			
Temporary Internet files								✓					
User names							✓		✓				
User-created directory and file names that classify copyrighted software												✓	
User-created directory and file names that classify images	✓												
Vehicle insurance and transfer documentation										✓			
Victim background research					✓								
Web activity at forgery sites										✓			
Web page advertising		✓											

Figure 1c – Source: U.S. Department of Justice

Securing the Scene

In a case where digital evidence may be involved, first responders have a number of responsibilities that cannot be ignored. Failing to follow procedure can result in destruction of both physical and digital evidence or, inadmissibility of some or all of the evidence found.

First and foremost, it is the responsibility of first responders to assure the safety of all persons at the scene. The U.S. Department of Justice outlines the steps that should be followed once the scene and all persons have been secured:

- Immediately secure all electronic devices. This does not mean "seize." It refers to assuring that no unauthorized person has access to any electronic devices. All persons should be removed from the immediate vicinity and offers of technical assistance from unauthorized persons should be refused.
- Ensure that the condition of any electronic device is not altered. If it is on, leave it on. If it is off, leave it off. Absolutely nothing should be touched before documentation of the scene is completed.
- Without touching anything, try to determine the power state of the computer (or electronic device) and take note of any current activity which may indicate that evidence is in the process of being destroyed, such as:
    - Words like "delete," "format," remove," "copy," "move," "cut," or "wipe" on the monitor.
    - Indications that the computer is being accessed remotely.
    - Signs of ongoing communications such as open instant message or chat windows.

  In some cases, immediate action may be necessary. For instance, if a hard drive is in the process of being wiped, it may be necessary to take steps to halt the process, at the expense of possibly losing other evidence. The person in charge would have to make the determination.

Interview Persons of Interest

The Department of Justice also recommends that, within the boundaries of all Federal, State, and local law, adult persons at the scene should be interviewed concerning:

- Users of all electronic devices
- Purpose and uses of all electronic devices
- Computer and Internet user information
- Type and provider of Internet access
- Offsite storage information
- All software in use along with its documentation
- Destructive devices in use
- Automated applications in use
- Data access restrictions in place
- All account names, screen names or usernames, and passwords

The following is an interesting snippet concerning asking people for their passwords. Steven Boucher, a Canadian citizen residing in the U.S., was returning to Canada for a visit in 2006. Boucher's laptop was searched by Immigration officials at the Canadian border. The searching official found thousands of image files that were, by their file names, suspected of being child pornography. Border patrol seized the laptop and shut it down. Unknown to the officials, Boucher had a program on his laptop that encrypted its contents at shut down. Boucher refused to give officials the password needed to decrypt his hard drive. In 2007, a magistrate judge ruled that Sebastien Boucher was not required to provide his password to law enforcement as it would violate his right against self-incrimination. In 2009, a federal district court judge in Vermont disagreed and overturned that ruling. The decision is still in the appeals process.[14]

Documenting the Scene

Documentation of the scene is a critical phase in an investigation. A formal record of the scene is not only helpful for recall purposes, but is necessary from a legal standpoint. Sometimes, the true value of something may not be immediately apparent. The connection an item has to a crime may come from something as simple as its location relative to another item at the scene. For instance, if it was important to know who last used a computer and one person in the house was left-handed while the other was right-handed, the location of the mouse might be an indicator.

At this point, nothing has been touched yet, nor should it be in this phase.

- Note and record the location of all electronic devices, whether connected to something or not. Include all cables in the notes.
- If possible, try to determine the operating system on the computer. This may be helpful information when it comes time to collect the evidence.
- All model and serial numbers of every device should be recorded. If it is not possible to get this information without moving something, wait until the collection phase to gather that information.
- Pictures and video of the entire scene (360 degrees) should be taken. Close-ups should be taken of all cabled connections. Network and wireless access points may indicate the existence of evidence beyond the initial scene. All computer screens should be photographed, even if they are blank or off at the time.
- Do not rely solely on pictures and video. Make sketches when needed and take detailed notes.
- The state, power status, and condition of all electronic devices should be recorded. It is important to keep in mind that, in some cases, evidence may be lost when a device loses power. Battery-powered devices may require more immediate attention than something connected to a wall outlet.

Documentation is not limited to electronic devices. Pieces of paper laying nearby or sticky notes on the computer could reveal possible usernames or passwords. Additionally, other items in the room may reveal important clues. For example, if the room contains Lord of the Rings books, DVDs and posters, the likelihood of Lord of the Rings-related usernames or passwords may be increased. This information can be useful when creating custom dictionaries for use in a password cracking utility, such as PRTK. It is important to note that all items, whether they are going to be seized as evidence or not, should be included in the documentation of the scene. [15, 16]

Seizing the Evidence

After a thorough documentation of the scene, the collection process can begin. This part can get tricky. There are multiple factors which can determine the best course of action and multiple schools of thought on which way is best. Changing technologies make the decisions even more difficult. For instance, performing a RAM dump may prove useful in certain situations but, with newer operating systems that store the contents of RAM at shutdown, this action may not necessarily prove useful.

Additionally, with the introduction of features such as BitLocker*, the decision on how to proceed becomes even more complex. Should you image a live hard drive, or should the system be powered down, taken in, and imaged at the lab? There are no simple answers. As technology continues to evolve, it becomes even more important to have a knowledgeable technician at the scene. The Department of Justice suggests the following:**

Monitor

- If the monitor is on and displays an open program, email, etc., photograph and record the information displayed.
- If the monitor is on and either the screen is blank or a screensaver is visible, move the mouse slightly. Photograph and record the resulting screen activity. If no activity occurs, confirm there is power to the monitor and check the computer for indications that it is, in fact, on (fan noise, lights). If the computer is off, do not turn it on.
- If the monitor is off, turn it on. Photograph and note any activity or lack thereof.

Computer – If the computer is on: "For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the screen, you may need to request assistance from personnel who have experience in volatile data capture and preservation." If there is any indication that data is actively being deleted, overwritten, or otherwise destroyed, immediate disconnection of the power is recommended.

Generally, in a Windows environment, when pulling the plug from the back of the machine, valuable information (such as, most recently used commands, last user login) is preserved. However, disconnection of power is not recommended in the following instances:

- Obvious evidence is in plain view on the screen
- Indications exist that any of the following are active or in use:
    - Chat rooms
    - Open text documents
    - Remote data storage
    - Instant message windows
    - Child pornography
    - Contraband
    - Financial documents
    - Data encryption
    - Obvious illegal activities [19]

*BitLocker is a logical volume encryption system that encrypts the specified volume(s) at shut down in order to protect the data if the equipment is stolen or if the machine comes under attack when off. BitLocker does not protect data on a running machine. [17]

**Before proceeding, keep in mind that digital evidence may also contain evidence of a more physical nature, such as fingerprints. Some materials used to collect physical evidence, such as fingerprint powder, may corrupt or destroy digital evidence. With this in mind, it is generally necessary to perform the needed digital processes before the physical processes. Proper caution should be exercised when collecting digital evidence to prevent the destruction of physical evidence unnecessarily. [18]

If needed and performed, once volatile data capture is complete, the collection process can continue. Imaging may or may not be needed at the scene as well. Whatever the case, the proper documentation should be made. Paperwork requirements will be covered in the next section, the imaging process in another. Once the powered-on computer has been dealt with appropriately, collection can continue using the guidelines for a powered-off computer.

If the computer is off:

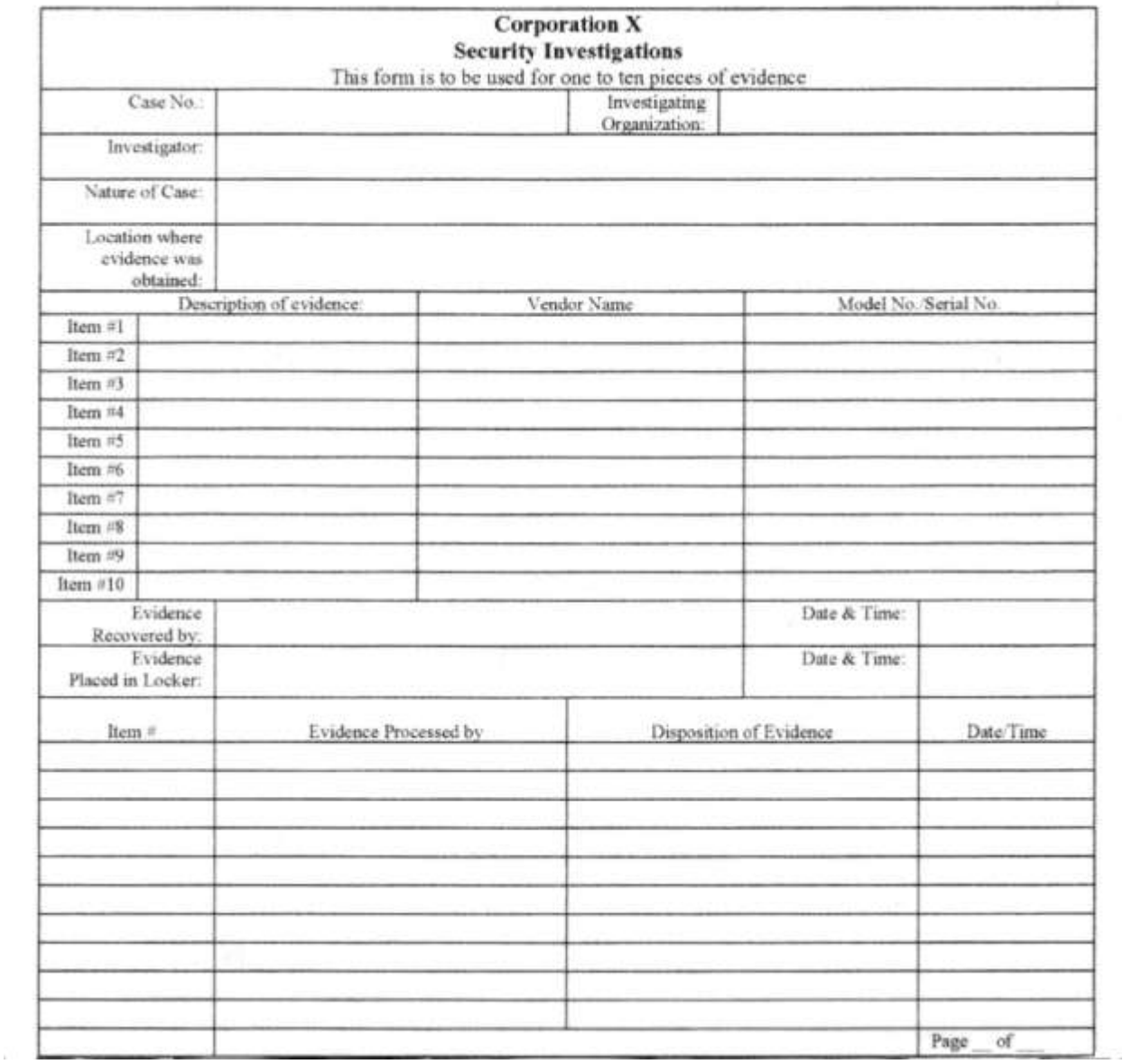
- Document, photograph and/or sketch all devices connected to the computer that were unable to be documented earlier in the "do not touch" phase.
- Uniquely label all cords, cables, and devices along with their corresponding connections on the computer and other devices.
- Photograph everything that was labeled.
- Remove all power supplies, cords, and batteries. Power cords should first be removed from the back of the computer, then from the outlet or power strip
- Remove all remaining cords and devices from the computer.
- If a floppy drive is present and a disk is inside, the disk should be removed and labeled. A spacer should also be put in the floppy drive to protect the heads during transport. Put evidence tape over the slot, making sure to put some type of identifying mark on the tape to prevent tampering.
- If possible, check CD/DVD trays/slots for media and note the status. Tape shut and initial.
- Tape and initial the power switch.
- Record any information that was not viewable earlier (make, model, etc.) and anything that uniquely identifies the computer or components.
- Log all items according to agency procedure.

Chain of Custody

It is critical to properly document all evidence in order to establish a chain of custody. If evidence is to be used in a court of law, the court must be satisfied that the evidence was properly handled and was not tampered with. This begins at the scene. Every item that is taken must be "tagged and bagged," with documentation of this on an evidence form. There is no one specific form that must be used but, all forms should have the fields necessary to record the most pertinent information. Figures 2 and 3 are examples of such forms; one is a multi-evidence form, the other, a single evidence form.

The multi-evidence form is used for multiple pieces of evidence from the same location. If more items are seized than will fit on one form, multiple forms must be filled out and page numbers indicated. A new form must be filled out for each location. The single evidence form is for one single piece of evidence. It offers more flexibility in terms of keeping track of the evidence for chain of custody. If a multi-evidence form is used and evidence is stored in multiple locations, where should the evidence form be kept? The single evidence form solves this problem. All evidence forms remain with the evidence. Of course, best practice would be to use both. The single forms stay with the evidence,

the multi-forms with the case file. The redundancy also adds an extra measure of security.



Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Description of evidence:	Vendor Name	Model No./Serial No.
Item #1		
Item #2		
Item #3		
Item #4		
Item #5		
Item #6		
Item #7		
Item #8		
Item #9		
Item #10		

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of __

Figure 2 – Multi Evidence form
Source: Guide to Computer Forensics and Investigations, Second Edition, Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, 2006

Metropolis Police Bureau
High-tech Investigations Unit

This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of ___

Figure 3 – Single evidence form
Source: Guide to Computer Forensics and Investigations, Second Edition, Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, 2006

Commonly found fields are:

- Case number – this is typically assigned by the organization conducting the investigation but can also be assigned by the law enforcement agency in charge of the case.
- Investigating organization – More than one organization can be in charge of investigating different evidence from the same case. It is important to keep track of who is doing what.
- Investigator – If more than one person is assigned to a case, the lead investigator's name would appear here.
- Nature of case – a brief description of the case, such as, "Kidnapping across state lines"
- Location evidence was obtained – This could be as general as an address or as specific as the exact location in the residence where the evidence was found.
- Description of evidence – should not be too general. If the evidence is a 4 GB flash drive, do not simply list "flash drive."
- Vendor name – manufacturer's name, if available.
- Model and serial number – if available.
- Evidence recovered by – the name of the person who bagged the evidence. This is where the chain of custody begins. The person named here is responsible for the evidence until it reaches the evidence locker in which it will be stored. If this is not possible, the point at which the evidence switched hands must be documented. Any break in the chain of custody can result in evidence being declared inadmissible.
- Date and time – precisely when the evidence was seized.
- Evidence placed in locker – specifically when and where the evidence was placed in the storage location.
- Item number/Evidence processed by/Disposition of evidence/Date/Time – If an evidence item was removed from the locker for processing, these items must be noted. The "Item number" field is, of course, absent from the single evidence form. It is important to remember that, if both single and multi-evidence forms are being used for the same piece of evidence, the information must be noted on both forms.
- Page – Whether using one single form or multiple pages, the format should be "Page 1 of 4," "Page 2 of 4" and so on. [20]

Transporting Evidence

Chain of custody was established when the evidence was tagged and entered into the evidence forms. The equipment must now be securely transported to the examination site. Digital evidence is susceptible to damage from many sources. Care must be taken in the packaging and transporting phase in order to avoid damaging or destroying the evidence. Extremes in temperature, static electricity, humidity, magnetic fields, and rough handling can all potentially destroy data.

Anti-static packaging should be used on all digital evidence. Paper is a good choice, whereas plastic should be avoided. Packaging can consist of various size bags,

envelopes, boxes, and anti-static containers, both padded and non-padded. Large or more fragile items should be place in appropriately padded containers. Mobile phones should be packed in signal-blocking material to avoid transmission of data in either direction. Also, consider using anti-static pads and wrist straps when collecting evidence. Special evidence tape should be used as well. When removed, this tape will either not re-stick or will be destroyed upon removal. When something is tagged or taped, the tape should be initialed by the person securing it. This lessens the chances of tampering. Recall that photographs were taken of all items, both before and after tagging. The same rules should apply to packaging. All items should be clearly labeled and photographed after packaging.

Once bagged, tagged, and photographed, the items are ready for transport. Keep in mind that evidence should not be left in vehicles for long periods of time due to temperature extremes in that type of environment. Avoid putting evidence on heated car seats or near speakers and other devices around which magnetic fields are present. Avoid taking "the bumpy road" if at all possible. Upon arrival at the storage or examination location, be sure to properly document the event on the evidence forms. The evidence is now ready for examination.

At the Lab

The evidence has been properly collected and documented, and has arrived at the lab. What happens now? The examination process is ready to begin. After collecting the evidence from the evidence locker and duly noting this on the evidence form, the examiner can begin. If it was not already done at the scene, the first course of action will be to image the hard drive. What does this mean? Concerning digital forensics, imaging is the process of creating a forensic image of a device with the intention of examining that image for possible evidence. The image is examined, rather than the actual device, in order to avoid altering or destroying the original.

What exactly is a forensic image? The result of a process in which "all areas of the physical disk are copied, sector by sector, to storage media…These images replicate exactly all sectors on a given storage device. All files, unallocated data areas, and areas not normally accessible to a user are copied."[21]

In order to create a forensically sound image, certain procedures must be followed and rules observed.

Write Blockers

First and foremost, when preparing to image an electronic device, a hardware write blocker must be used. Simply put, a write blocker is a device that prevents one device from writing to another. When creating an image of a hard drive, it is imperative to ensure that no data is altered on the drive being copied. Software write blockers exist but, for the purpose of creating forensic images, they are generally not used due to reportedly higher error rates. However, all hardware write blockers are not created equal,

hence the need for standards. NIST, the National Institute of Standards and Technology, outlines the following requirements for hardware write blockers used in forensic imaging:

> **HWB-RM-01** A HWB shall not, after receiving an *operation of any category* from the host nor at any time during its operation, transmit any *modifying category operation* to a protected storage device.
> **HWB-RM-02** A HWB, after receiving a *read category operation* from the host, shall return the data requested by the read operation.
> **HWB-RM-03** A HWB, after receiving an *information category operation* from the host, shall return a response to the host that shall not modify any access-significant information contained in the response.
> **HWB-RM-04** Any error condition reported by the storage device to the HWB shall be reported to the host. [22]

Of course, there are a number of different ways in which a write blocker can be connected, depending on the device being imaged and whether or not a live imaging is being performed. Suffice to say that a write blocker must be used between the source and target.

Imaging Tools

The next order of business is an imaging tool. While there are many programs out there for creating disk images, when creating an image for forensic use, a tool specifically designed for this purpose should be used. Imaging tools are included in most forensics suites such as Access Data's Forensic Took Kit, EnCase, and ProDiscover. As with write blockers, imaging tools also require adherence to a set of standards if the images are to be used for analyzing evidence that will be used in a court of law. NIST outlines the following requirements:

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall be able to verify the integrity of a disk image file.
- The tool shall log I/O errors.
- The tool's documentation shall be correct.

And more precisely:

5.1 Mandatory Requirements
5.1.1 The tool shall not alter the original
5.1.2 If there are no errors accessing the source, then the tool shall create a bit-stream duplicate or image of the source.
5.1.3 If there are I/O errors accessing the source, then the tools shall create a qualified bit-stream duplicate or image of the source. (A *qualified bit-stream duplicate* is defined to be a duplicate except in identified areas of the bit-stream.) The identified areas are replaced by values specified by the tool's documentation.

5.1.4 The tool shall log I/O errors in an accessible and readable form, including the type of error and location of the error.

5.1.5 The tool shall be able to access disk drives through one or more well-defined interfaces.

5.1.6 Documentation shall be correct insofar as the mandatory and any implemented optional requirements are concerned, i.e., if a user following the tool's documented procedures produces the expected result, then the documentation is deemed correct.

5.1.7 If the tool copies a source to a destination that is larger than the source, it shall document the contents of the areas on the destination that are not part of the copy.

5.1.8 If the too copies a source to a destination that is smaller than the source, the tool shall notify the user, truncate the copy, and log this action. [23]

The document continues with specifications for added features, if they exist.

When creating a forensic image for examination, it is considered good practice to create multiple images of the device in the same session; at least two. One copy is used for examination; the other(s) is kept as a backup in case the first copy is destroyed or damaged in any way. Since digital evidence is inherently fragile, it should be handled as little as possible in order to avoid damage and loss of data. With multiple images created, the examiner can return the original to its secure locker, allowing risk of damage to be kept to a minimum.

The Examination

As we will see, evidence can be found in some of the most unlikely places, but more often than not, it is found in the most likely places. It is the job of the examiner to find these places, likely or not, and report the findings without bias.

The examiner, armed with the image(s) and proper forensic tools, can now begin the analysis. There are a number of forensic tools available to perform such an analysis and each has its own strengths and weaknesses. For this reason, examiners often use multiple tools to examine the same image. When beginning an examination, the most pressing question is, "Where do I look first?" The previous listing of case types and likely evidence is a good place to begin. Most forensic tools categorize information by various types in order to help process a case in the most efficient manner. Some of the common categories include: email, media, executables, graphics, OS system files, folders, file system slack, and deleted files. (In a later section, Access Data's approach will be looked at.)

When beginning an analysis, in addition to knowing the type of case and the role the computer had in the crime, it is also helpful to know as much as possible about the circumstances surrounding the case. For instance, is it likely that any of the suspects (or users of the computer) are tech savvy? If so, what is their probable level of experience?

This information may give the examiner additional clues as to where evidence may exist on the computer.

Aside from a user deleting something in an attempt to get rid of it, most digital evidence found is not purposely hidden per se. In most cases, the user simply lacks an understanding of where, when, and how the computer stores information. This makes the examiner's job much easier; the evidence is right there, just where he expected it to be. However, if the user was more skilled, the job of the examiner can become significantly more difficult. Data can be altered and/or hidden in places that are much less obvious. An example of this would be hiding data in file slack. File slack is the "space between the logical end of the file and the end of the last allocation unit (cluster) for that file." [24]

File slack is important to the examiner not only because data can be purposely hidden there but, also because it "could contain fragments of email messages, word processing documents and other sensitive data" [25] such as passwords and login IDs from files that were previously allocated to that cluster. The following explains the two different types of file slack and what each may contain:

- RAM slack - "DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector... [The difference is made up] by padding the remaining space with data from the memory buffers of the operating system. RAM slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. RAM slack pertains only to the last sector of a file."

- Drive slack – "is stored in the remaining sectors which might be needed by the operating system to derive the size needed to create the last cluster assigned to the file…Drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with the disk storage space that has yet to be used by the computer." [26]

Another place that contains potentially valuable information is unallocated space. Unallocated space is defined as "allocation units (sectors or clusters) not assigned to active files within a files system." [27] It in includes, but is not limited to, deleted files. When a file is deleted, the actual data is not deleted; just the pointer to its location in the file system. More specifically, the file name is marked with a special character indicating that the file has been deleted by a user. The computer now views that space as available to store new data or "unallocated." Until the data has been overwritten, it still exists in the same space it has occupied since it was created.

Others ways that one might hide information is through the use of encryption or steganography. Encryption is the process of transforming data, by use of an algorithm, to an unreadable form. A "key" is needed in order to decrypt the data. Steganography is "the art or practice of concealing a message, image, or file within another message,

image, or file." [28] This is done by replacing bits of data from the target file with bits from the source file. The benefit to this is that one can hide secret information in something completely innocent, such as a picture, and it would not be obvious to anyone accessing it. A picture of a family gathering might contain the customer list of a drug dealer, or stolen company secrets. This differs from an encrypted file, which is obviously encrypted to anyone attempting to view it. Steganography tools often include an encryption feature as well. The file is first encrypted and then hidden inside something else.

With these things in mind, even the most skilled technicians can have their work cut out for them. At this point, since I'll be using Access Data's suite of forensic tools (student version) to complete this project, I'd like to turn the focus to Access Data, the tools that they offer, and the purpose of each tool.

AccessData

Access Data, a worldwide industry leader in digital investigations, has been in existence for over 20 years. Their products are intended for use in both law enforcement and corporate environments where there is a need to access and determine the evidentiary value of various forms of electronic data and their associated components. [29] In addition to widespread local law enforcement use, Access Data's Forensic Toolkit is the primary tool used by CART in the training of their examiners. CART Certification is a requirement for all FBI Forensic Examiners. [30]

Unless otherwise cited, the following information is taken from Access Data's FTK 3.0 User guide. [31] While the offerings include many network-related tools, these are not available in the student edition that I will be using. I will mention their uses here, but my focus will be on those related to stand-alone computer systems.

AccessData eDiscovery

By definition, eDiscovery is "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case." [32] AccessData eDiscovery is a custodian-based, end to end solution designed to gather data required for investigating a legal matter. It also allows tracking of multiple legal matters and groups their data into "collections." Each collection can contain any combination of human, share, or computer elements. The collection process can be run across entire networks and filters can be applied to either include or exclude specific types of data. Data collection can be scheduled and managed through an intuitive "dashboard." In addition to collection and processing of data, a reporting function allows for relevant information output in a compact, usable format.

AccessData Enterprise

AD Enterprise is an investigative solution geared toward large-scale investigative processes. While AD eDiscovery is geared toward collection and reporting of information, AD Enterprise can additionally respond to incidents as they occur. Solution highlights include:

- Live memory searching
- Integrated incident response console
- Process kill capability
- Viewing of static and volatile data within same interface
- Rapid analysis of thousands of machines, proactively or reactively
- Single click acquisition of hard drives, RAM and volatile data
- Market-leading decryption, password recovery and cracking
- Distributed processing, allowing quick processing of large amounts of data

FTK Imager

FTK Imager is Access Data's evidence acquisition tool. It is used to quickly preview and create a forensically sound image of the disk if the preview warrants such action. "It makes a bit-by-bit duplicate of the media, rendering a forensic image identical in every way to the original, including file slack, and unallocated and free drive space."

Imager allows for the preview and imaging of local hard drives, network drives, floppy disks, ZIP disks, CDs, DVDs, memory cards, USB storage devices, and other devices. It also allows for the preview of previously created images in a variety of image formats. When an image is created, Imager creates and verifies hashes for both the original drive and the image in order to prove the integrity of the case evidence. Additionally, files and folders can be exported from images, and hash reports for regular files can be generated.

Forensic Toolkit (FTK)

FTK is used to filter, analyze, investigate, and report on acquired evidence. It "provides users with the ability to perform complete and thorough computer forensic examinations. FTK features powerful file filtering and search functionality. FTK customized filters allow you to sort through thousands of files so you can quickly find the evidence you need. FTK is recognized as the leading forensic tool for performing email analysis." Additionally, FTK provides bookmarking, reporting, decryption, and password cracking; all within a customizable, user-friendly interface. A closer look will be taken at FTK and its functions during the analysis phase of this project.

Labs

While FTK by itself is able to harness the processing power of up to four machines or "workers" from one centralized workstation, its functionality can be expanded for use in larger, multiple-person labs. Figure 4 shows the functionality of the two lab expansions available.

WHICH SOLUTION IS RIGHT FOR YOU?

FUNCTIONALITY	FTK	AD LAB LITE	AD LAB
Distributed Processing	4 WORKERS	EXPANDED	UNLIMITED
Share a Central Database Infrastructure	NO	NO	YES
Investigator Collaboration	NO	UNLIMITED	UNLIMITED
Case and Task Management	NO	YES	YES
Role-based Permissions to Control Access & Activity	NO	YES AT THE CASE LEVEL	YES AT THE DATA LEVEL
Web Review & Analysis	NO	NO	UNLIMITED

Figure 4
Source: http://www.accessdata.com/lab.html

Mobile Phone Examiner
This program actually reads and images data from cell phones and cell phone data card readers. "It can be run as a standalone program or, as an add-on to FTK. When run as a standalone program, it reads and images the data. You would then add the image file to a case in FTK. When installed on a machine that also has FTK installed, the phone or device can be detected when adding new evidence, and the data, when imaged, is automatically added to the current FTK case."

Registry Viewer
This tool allows you to view the contents of Windows operating system registry files on the imaged drive, including files in the registry's protected storage that are not accessible with Windows Registry Editor. Protected storage contains such items as usernames and passwords. Registry viewer will be looked at more closely in the analysis phase of this project.

SilentRunner Sentinel
SilentRunner is "a passive network monitoring solution that visualizes network activity by creating a dynamic picture of communication flow, swiftly uncovering break-in attempt, weaknesses, abnormal usage, policy violation and misuse, and anomalies – before, during and after an incident." Its features include:

- Real-time network capture and visualization
- Pattern and content analysis
- Forensic analysis and on-demand incident playback

Password Recovery and Decryption
Access Data provides two programs for use in recovering passwords and keys for decryption; Password Recovery Toolkit (PRTK) and Distributed Network Attack (DNA). Both programs perform the same function, but DNA uses the processing power of machines across a network to help in the recovery effort. PRTK is limited to the

processing power of the machine that it is installed on. "Both programs analyze file signatures to find encryption types and determine which recovery module to use."

Methods such as decryption and dictionary attacks are used to recover passwords. Various included dictionaries, as well as custom user dictionaries, can be used in recovery efforts.

In addition to password recovery, both programs perform file hashing. Each file is hashed when added to the program for recovery. It is hashed again when the password is recovered. This verifies that the file has not been altered during the recovery process.

Once passwords are recovered, these passwords can be entered into FTK. This may prove useful in decrypting some of the files that FTK determined were encrypted. Keep in mind that, in order to be opened, some files require that the program used to create it be used to open it. At the very least, a viewer for that file type will be needed. If the program or viewer is not available on the machine being used, the file can be exported out for viewing on another machine.

Portable Office Rainbow Tables (PORT) and Rainbow Tables (pre-computed brute-force attacks) are add-ons that can significantly reduce the amount of time needed to recover passwords. While PORT are in fact portable, fitting on a single DVD, Rainbow tables will cost you quite a bit in terms of space - 3 TB per table.

PRTK will be used in the analysis phase of this project.

Student Version

Licensing options for Access Data's tools vary by the type of institution and its intended use of the products. A USB "CodeMeter" is used to store licensing information and is required for full functionality of the tools for which licenses were purchased. Previous version of FTK allowed limited processing (5000 files) without a license dongle. FTK 3.0 does not offer this limited functionality. Included in the student version that I will be using are FTK Imager, FTK, and PRTK.

The Project

As stated in the Introduction, the purpose of this project is to show what Access Data has to offer in terms of tools for forensic analysis of digital evidence. The various products were discussed, but the best way show their value is by putting them to the test. I will accomplish this by fabricating evidence for three different cases, using three different laptops. I will also attempt to hide some of the evidence using various techniques such as deletion, encryption, and steganography.

Once the evidence has been planted, I will image the hard drives using FTK Imager and analyze the images using FTK. PRTK will also be used in an attempt to break passwords and recover encryption keys in some of the cases. I will provide screenshots of my

findings along the way, in order for readers to get a closer look at Access Data's products in action. Finally, I will report my findings using FTK's reporting tool.

The goal is to come up with three hard drive images that can be used in the MSIS Computer Forensic class. The images should be usable with a variety of computer forensics software, not FTK exclusively. Students will be presented with a case background and a hard drive image, and will be expected to find any evidence that may point to the guilt or innocence of the suspects involved.

Background

In an attempt to show how FTK performs under realistic circumstances, I will plant evidence that is similar to that which was recovered in actual cases. While it would be easy to plant an abundance of evidence, realistically, there generally is not a lot of evidence found in a single case. In most cases, digital evidence does not provide law enforcement with the "smoking gun." More often it provides evidence that supports a particular theory. With that in mind, let the games begin!

Case # 1 – Murder

Reference Case: In July 2009, Steven Zirko was found guilty in the murders of his ex-girlfriend, Mary Lacey, and her mother, Margaret Ballog. There was a long history of domestic violence between Zirko and Lacey, but no physical evidence linking him to the murders.

Zirko and Lacey were together from 1997 to 2003. They had two children together. Zirko was a professional piano player but was unemployed at the time of the murders. He was previously employed as a piano player on a cruise ship. Job history after that is sketchy. Apparently, after years of domestic problems, the couple split up. The children went to live with Lacey. According to testimony, Zirko had anger management issues and became enraged when Lacey allegedly refused to let him see his children. On the witness stand, Zirko's chiropractor testified that Zirko had asked if him if he knew anyone that he could hire to kill Lacey. In the end, apparently Zirko gave up the idea of trying to hire a hit man and decided to do the job himself. It was also theorized that Zirko may have killed Lacey in order to collect on the $500,000 life insurance policy he had on her.

The Chicago RCFL (Regional Computer Forensics Laboratory) provided critical digital evidence that helped convict Steven Zirko. When they examined Zirko's computer, they found Internet search histories that included terms such as "GHB," a known date-rape drug, "hire a hitman," and "hire a mercenary." Additionally, Lacey had recently moved, and investigators found MapQuest directions from Zirko's house to Lacey's and from Zirko's current girlfriend's house to Lacey's house. It is believed that Zirko used his girlfriend's Jeep when he drove to Lacey's to commit the murders. Examiners also found that Zirko checked his children's school schedules online, presumably to make sure they were not going to be home at the time of the murders. As for Lacey's mother, it is believed that she was just in the wrong place at the wrong time. [35, 36]

Fabricated Case: The suspect, Steve Zippo, will have the same history; former cruise ship piano player, currently unemployed, with an ex-girlfriend who will not let him see his children. The same type of evidence will appear on my suspect's computer. Additionally, in order to show some history, there will be emails between Zippo and Laney (the victim) concerning refusal of child visitation. There will also be addresses in Zippo's address book so the driving direction lookups can be referenced to something.

Case details that will be given to students: Steven Zippo, a former cruise ship piano player, is charged with murdering Mary Laney, his ex-live-in-girlfriend, in her home.

Zippo and Laney have two children together, both students at Lewis Yew Elementary. The former couple has a long history of domestic violence. The police were called to their home on numerous occasions during the years they were together. Family members state that Laney was forced to change residences several times in fear for her safety. Additionally, two witnesses told police that Zippo had approached them about "hiring a hit man to kill the mother of his children."

Zippo's current girlfriend, Nell Phillips, claims that Zippo was helping her paint her house at the time of the murder. However, a credit card receipt and security footage show that Zippo was purchasing gas approximately two hours before the murder.

While the history of domestic violence and witness testimony seem to implicate Zippo as the likely murderer, police lack any physical evidence. You are charged with the task of examining Zippo's computer in an attempt to find evidence that may support or refute witness testimony

Case # 2 – Stealing Company Secrets

Reference case: Sergey Alenyikov was indicted on charges that he stole proprietary computer code from his former employer, Goldman Sachs.

According to the indictment, filed on February 11, 2010, Alenyikov worked for Goldman Sachs from May 2007 to June of 2009. During that time he was responsible for developing programs supporting the high-frequency trading platform which generates millions of dollars per year in profits for the firm.

Alenyikov resigned in April of 2009 and accepted a position at Tezra Technologies. He was hired to develop Tezra's own version of the computer platform. On Alenyikov's last day working for Goldman Sachs, he transferred large portions of computer code from his work computer to a server in Germany. Before transferring the code, he encrypted the contents and subsequently uninstalled the encryption program.

Additionally, during the years that Alenyikov worked for Goldman Sachs, he transferred, without authorization, thousands of computer code files related to the trading program. He did this by sending the files from his work email account to his personal email account. He also stored versions of the code files on his home computer, laptop, a flash drive, and other storage devices. Alenyikov was arrested at an airport in Chicago. At the

time of arrest, he had the laptop and another storage device containing the stolen code in his possession. [33]

Fabricated Case: The idea will be to create the same kind of evidence scenario, not necessarily the same type of evidence. Rather than computer code, my suspect, Sergio Natooslik, is going to steal secret recipes and not-yet-released menus from the catering company that he works for.

Case details that will be given to students: Goldmoon Saques is a small, upscale catering business that provides fine, exotic cuisine for small events. It is well known to the locals that the quality and taste of Goldmoon Saques's food is consistent due to strict adherence to their top-secret recipes. The business does quite well and is always fully booked well into any given year. Employees are required to sign a confidentiality agreement, stating that they will not discuss or otherwise provide any information concerning Goldmoon Saques's recipes to anyone outside of company for any reason.

Sergio Natooslik worked for Goldmoon Saques Catering from May 2008 until April 2010. After resigning, Natooslik opened up his own catering business on the other side of town. It is believed that Natooslik stole secret recipes from Goldmoon Saques before he left, in order to help assure the success of his own business. Additionally, he may have stolen the customer list in an attempt to lure some of Goldmoon Saques's customers away.

Case # 3 – Wasting Time on the Company's Dime

Reference Case: CCL Forensics, a company that provides digital forensic and e-discovery services, was asked to investigate the computers of a number of employees in the IT department. Due to lack to lack of productivity in that department, it was suspected that the employees were wasting time by visiting auction and social networking sites during working hours.

Paying particular attention to internet history and chat logs, CCL found that, not only were the employees wasting time on social sites, but they were also selling both personal and company-owned items on various auction sites. The employees were suspended, and after further investigation, permanently dismissed. [34]

Fabricated Case: My suspect, Lewis Capstone, will leave the same type of evidence. Email, Internet history, and documents on his computer will show that he spends entirely too much time goofing off at work. Additionally, there will be evidence that he is most likely selling items that the company keeps in storage.

Case details that will be given to students: Lewis Capstone works as a tech in the IT department of Lion's Legal, a large law firm in town. Lion's Legal has a strict policy prohibiting Internet use for anything but company business during work hours. During a quarterly employee review, management notices that Lewis is not as productive as his co-workers in the same department. Lewis's attendance is not an issue; in fact, he is often in the office long after his co-workers have gone home for the day. Management suspects that Lewis is spending his work time performing unrelated activities. Since Lewis's

performance is substandard, his extended work hours are suspect as well. Before any accusations are made, it is decided that the first course of action should be to check his computer for unauthorized use. On a Sunday night when the office is closed, management has Lewis's hard drive imaged and sent for analysis.

Preparation and Imaging

Before I begin, I'd like to thank Dr. Faisal Abdullah, Dr. Ray Klump, and Joseph Ninh for providing me with the direction and resources needed to complete this project. I could not have done it without their assistance. Gentlemen, thank you for your support.

Computers used to plant evidence: Three Dell Latitude D620 laptops, each with an 80 GB hard drive running Windows XP Professional.

As described in the case listings above, one case at a time, evidence was created on each of the three laptops. Of course, there is always a glitch or two that needs to be dealt with and there was no exception in this case. Much of the evidence, such as email, was created ahead of time so all the dates would not be identical. Unfortunately, I gave one of the suspects a Yahoo Mail account. In order for FTK to identify and process email, it has to be retrieved using an email client such as Outlook or Outlook Express. Unless the account is a premium (paid) account, Yahoo Mail cannot be retrieved using an email client.

Due to time constraints, there was not a lot that could be done to rectify the situation. A new Hotmail account was created for the suspect and all mail that existed in the Yahoo account had to be copied and sent through the new Hotmail account. What this meant for the case was that all email in that account would now be dated the same. Additionally, random emails, such as newsletter subscriptions used to create non-evidence filler email, could not be copied or forwarded. While this is not tragic for the case, it does make it less believable.

The next glitch to be dealt with: Due to unforeseen circumstances, the write blocker was unavailable for use at the time of imaging. Since these cases will not be used in a court of law, this was not a deal breaker. Instead, the images were created by downloading FTK Imager (version 2.6.1.6.2) to the laptop in use and imaging it from within the same drive. While the images created will show the download and installation of FTK Imager, this does nothing to affect the evidence planted.

Thankfully, these were the only problems that we encountered during the process. With that said, we begin with a look at FTK Imager. The interface is simple and intuitive. In order to create an image, simply select "Create Disk Image." (See figures 6-10) A source type is then chosen and other selections made from available choices. For this project, "Physical Drive" was chosen. Various information concerning image type and case details are added and the image is created. Time required to create an image varies with the size or capacity of the source being imaged, and the power of the equipment used for imaging. For this project, image creation took approximately 2 hours per 80 GB hard drive.

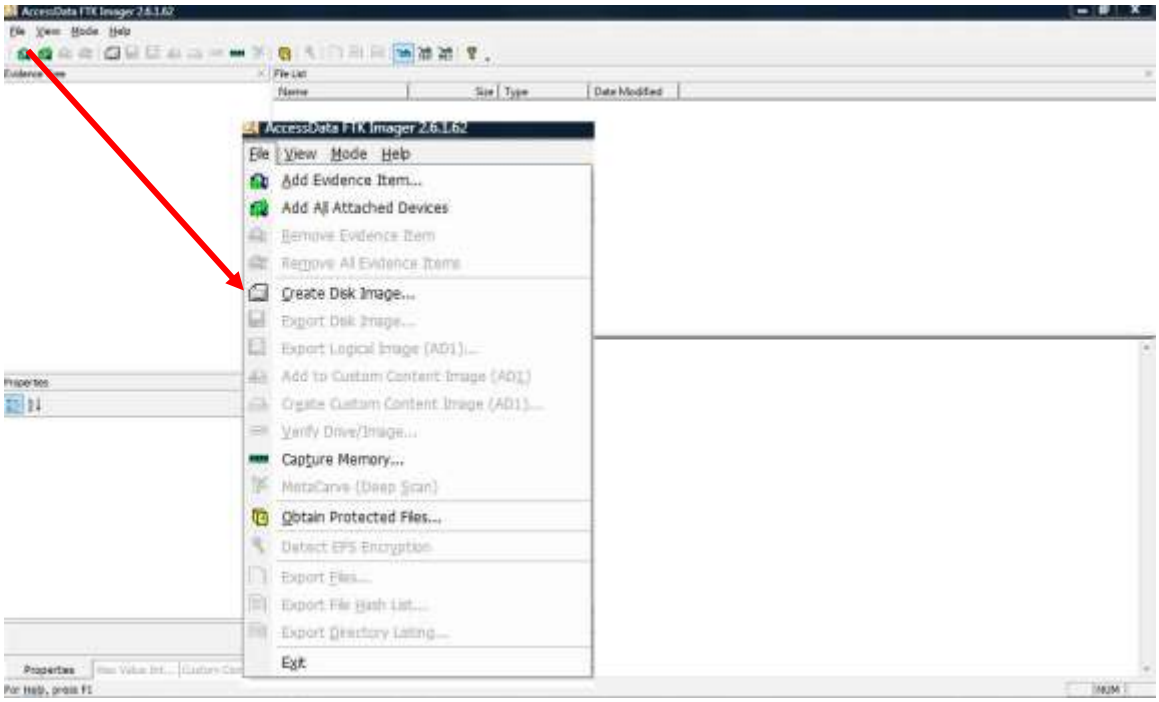


Figure 6 – Creating a disk image

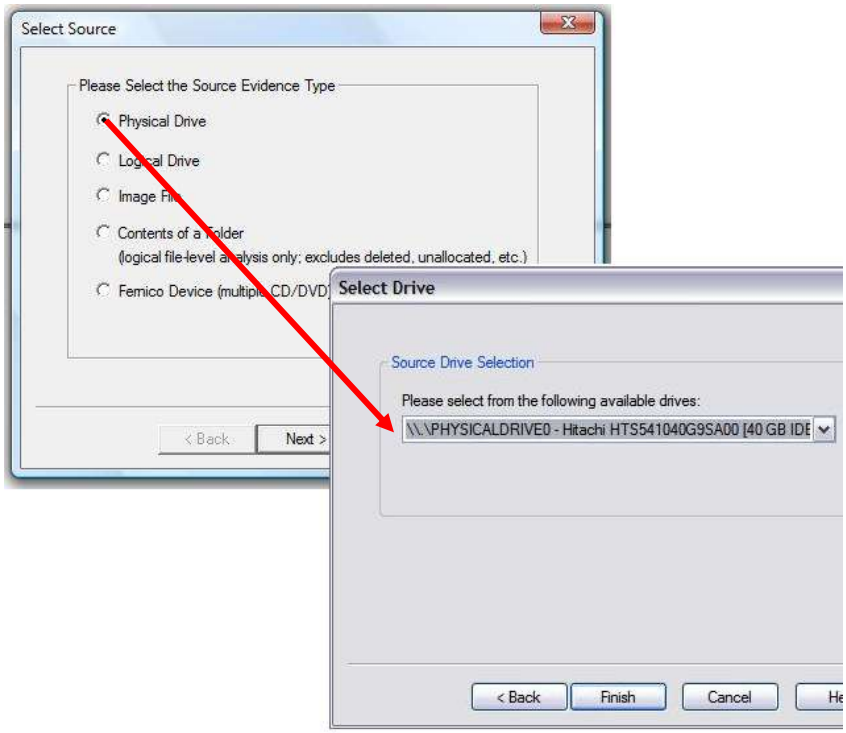


Figure 7 – Image source selection

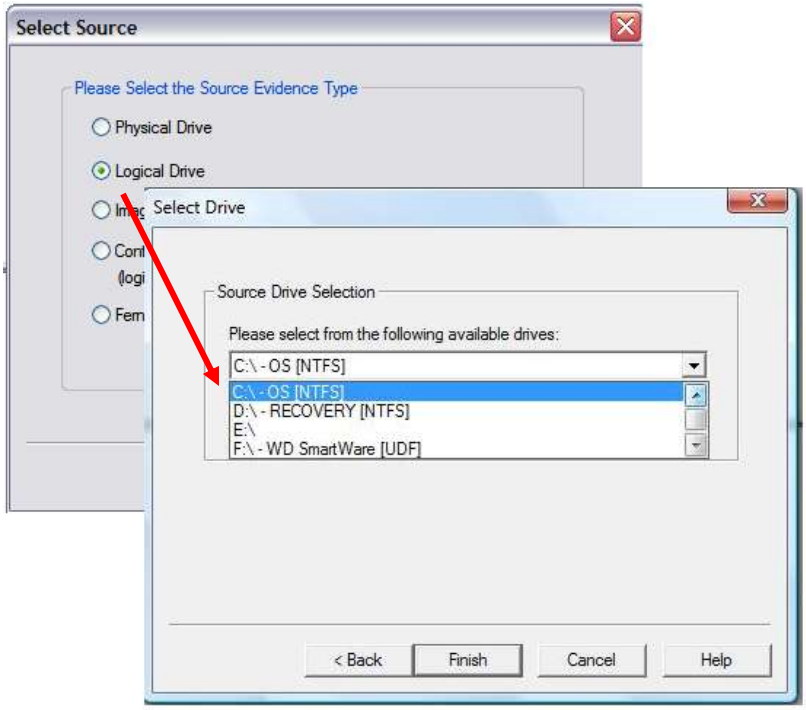


Figure 8 – Image source selection

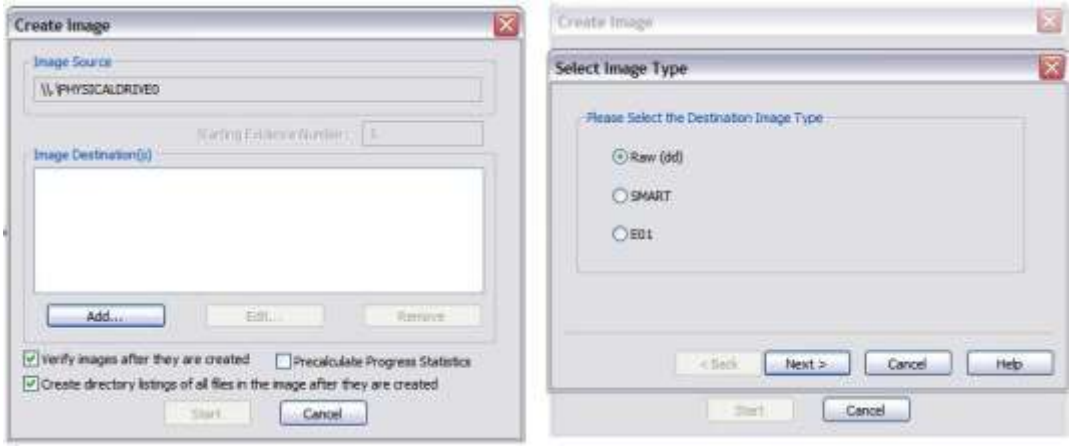


Figure 9 – Selecting output image type

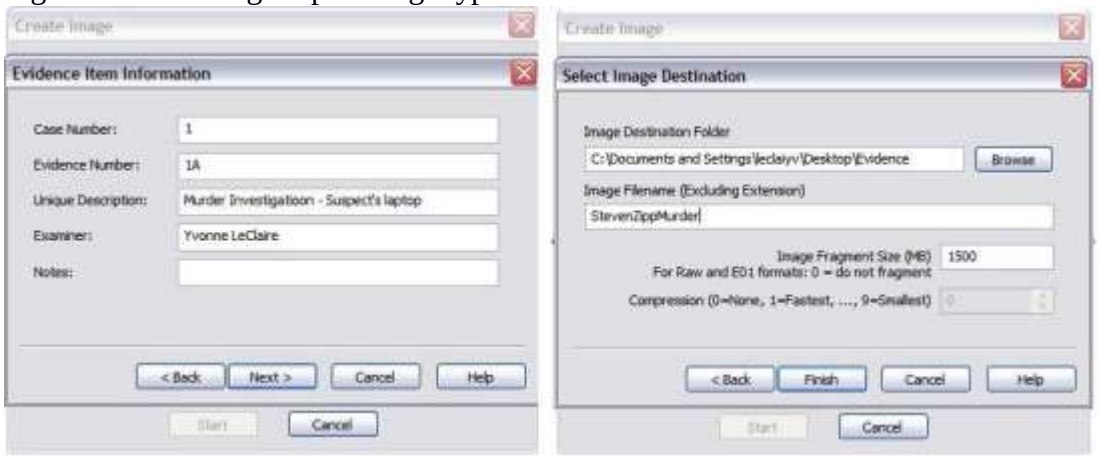


Figure 10 – Selecting the details

While it may sometimes be necessary to fragment images, it is important to note that, depending on the image type you choose to create, fragmenting should be avoided in some cases. The E01 image type is an Encase Forensic Image File. If you choose to fragment this image type, each file is given a consecutive number (i.e. E01, E02, E03, etc.). FTK recognizes E01 as a valid image file and can be loaded into the program. However, all remaining files are not recognized and cannot be loaded into the program. These image files would be usable in Encase, but not FTK. Of course, I found this out the hard way. After making this discovery, all images for this project were created in the Raw format and were not fragmented.

After the image is created its integrity is verified. The hash values of the source and the image are compared and the results shown. Once the image is loaded into FTK Imager, other functions can be performed such as, reviewing the contents of the image, exporting the image or individual files out for further analysis in other utilities, creating custom content images, or exporting hash lists.

Case Creation

The first step in the analysis process is case creation. In this phase various options are chosen, depending on your plan of action for processing the case. If time constraints pose a problem, it is possible to create a case but leave some of the more time consuming tasks for additional analysis at a later time. As with the imaging process, case creation time varies with both the size of the image(s) to be processed, and the processing power behind the machine(s) being used for analysis. Each case can contain multiple images or, evidence items. For this project, one image was used per case. Case creation took an average of eight hours per case.

Rather than go through all options available in FTK, which is a book all in itself, I will discuss those that concern the three cases being analyzed here. This should give a sufficient view of the tool and its usefulness in forensic analysis of digital evidence.

During case creation, one of the options that I chose in all three cases was dtSearch Text Indexing. All text in the case file is indexed, thus greatly reducing search and retrieval time when sifting through large amounts of data.

Another option I chose in one of the cases was data carving. Basically, data carving is the partial or total recreation of a deleted or altered file, derived from file structure, header, and footer information. The time needed for data carving in a case can be substantial. Since I knew the type of information I would find in each case, in order to save time, I only performed data carving on the case in which the suspect deliberately hid or deleted data. No additional information would have been gained were I to data carve in the other two cases. In an actual investigation, if time allows, it is generally a good idea to check the data carving option.

The Analysis: FTK in Action

Once the case is loaded into FTK, the following opening screen appears:

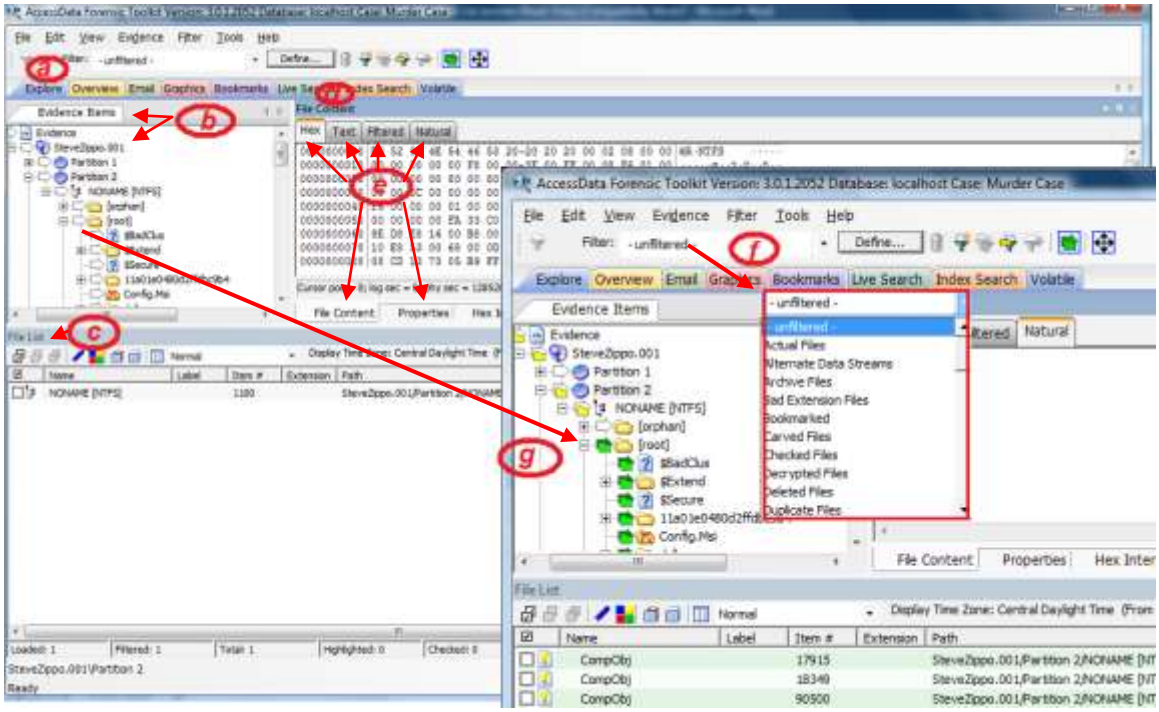


Figure 10 – FTK Explore tab view

Note the various panes, tabs, and menus. The case is first viewed from the Explore tab (a). The image file is listed in the upper left Evidence Items pane (b). Depending on the tab in use, the default panes vary. All panes can be rearranged to suit the examiner's needs. Additionally panes can either float or remain docked. The floating feature can be very useful when viewing larger files or scanning a large number of graphics files.

From the Explore tab, the directory structure can be viewed. For any item chosen, the file list for that specific item can be viewed in the lower File pane (c). For any file chosen in the File pane, its content and properties can be viewed in the upper right File Content pane (d). Note the various tab options in the File Content pane (e). File content can be viewed in hex, text, filtered, or natural states by clicking on the corresponding tabs in the upper File Content pane.

Various filters (f) can be applied to limit the files types that appear in the File List pane. Specific folders and subfolders can be included or excluded from a file listing by clicking on the arrow icon to the left of each item in the directory tree (f). Additionally, individual items in the file list can be check-marked for further action such as exporting or bookmarking.

Unless the examiner knows specifically what he is looking for and where it can be found, the Explore tab view can be a bit overwhelming. The remaining tab views are a little less daunting as they are more specific. Very briefly, The Overview tab gives the examiner a breakdown by file type, category, and status (Figure 11). The Email (Figure 12) and Graphics (Figure 13) tabs show precisely what their names imply. The Bookmarks tab is for viewing items that the examiner bookmarks for further analysis or for possible

inclusion in case reports. The Live Search and Index Search tabs are used for performing the respective search types. Live searches are useful for pattern searches such as, searching for phone numbers, credit card numbers, or social security numbers. The Volatile tab is for importing and examining volatile data files, such as RAM dumps.

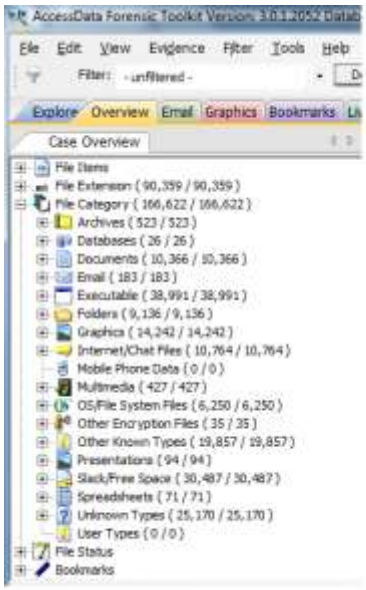


Figure 11 – Overview Tab

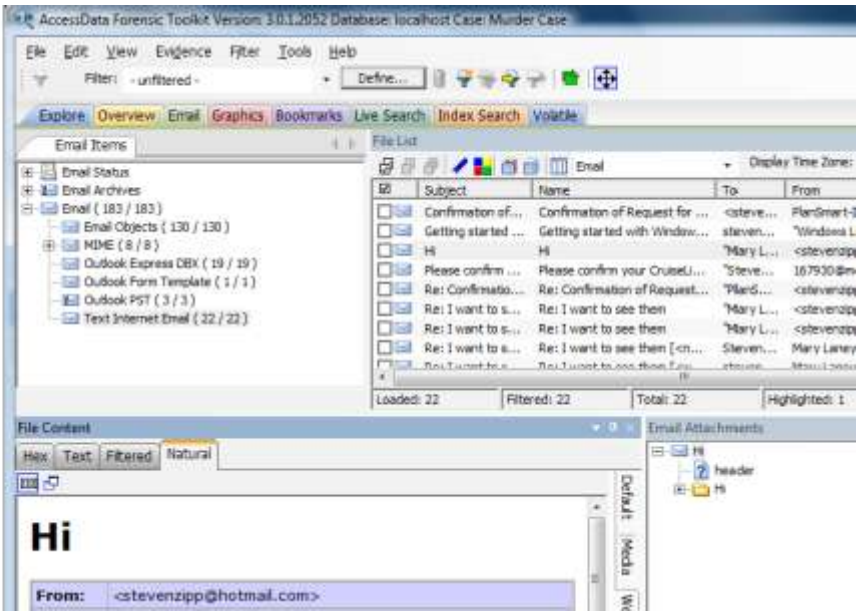


Figure 12 – Email Tab

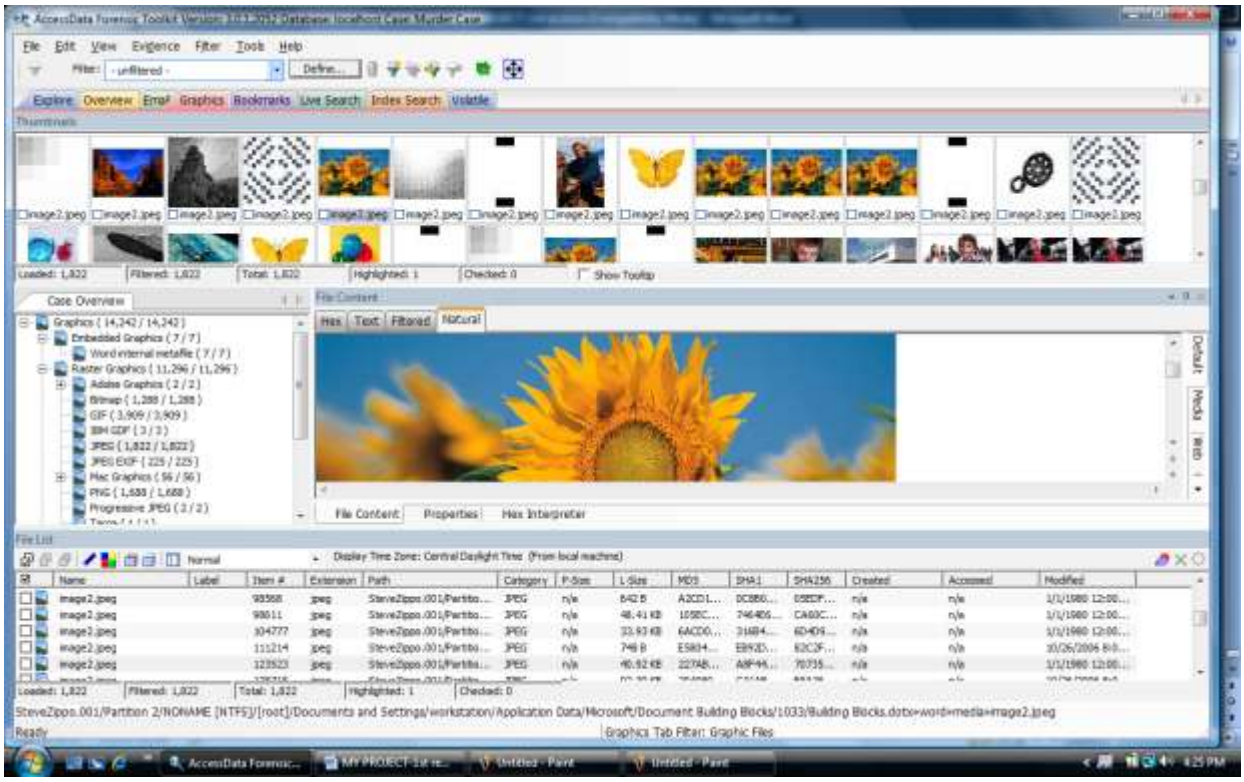


Figure 13 – Graphics Tab

While this is certainly not a detailed explanation of FTK's features, it is enough information with which to get started with evidence analysis.

Case #1 - Murder

Armed with the image and case history given earlier, students will be looking for evidence that Steven Zippo murdered his ex-girlfriend, Mary Laney. Since this is a murder case, a good place to start would be email (Recall case type/evidence type matrix.). From the Email tab in FTK, a number of emails both to and from Mary Laney are found.

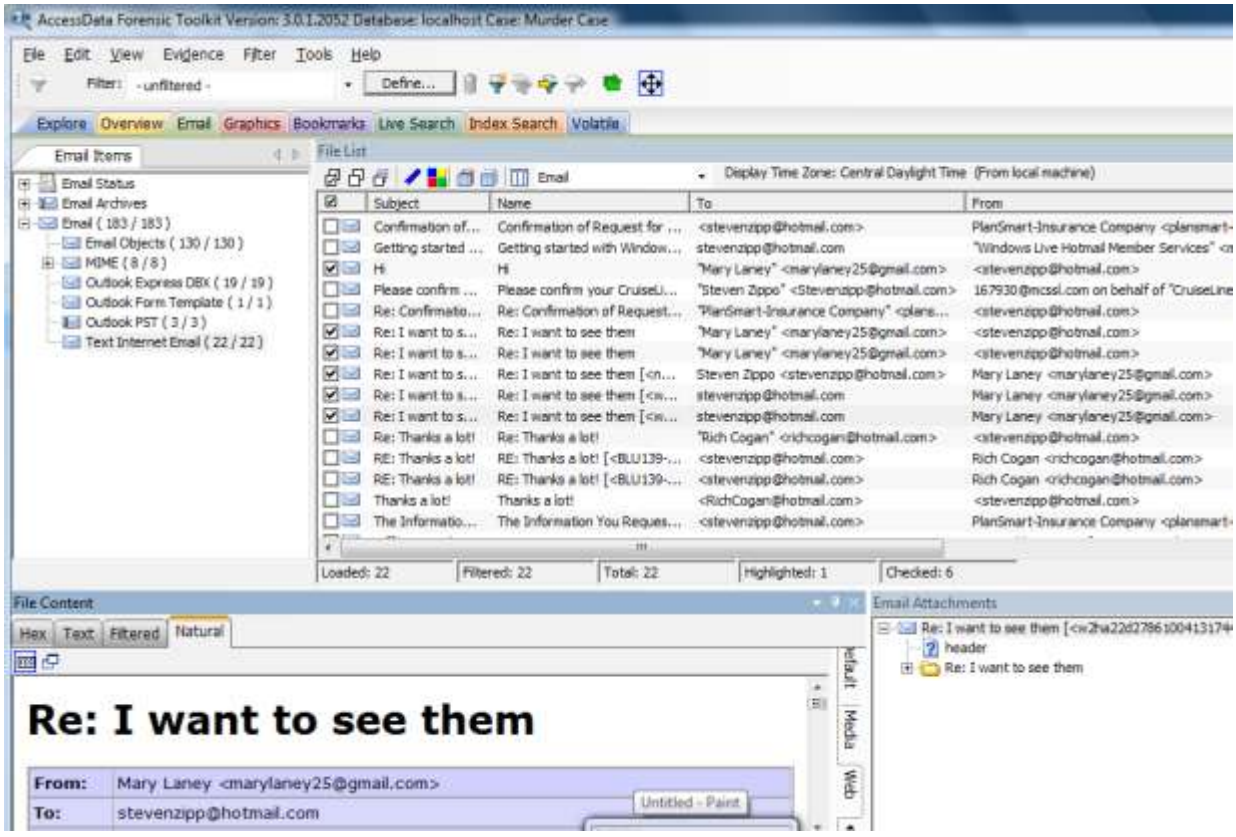
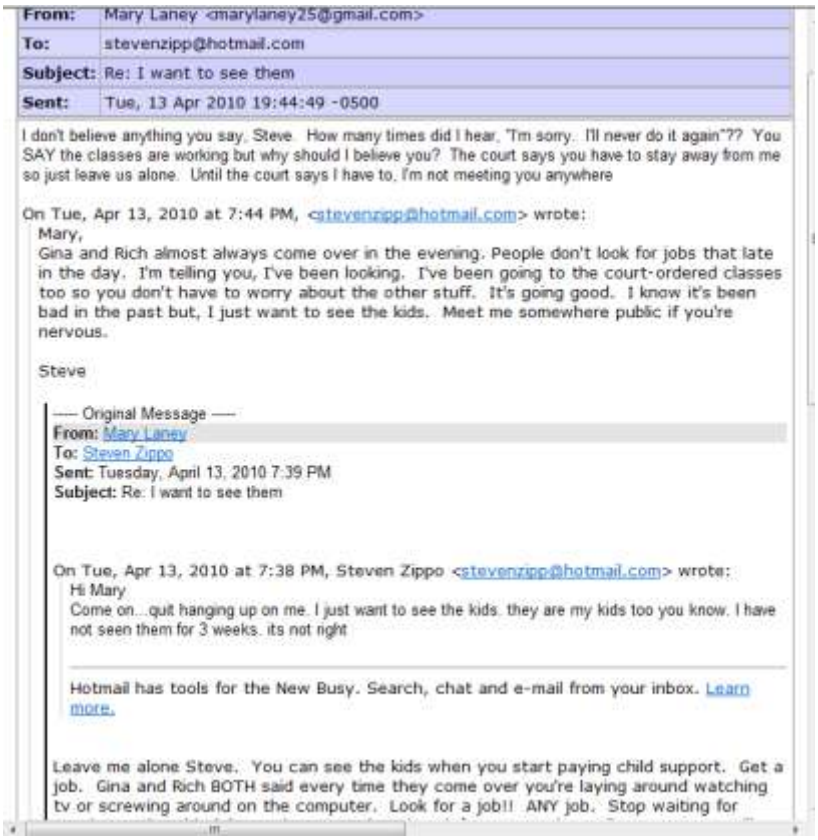


Figure 14 – Emails between Zippo and Laney

When viewing these items, it becomes apparent that there is friction between Zippo and Laney. He wants to see his children and she is denying him. There is also reference to possible past domestic violence (Figure 15). The items are checked and bookmarked (Figure 16) for inclusion in the case report. Once an item is bookmarked, its color in the list is changed. This is helpful in terms of organization and preventing duplicate entries.

In an email to his friend, Rich Cogan, reference is made to Zippo's current girlfriend, Nell Phillips. Additionally, there are two emails from an insurance agent. It seems that Zippo was inquiring about an insurance policy that he has kept on Laney since 1995 (Figure 17). These emails are checked and bookmarked as well. Things are beginning to look a little dismal for Zippo at this point.



From:	Mary Laney <marylaney25@gmail.com>
To:	stevenzipp@hotmail.com
Subject:	Re: I want to see them
Sent:	Tue, 13 Apr 2010 19:44:49 -0500

I don't believe anything you say, Steve. How many times did I hear, "I'm sorry. I'll never do it again"?? You SAY the classes are working but why should I believe you? The court says you have to stay away from me so just leave us alone. Until the court says I have to, I'm not meeting you anywhere

On Tue, Apr 13, 2010 at 7:44 PM, <stevenzipp@hotmail.com> wrote:

Mary,
Gina and Rich almost always come over in the evening. People don't look for jobs that late in the day. I'm telling you, I've been looking. I've been going to the court-ordered classes too so you don't have to worry about the other stuff. It's going good. I know it's been bad in the past but, I just want to see the kids. Meet me somewhere public if you're nervous.

Steve

---- Original Message ----
From: Mary Laney
To: Steven Zippo
Sent: Tuesday, April 13, 2010 7:39 PM
Subject: Re: I want to see them

On Tue, Apr 13, 2010 at 7:38 PM, Steven Zippo <stevenzipp@hotmail.com> wrote:

Hi Mary
Come on...quit hanging up on me. I just want to see the kids. they are my kids too you know. I have not seen them for 3 weeks. its not right

Hotmail has tools for the New Busy. Search, chat and e-mail from your inbox. Learn more.

Leave me alone Steve. You can see the kids when you start paying child support. Get a job. Gina and Rich BOTH said every time they come over you're laying around watching tv or screwing around on the computer. Look for a job!! ANY job. Stop waiting for

Figure 15 – Email between Zippo and Laney

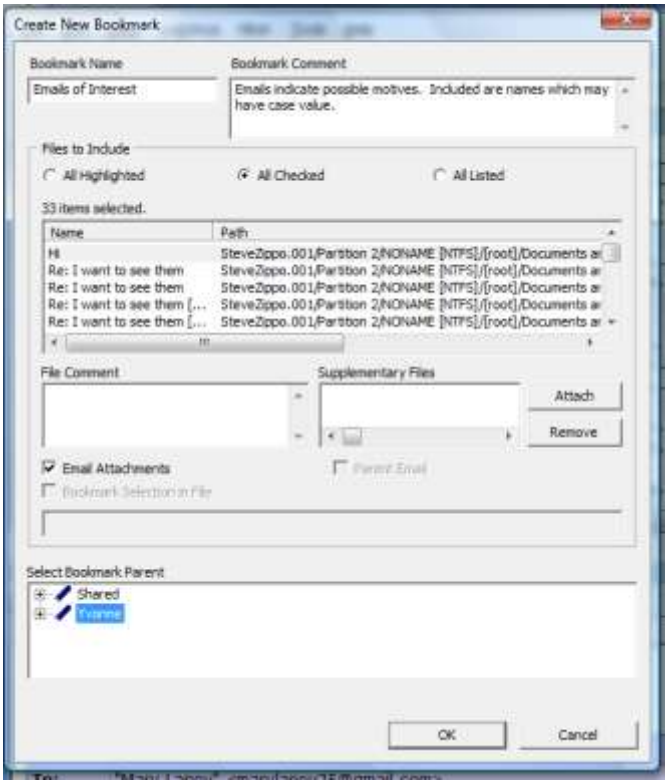


Figure 16 – Creating bookmarks

Figure 16 – Email from insurance agent

With no other items of interest in email, other areas can be explored. Names often prove useful in an indexed search. When a search for "Mary Laney" is performed, results are produced which include entries in Zippo's address book (Figure17).

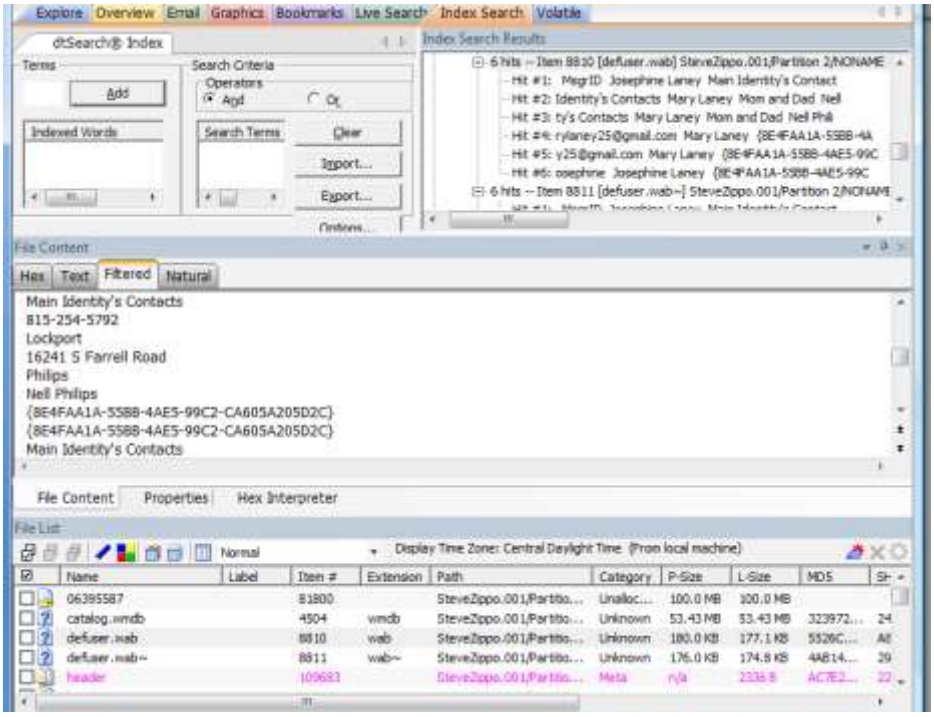


Figure 17 – Address book entries

Additionally, there is an indication that driving directions from Zippo's girlfriend's house to Laney's house were looked up on Google Maps (Figure 18) and saved to the Desktop. There are multiple indications that the file was saved to the Desktop, but the file was deleted and the Recycle Bin was emptied. Data carving was not performed in this case so FTK did not attempt to reconstruct the file. While the file no longer exists on the desktop, evidence of the direction lookup still exists.

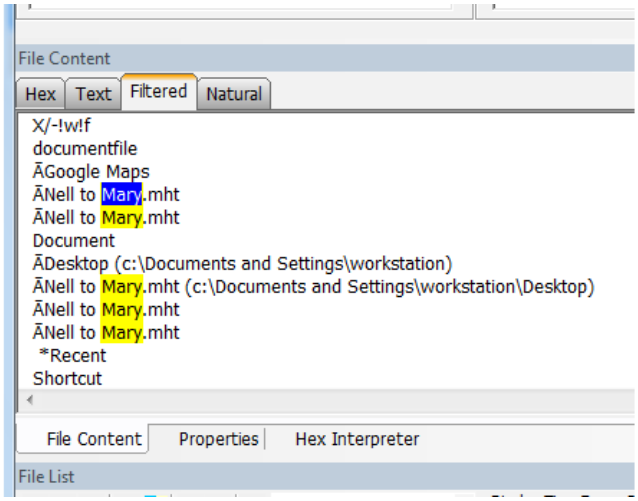


Figure 18 – Google Maps lookup

Back on the Explore tab, a look at the Temporary Internet Files confirms that Google Maps was used for directions from Nell Phillips house to Mary Laney's, and also from Zippo's house to Laney's (Figure 19).

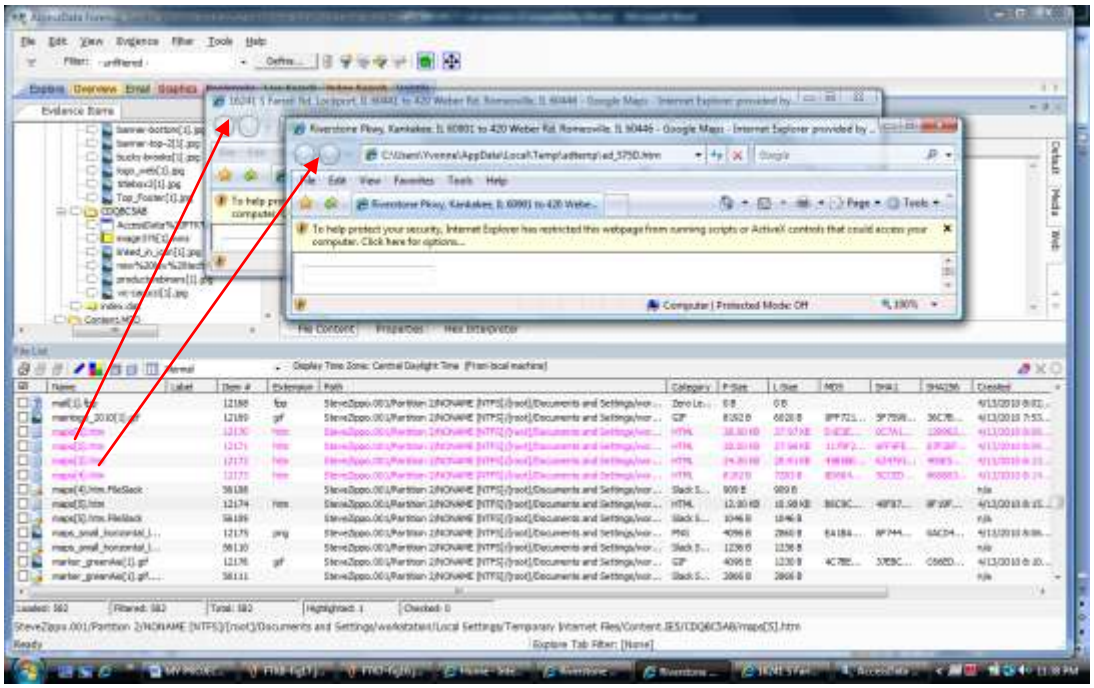


Figure 19 – Temporary Internet Files showing direction lookup

Another place that often yields useful information is the My Document's folder. In this case, the folder contains some random piano related documents. Recall that Zippo was previously employed as a piano player on a cruise ship. Additionally, there are a few documents pertaining to child custody matters. These will be bookmarked as they may point to motive. Finally, there is a resume for Zippo. While this may not be important to the case itself, it gives the students a reference for the previous Google Maps lookup. Phillips and Laney's addresses were referenced through Zippo's address book entries.

Additional information from the case details may prove useful when looking for evidence. Laney was murdered while her children were at school. The children attended Lewis Yew Elementary. Returning to the Index Search tab, a search for Lewis Yew Elementary yields some interesting results. The search results show that Zippo looked up his children's schedule online. While this may seem unimportant, it might also be used as evidence that Zippo was making sure his children would not be home at the time of the murder.

More concretely, included in one of the hits on the school search is a Bing search history. The history includes the items "GHB," "murder for hire," and "hire a hitman." Recall the case details. Two witnesses claimed that Zippo asked them about hiring someone to kill Laney. The recovered search terms might be used to aid in improving the credibility of the witnesses. At this point, the bookmarked files can be used to create a case report.

As previously stated, digital evidence rarely provides the "smoking gun." There is no conclusive evidence in this case. However, there is evidence that seems to support a theory; the theory that Steven Zippo murdered Mary Laney. Two possible motives that this case supports are rage at being kept from his children, and money; quite possibly both.

Knowing the evidence ahead of time certainly shortens the hunt. Students my travel down other roads before finding the evidence presented here. There is also ample opportunity to use Access Data's Registry Viewer. While Zippo did not specifically hide any of the evidence, students can still use Registry Viewer to uncover his passwords for various user accounts and to access other protected Registry files. Registry viewer will be covered in the third case.

Case 2 – Stealing Company Secrets

Sergio Natooslik is charged with stealing secret recipes and customer lists from his former employer, Goldmoon Saques. Students will be looking for any evidence that recipes or customer lists have "left the building" so to speak, as this action is strictly forbidden.

Once again, a good starting point is email. When viewing Natooslik's company email account, everything in the Inbox seems routine. However, there are a number of suspicious deleted emails that include attachments. The attachments are (distorted) pictures of flowers and trees. The emails appear to have been sent to Natooslik's personal email account (Figure 20).

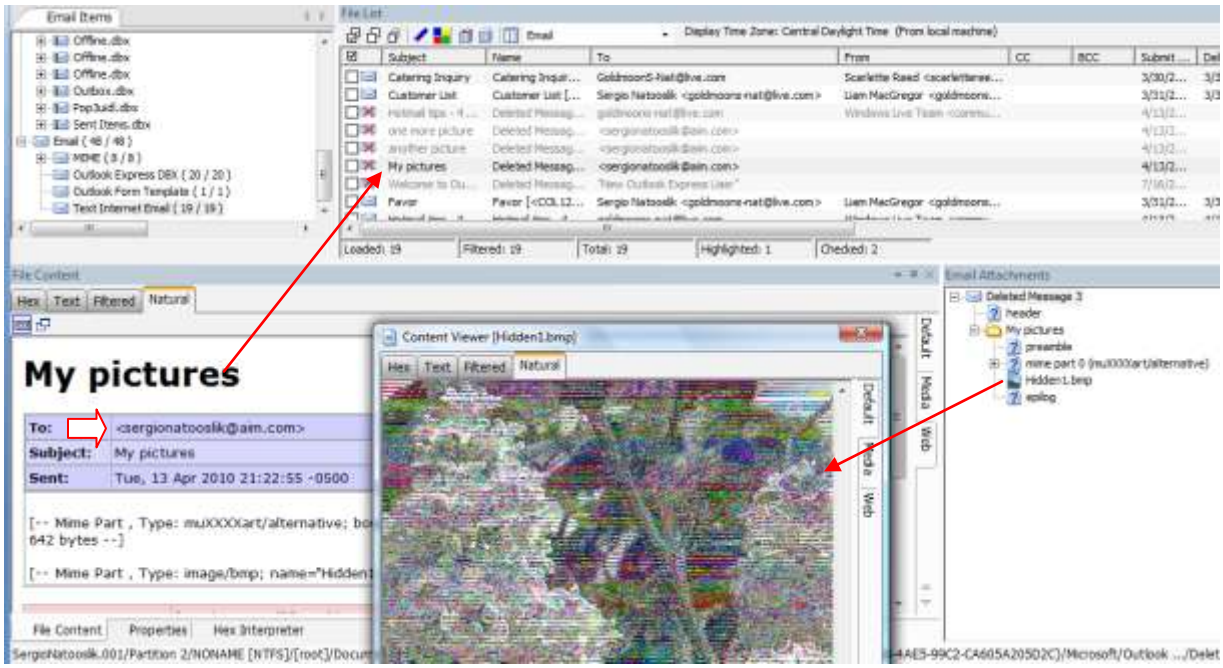


Figure 20 – Natooslik's deleted email

The fact the there is no text included in the deleted messages is suspicious in itself. The inclusion of nature photographs seems even more puzzling. These suspicious emails should be checked and bookmarked for inclusion in the report.

Since the emails were deleted and the Deleted folder was emptied, FTK had to carve the picture files in order to add them to the case. Unfortunately, during the carving process, the image files were altered which accounts for the distortion. In their original state, the pictures were crystal clear. There were actually recipe files hidden inside of them with a steganography program. Since the images were altered during carving, the steganography program can no longer retrieve the files hidden inside the pictures.

My hope was that the students would see the out-of-place nature pictures and immediately think 'steganography'. While there is no steganography program installed on Natooslik's computer, a look into the registry with Registry Viewer would show that a steganography program was installed and uninstalled from his machine. I chose a free steganography program so, after making the discovery, students could download and install it. After running the pictures through the program, the hidden recipe files would have been revealed; an exciting idea but a failed attempt. Score one for Natooslik.

Moving on to another area, Natooslik has a large number of files in his My Documents folder. Most of them are recipe files and are marked as confidential (Figure 21). Does Natooslik have authorization to have these files on his computer? We are not given this information. Therefore, the files should be bookmarked and added to the case report.

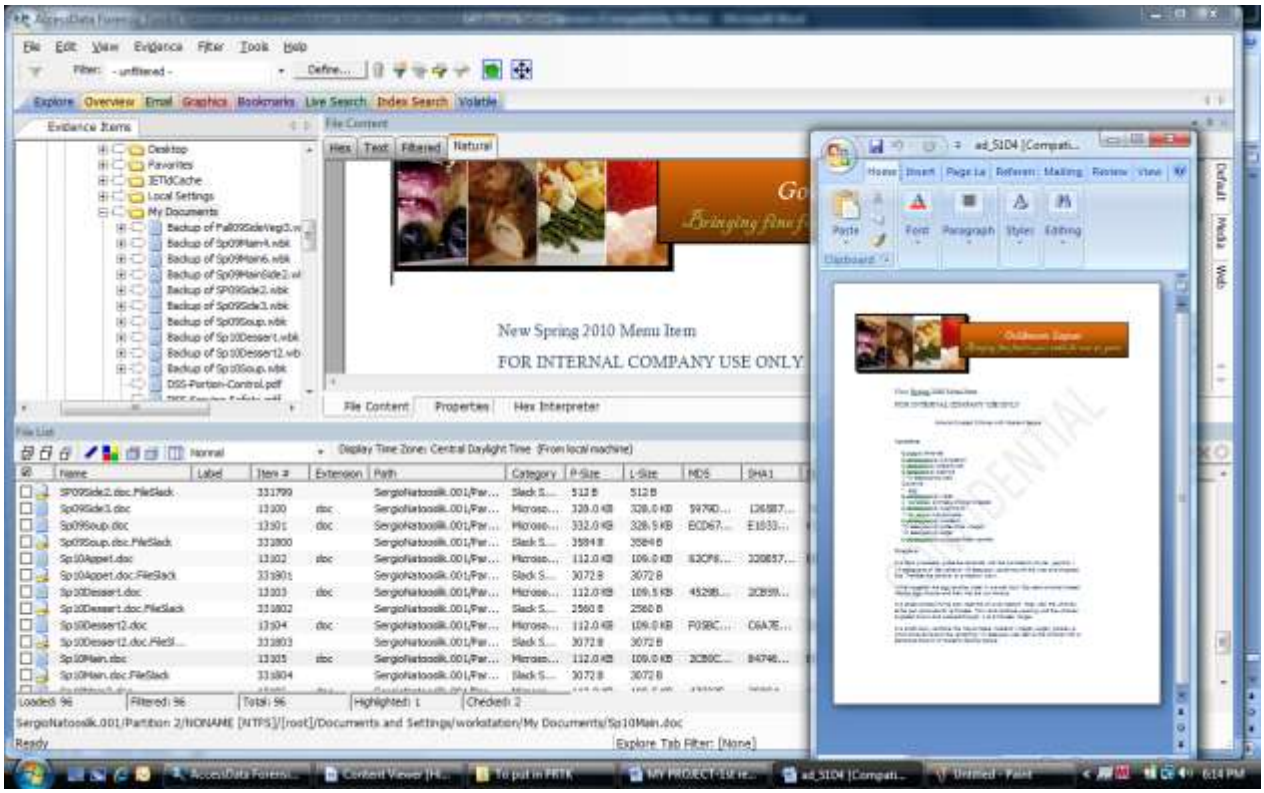


Figure 21 – Recipes in My Documents folder

Additionally, some of the files are password protected. Password protected/encrypted files appear in red. In order to view the contents, the files must be exported out and run through PRTK (Figure 22).

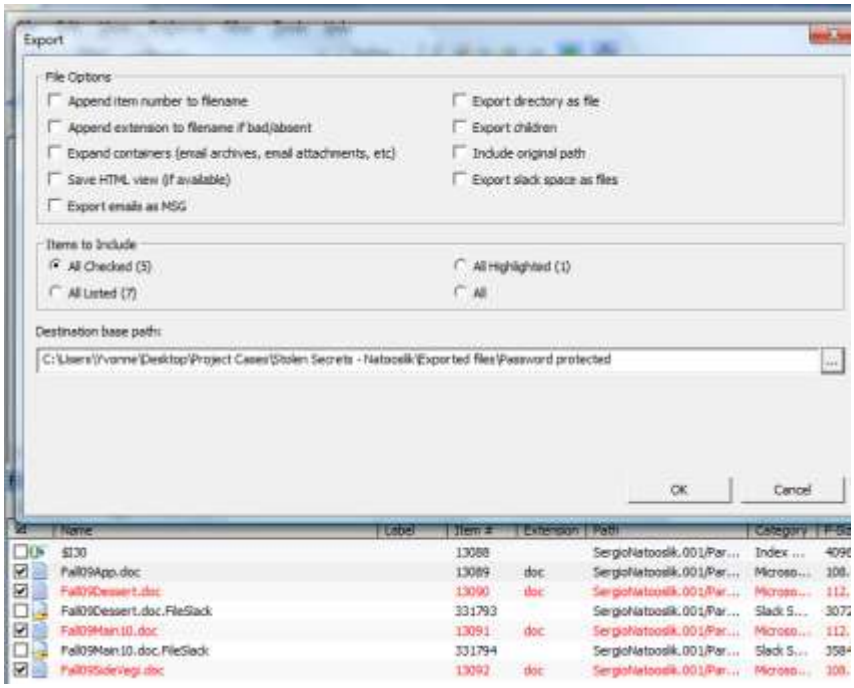


Figure 22 – Check files, right click and select Export

Once the files have been loaded, PRTK examines them and determines what needs to be done. In this case, the files were password protected with Microsoft Word. PRTK chooses the types of attacks to use in order to break the passwords (Figure 23). PRTK also allows the use of custom dictionaries for attacking passwords. Custom dictionaries can be created from sources such as word lists exported from FTK or Registry Viewer. Dictionaries can also be created from user-entered information such as the suspect's birth date or other personal information that is known.

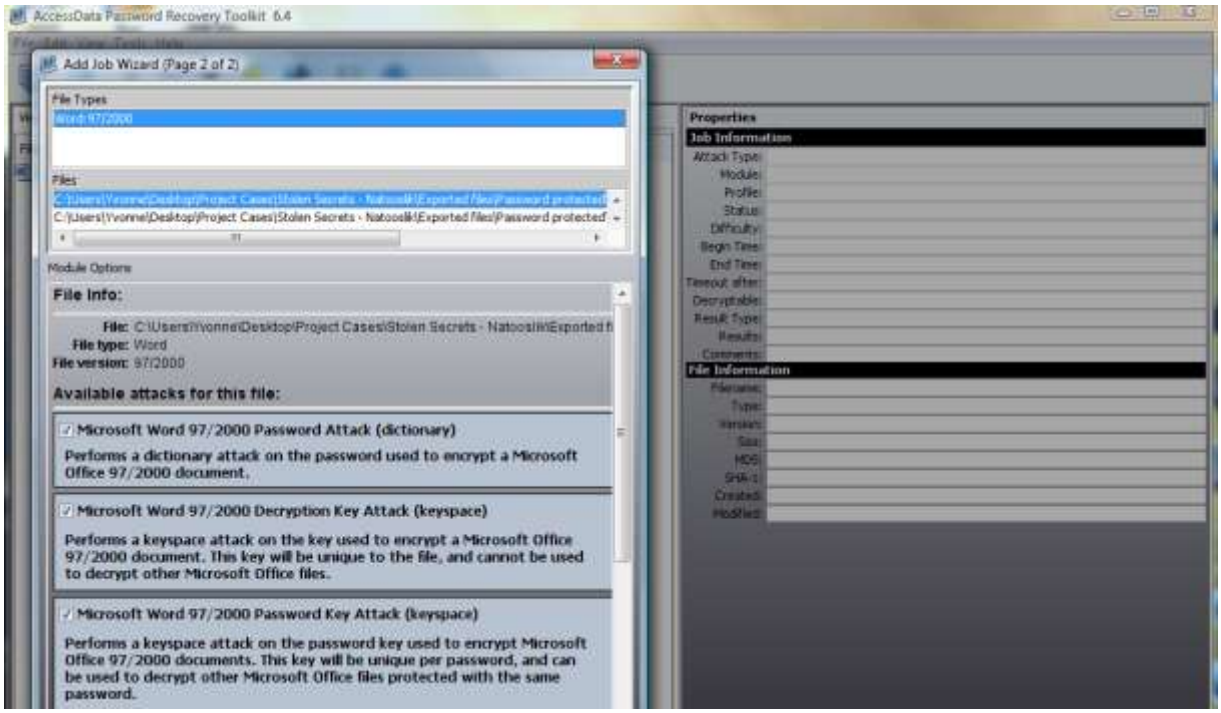


Figure 23 – PRTK chooses password attacks

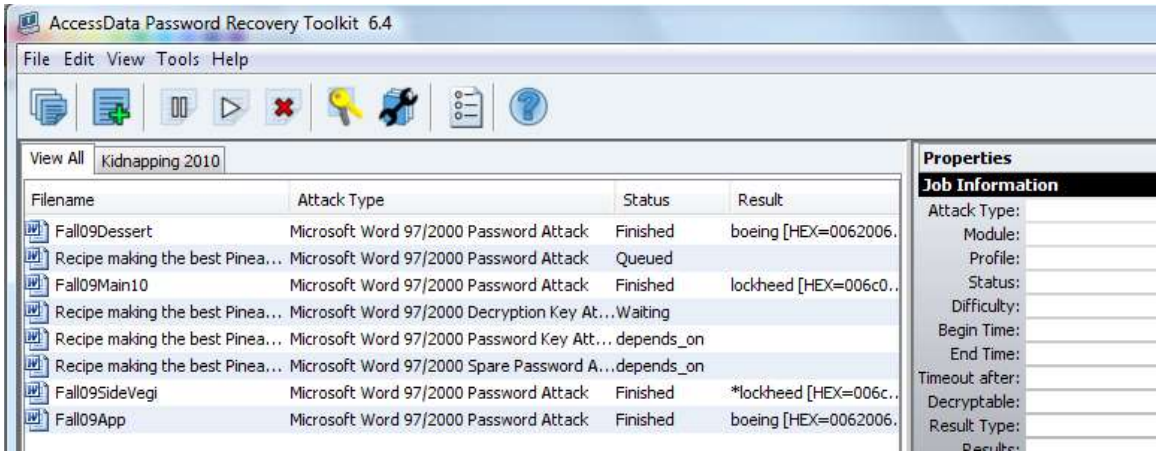


Figure 24 – PRTK in action

Once the passwords have been broken they can be put into FTK and used to open the password protected files. Once decrypted, the files will show up in the Overview tab under Decrypted Files (Figure 25). As suspected, the password protected files in this case were recipe files.

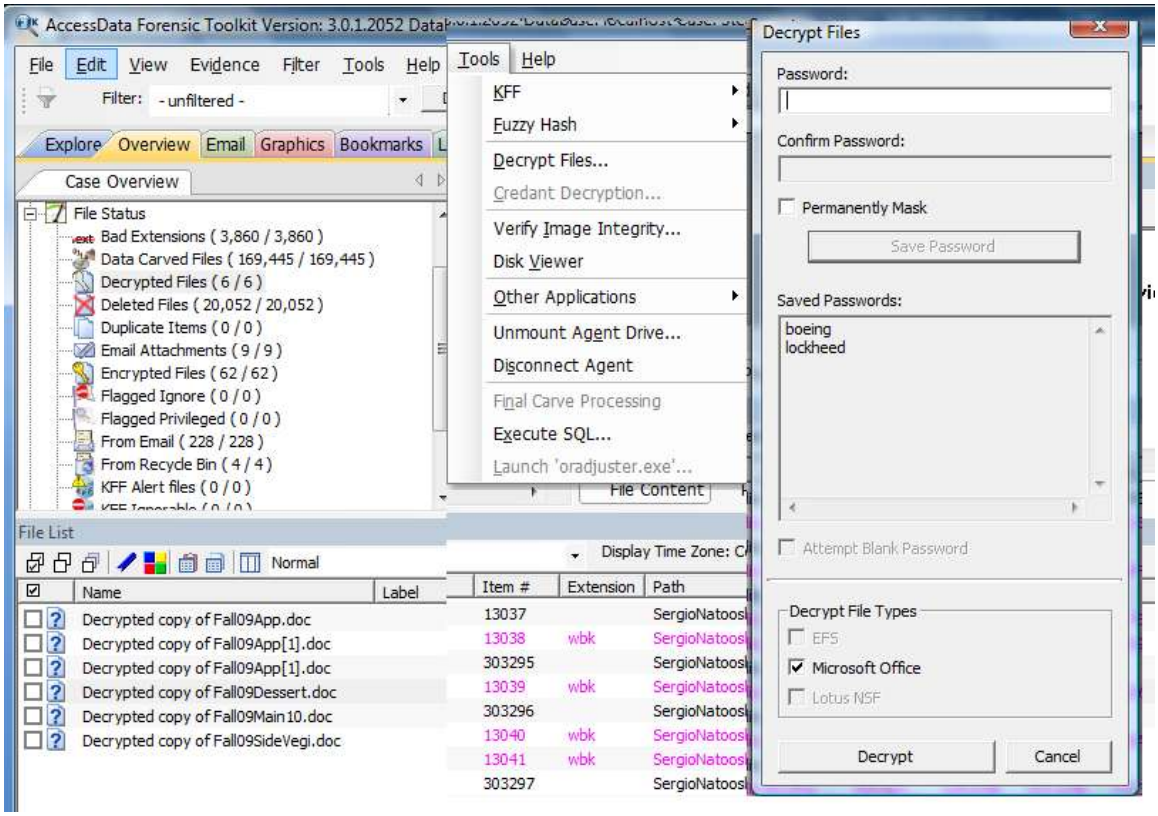


Figure 25 – Enter discovered passwords into FTK and select Decrypt.

A look at the Encrypted Files in the Overview tab reveals that there are 62 encrypted files. Most, given their location, are system or program files. Some are in unallocated space. Others have already been identified in this case. There are two files that stick out in the list. They look like copies of encrypted files from My Documents. What is interesting is their location. They are in Temporary Internet Files.

Upon navigating to the actual location of one of the files (Explore tab), another interesting item is found. In addition to the two encrypted recipe files, a document concerning a small business loan approval for Natooslik is found. It also seems that something is afoot with the Goldmoon Saques Client list. A look at the inex.dat file for IE5 history shows that Natooslik had apparently uploaded some recipe files and the client list to Megaupload.com (Figure 26).

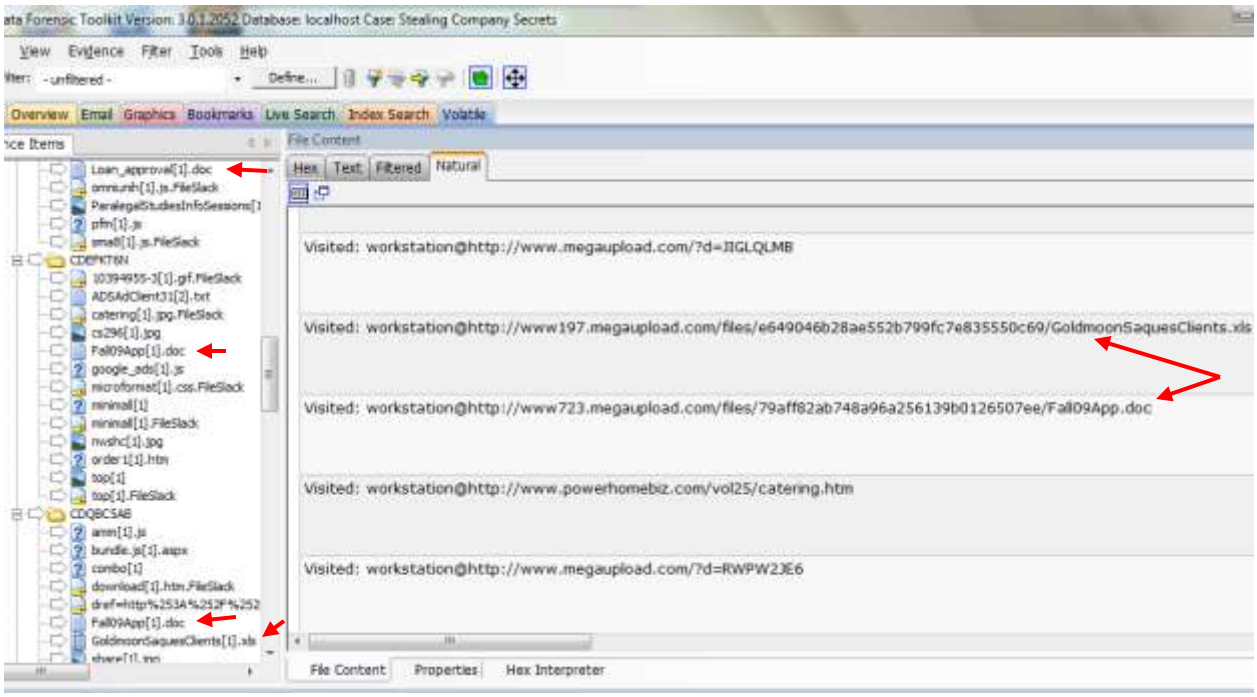


Figure 26 – Suspicious files in Temporary Internet Files and IE5 History index.dat file

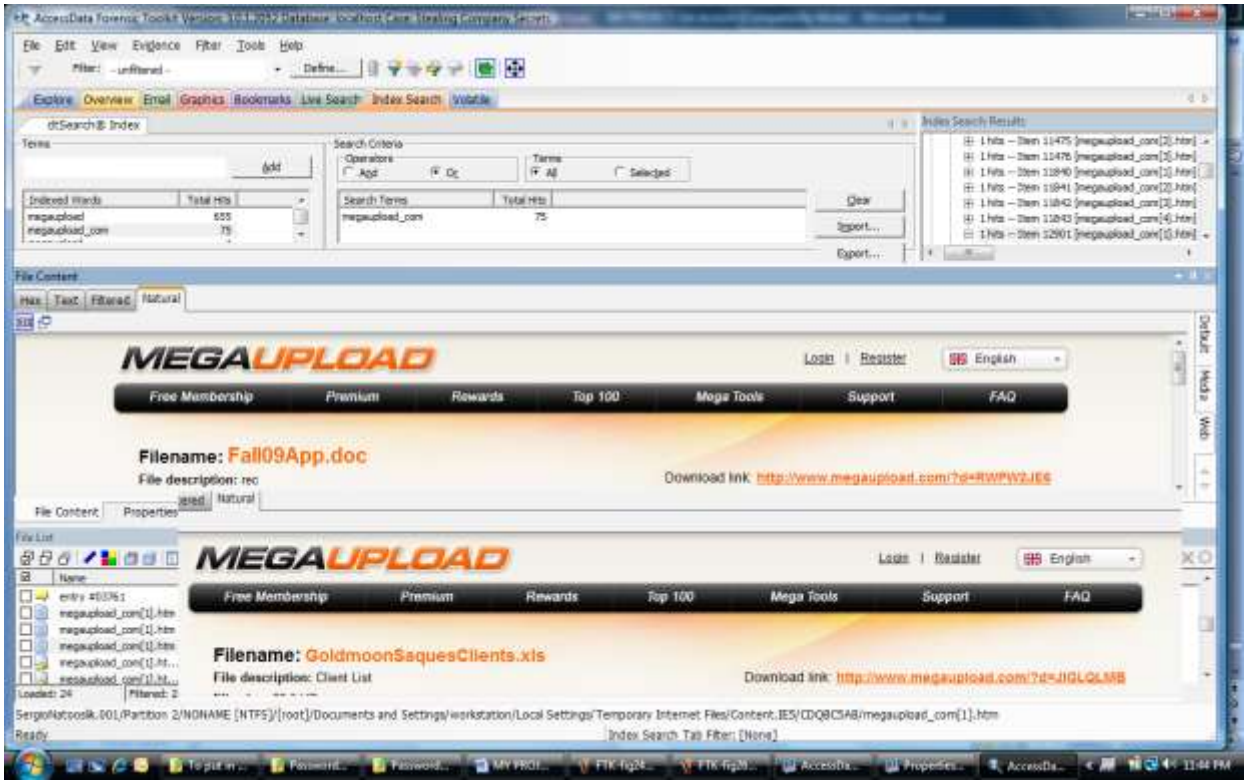


Figure 27 – Uploaded protected company files

A dtSearch of megaupload confirms that the files were uploaded to the site (Figure 27). The confidentially agreement that Natooslik signed when he was hired strictly prohibits actions such as this. It seems that Natooslik's goose is cooked.

Case 3 – Wasting Time on the Company's Dime

Lion's Legal suspects that Lewis Capstone is spending his work time on unrelated activities. Company policy restricts the use of computer equipment and Internet connections to work-related activities.

Even at first glance, it is obvious that Capstone is misusing company resources. While his work email account is used strictly for legitimate business, there is another account that has been accessed from his work computer. This seems to be a personal email account. His work account was being accessed with Outlook Express while he used Outlook for his personal account retrieval (Figure 28). Strike one for Capstone.

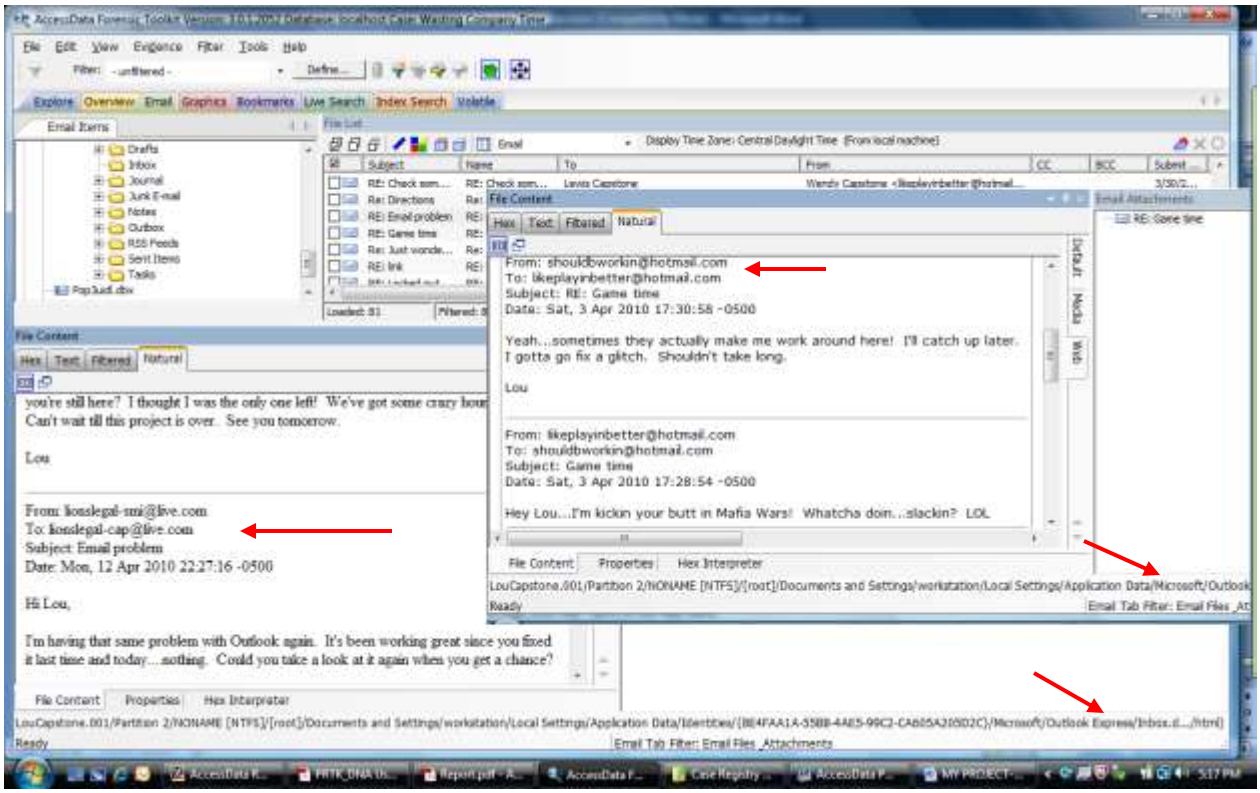


Figure 28 – Email from business and personal accounts

The emails in Capstone's personal account indicate that he likes to play computer games…a lot. There are multiple subscriptions to online game accounts, subscriptions to auction sites, game posts from facebook, and multiple emails indicating that he plays online games while he is at work. Of course, email boasts concerning work-time game playing are not concrete proof that the activities actually took place. Further examination will be necessary.

Before leaving the Email tab, another noteworthy item is discovered. In an email to his wife (Wendy), Capstone mentions an eBay account and a list of items for sale. The text indicates that something suspicious is going on concerning the items for sale (Figure 29). A document search may prove useful in shedding some light on the subject.

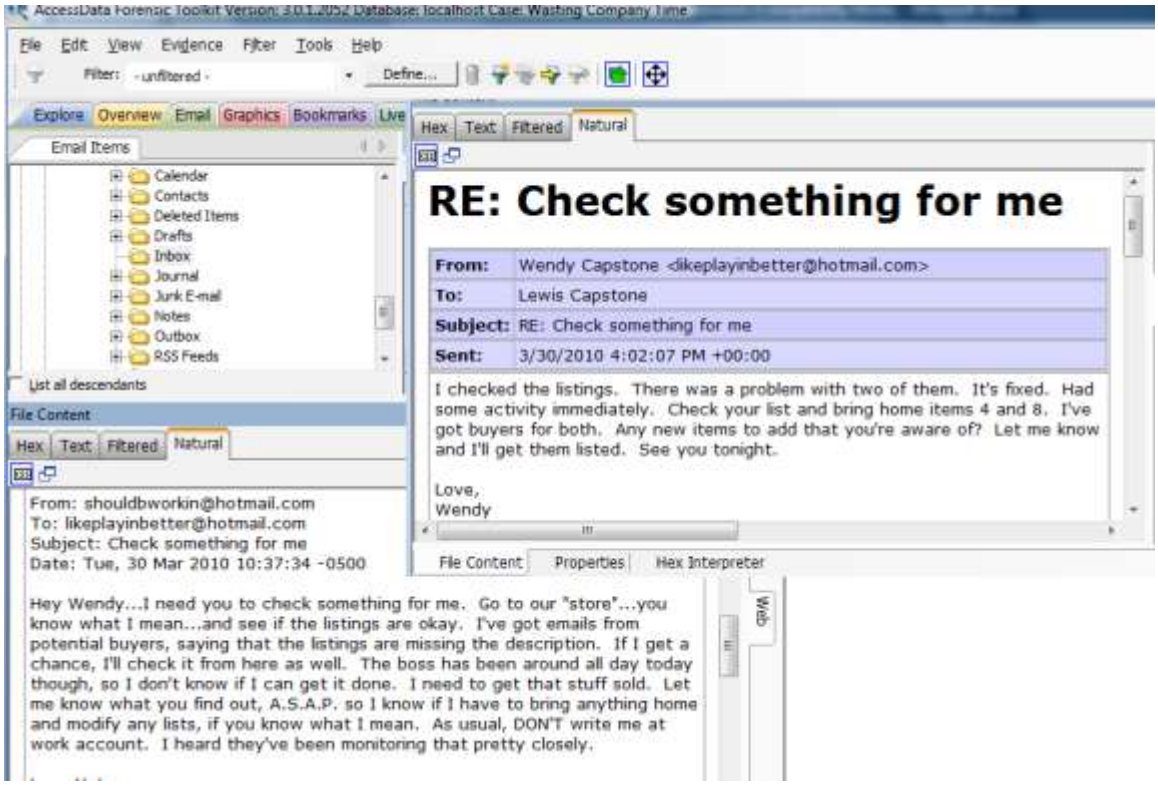


Figure 29 – Suspicious email

In the previous case, the Explore tab was used to view Internet usage information. The same can be done in this case. A look at the index.dat file for Internet Explorer history shows that Capstone regularly accessed unapproved sites. Note that Capstone even added personal and gaming sites to his Favorites (Figure 30). Strike two for Capstone.

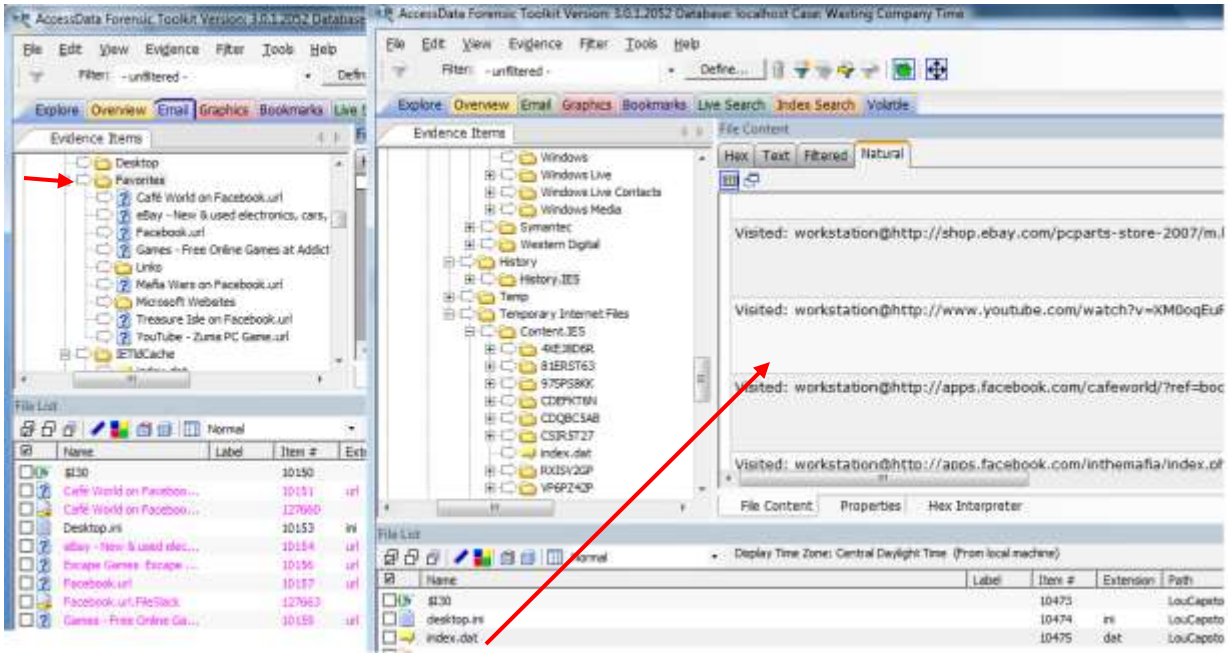


Figure 30 – Favorites and Internet Explorer History listing

The index.dat file can also be used in a password recovery process in PRTK. First, a look at some of the Registry files associated with the password recovery process.

To recover a Windows XP login password, the SAM file and System file are exported out and added to a PRTK job. An easy way to locate these files without recalling their exact location is through the Overview tab. Open the OS/File System Files category and click on Windows NT Registry. The alphabetical list of the contents appears in the File List pane. The files can be highlighted and exported from here (Figure 31).

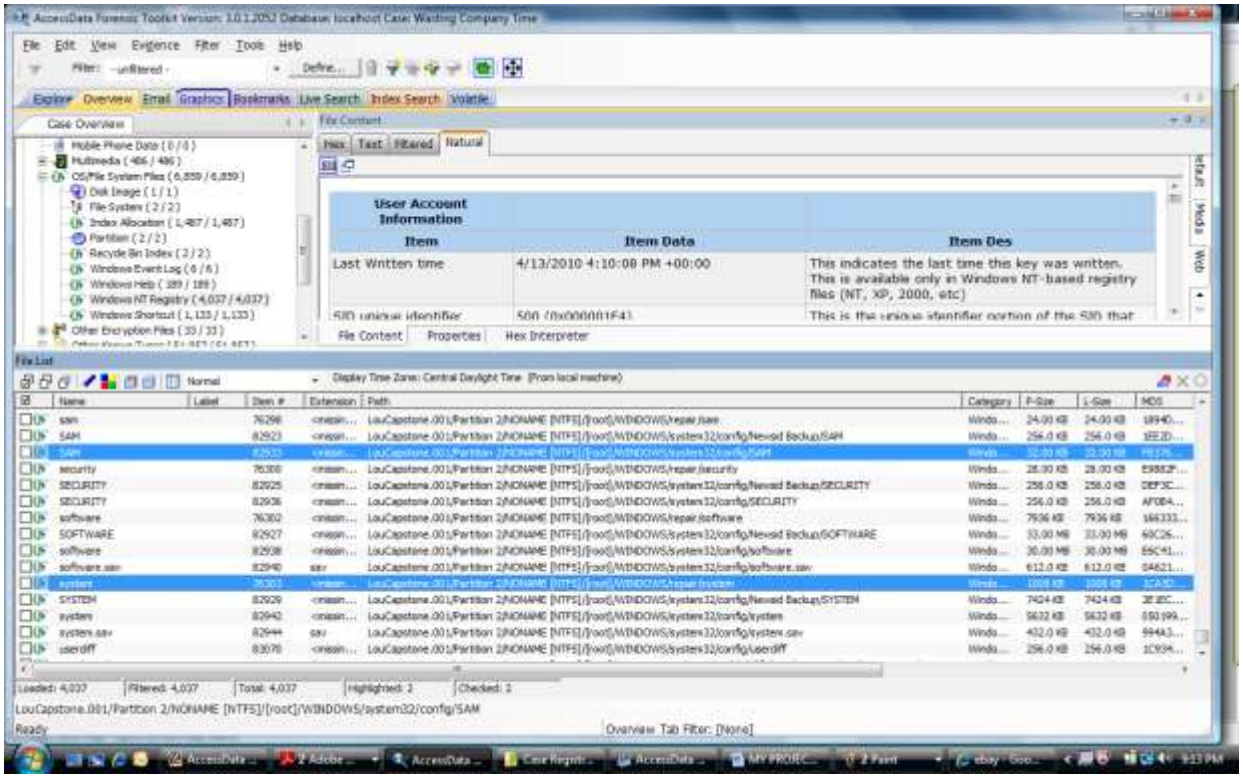


Figure 31 – Locating SAM and System files

Once they are exported out, add the SAM file to a job in PRTK. When adding the job, PRTK will ask for the location of the System file. Browse to the location to select, and start the job. In this case, Capstone (Windows account: workstation) did not use a Windows login password (Figure 32).

Another Registry file that can yield potentially useful information is the NTUSER.DAT file. A look at this file in Registry viewer shows some interesting information. Figure 33 shows the sub-keys indicating that Capstone uses MSN Messenger and logs his chat history to C:/Documents and Settings\workstation\My Documents\Received Files\shouldbworkin3103744162\History. Upon navigating to this location in FTK, the chat logs are found (Figure 34). Additionally, the chat log shows that a file was sent and saved to C:\Documents and Settings\workstation\My Documents\Received Files.

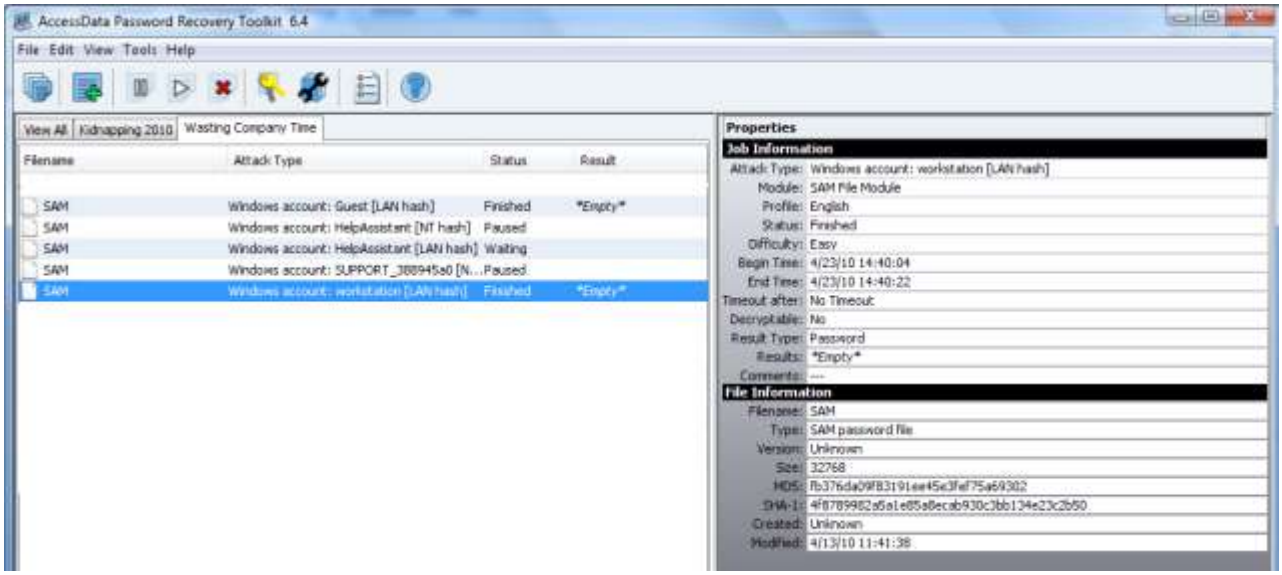


Figure 32 – PRTK shows Windows login password as “Empty”

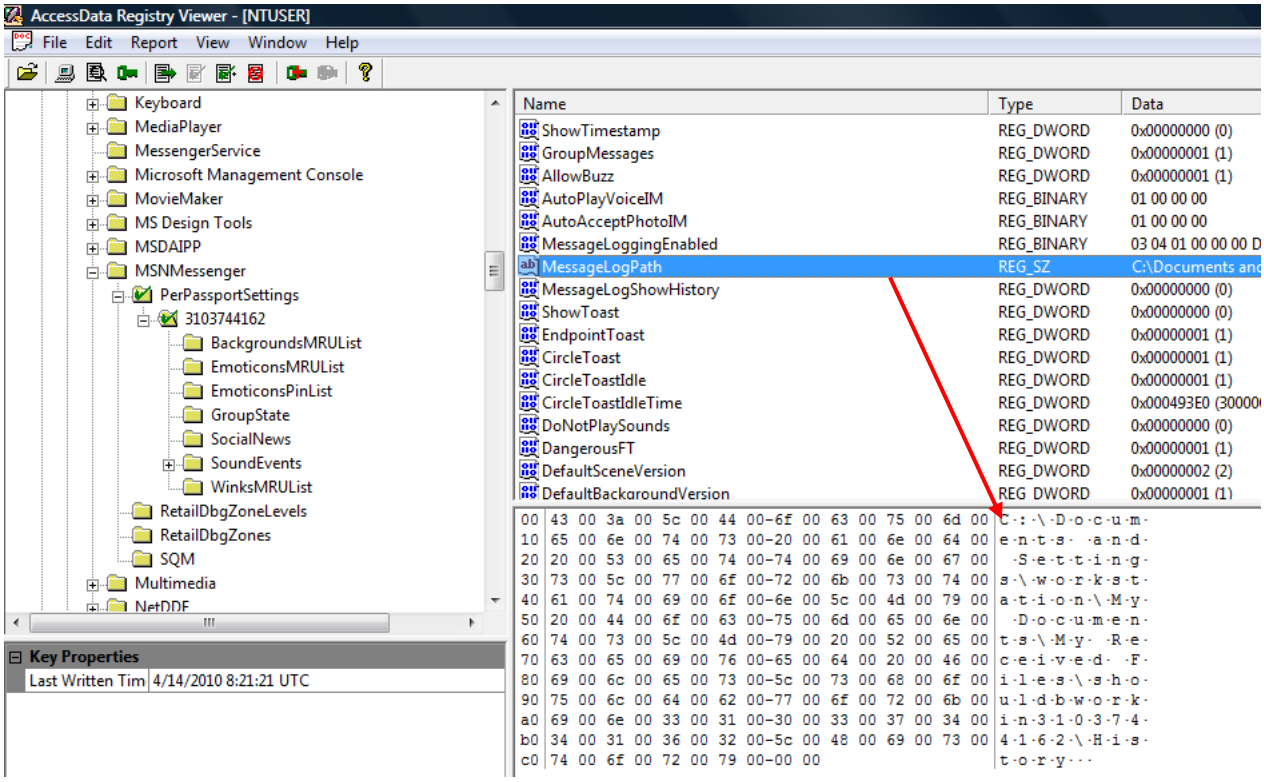


Figure 33 – Registry Viewer shows saved chat log file path

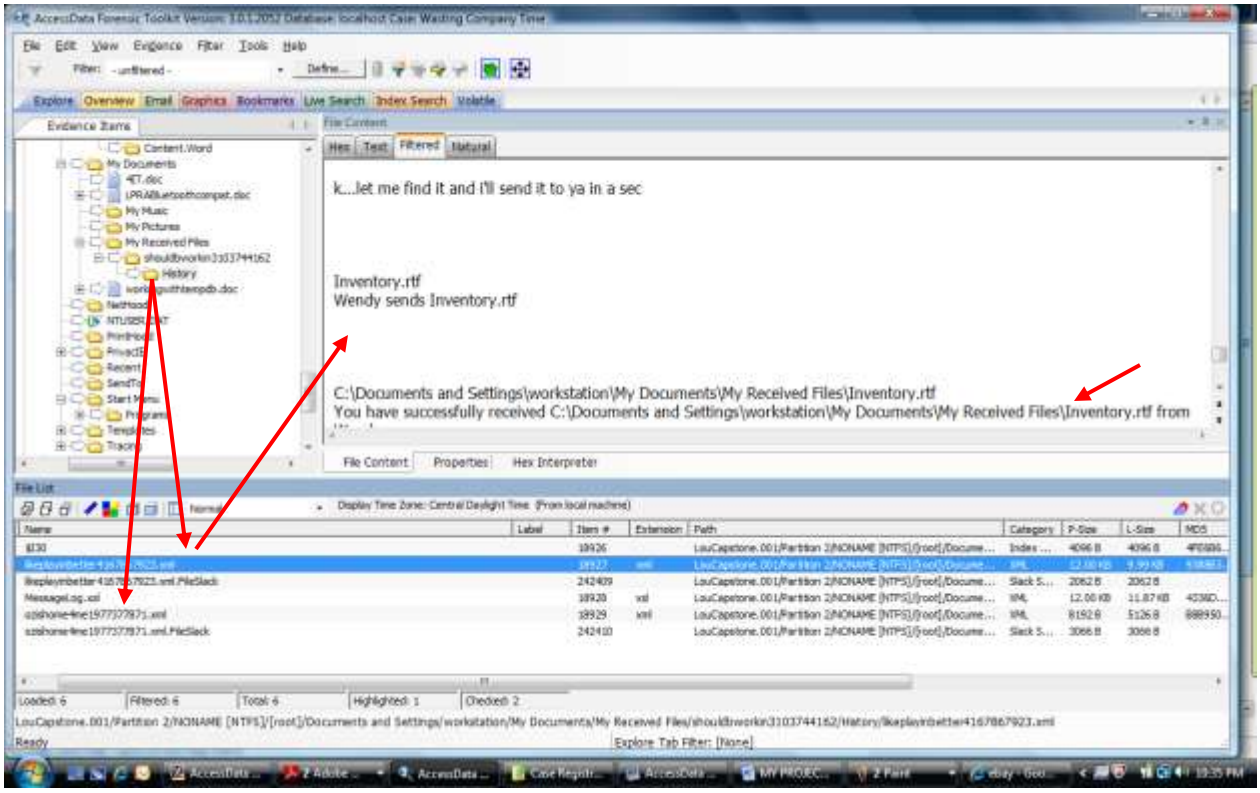


Figure 34 – Chat log showing sent file.

When navigating to this location in FTK, the sent file is found (Figure 35). Interestingly, the file contains a list of computer equipment and its location in various storage closets. Because of their numbering, one can assume that these storage closets are not in Capstone's home. This could possibly be the list referred to in an earlier email. Since the email concerned selling items on eBay and was obviously meant to be secret, one might suspect that the listed computer equipment belongs to the company. It seems that Capstone may be stealing stored company computer equipment and selling it on eBay. This was not something that the company expected to find when examining Capstone's work computer. Not only is this strike three for Capstone, but it looks like criminal charges may be in his future as well. Not a good day for Louie.

Other noteworthy items in the NTUSER.DAT file include MRU applications and files, Capstone's Hotmail password (This password is shown in plaintext and did not require decryption in PRTK), typed URLs, and Favorites listing. There is also a sub-key called IntelliForms which contains encrypted login information that was saved by Internet Explorer.

The information in the IntelliForms sub-key can be decrypted in PRTK. In order to do this, the following files must be exported out of FTK:

- NTUSER.DAT file for the user (user = workstation in this case)
- Master Key File (In this case, all files contained in the folder C:\Documents and Settings/workstation\Application Data\Microsoft\Protect)

- Internet Explorer Browsing History Index.dat file (found earlier in the case).

Additionally, a blank text file should be created for PRTK output data. Once the required files are exported and created, the NTUSER.DAT file can be dragged into PRTK. (Note: Before attempting this recovery, the Windows login password must be found using the SAM and System files. This procedure was completed earlier in the case.) PRTK recognizes that it must decrypt the IntelliForms data and prompts the user for the required information (Figure 35).

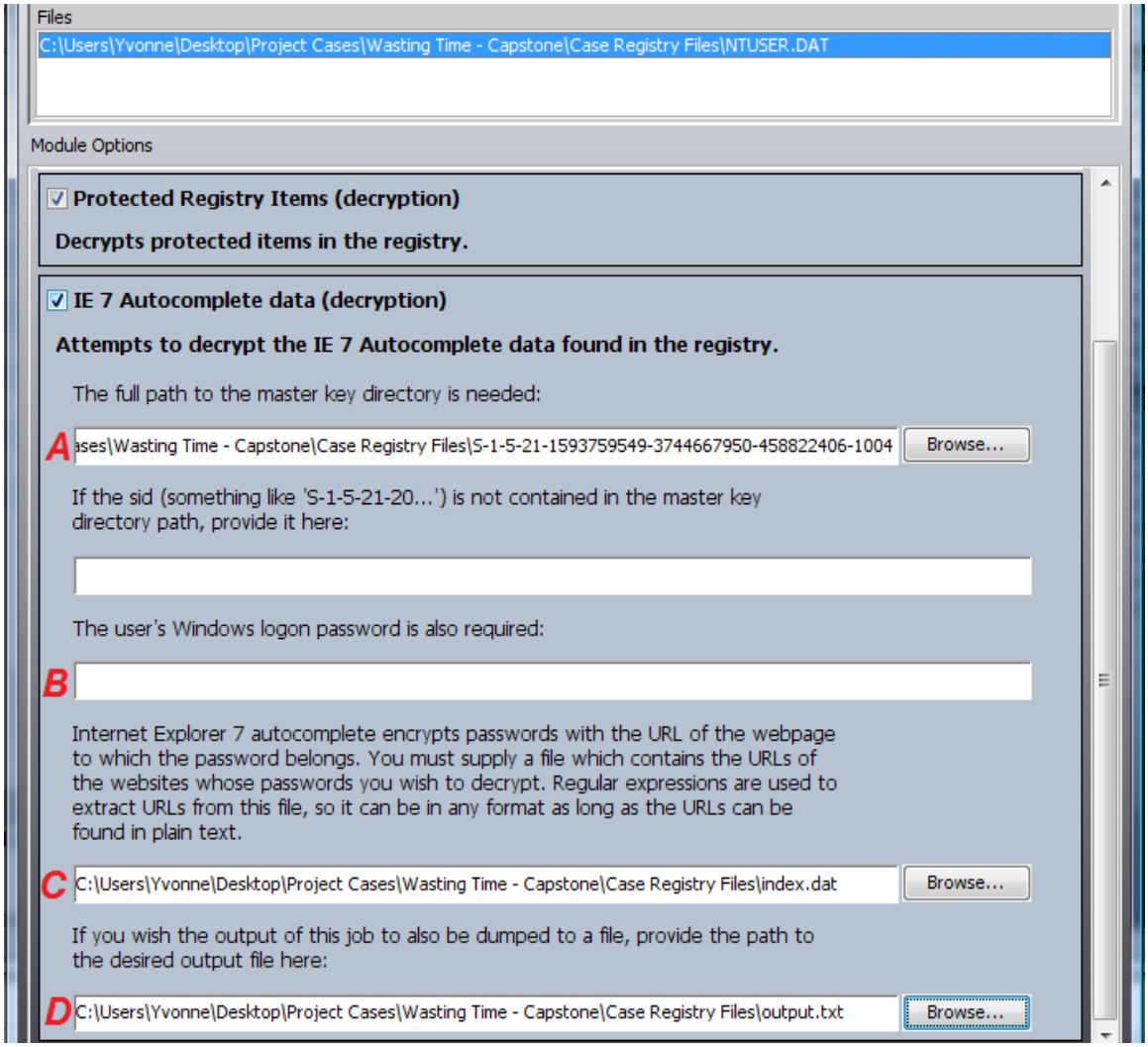


Figure 35
A. Location of exported master key directory
B. No Windows logon password in this case
C. Location of exported index.dat file
D. Location of created blank text file

The password results are shown in PRTK as they are discovered (Figure 36).

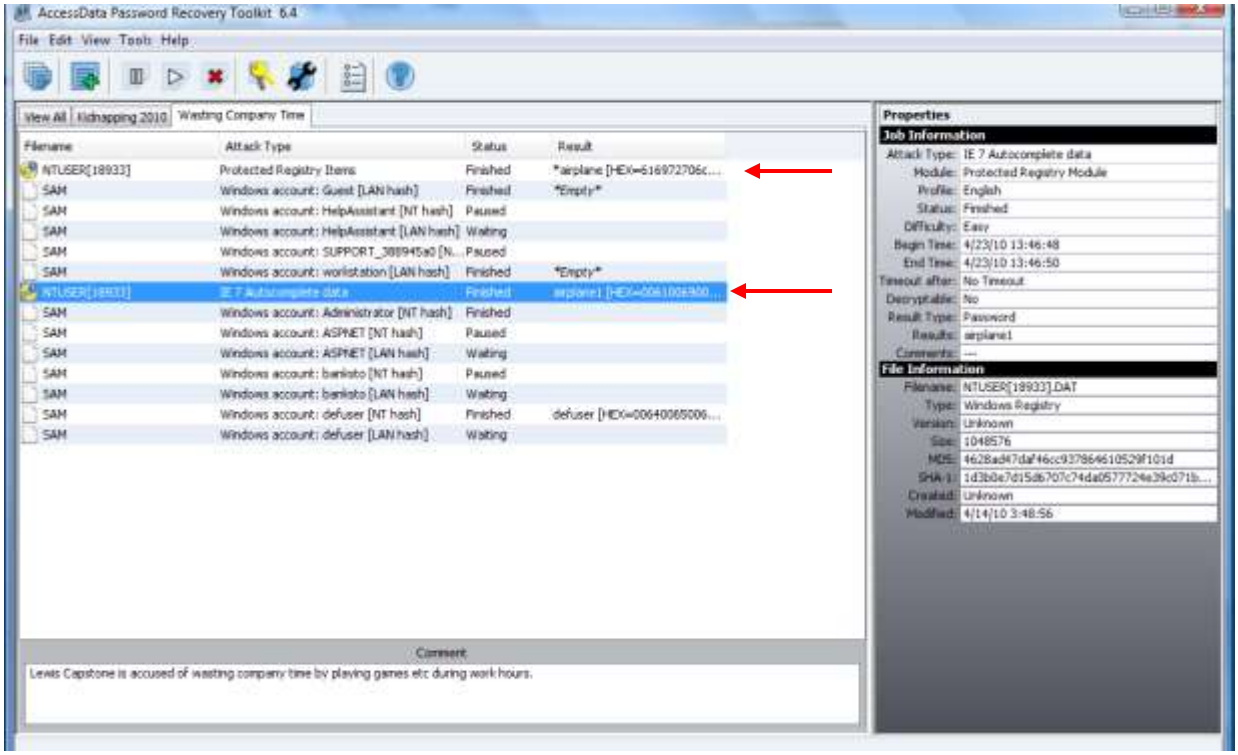


Figure 36 – Password recovery

Open the text file created earlier to view complete information dumped to the file by PRTK (Figure 37).

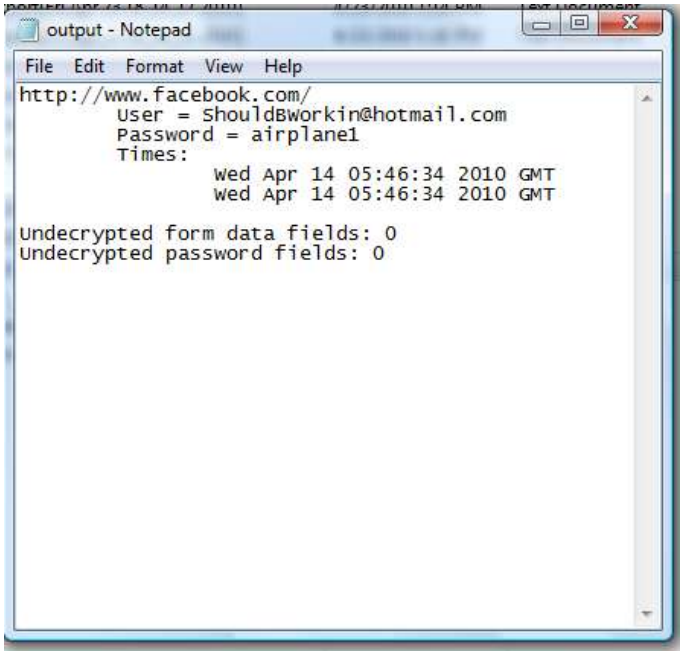


Figure 37 – Decrypted IntelliForms data showing Capstone's facebook account information.

Once examination of a registry file is complete, a HTML report can be created from the items of interest that were checked during the examination (Figure 38). Registry items can also be added to the case report through FTK.

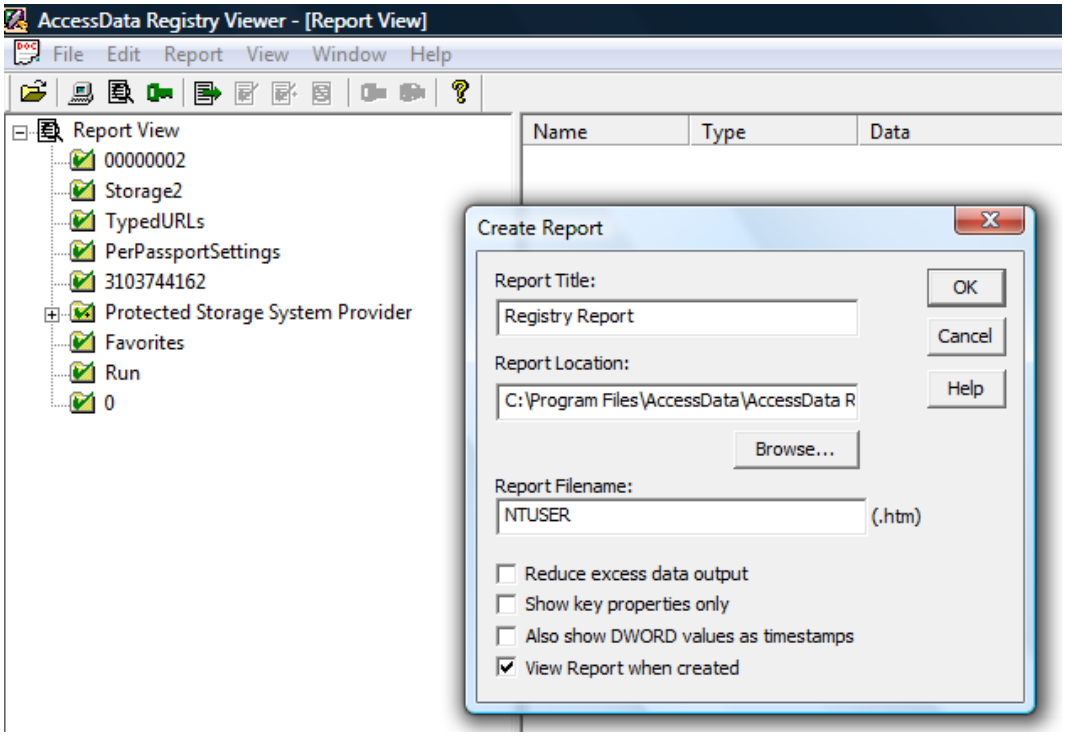


Figure 38 – Creating a Registry Report in Registry Viewer

At this point, enough evidence has been gathered to show that Capstone had been misusing company property and wasting company time. A case report can now be generated in FTK. The report can be customized to include or exclude specific items. Figure 39 shows a sample of the report creation options. Figure 40 is an excerpt of the completed case report.

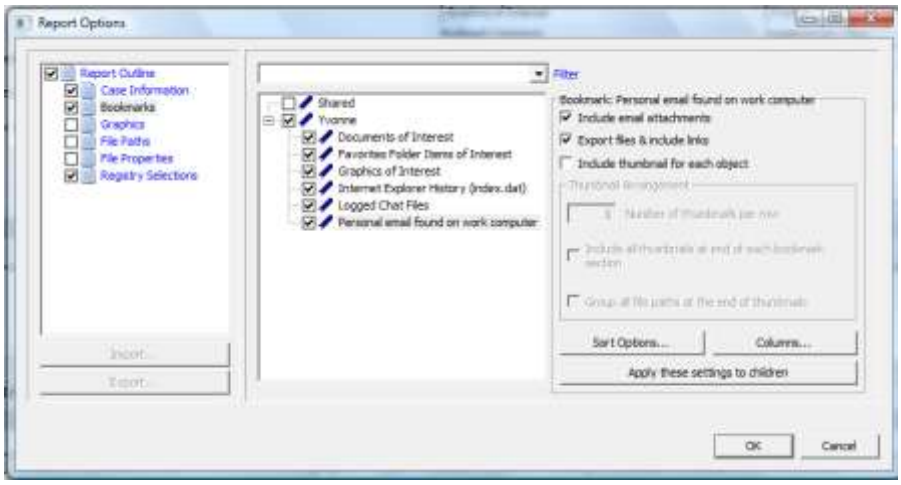


Figure 39 – FTK case report creation

Figure 40 – FTK Case Report

This concludes my analysis of the three case image files using Access Data's FTK, PRTK, and Registry Viewer. It is by no means meant to be a complete review of Access Data's capabilities but rather an introduction into forensic analysis of digital evidence. Although some things did not go as planned in the case creation and analysis processes, each image file contains enough evidence to make it both useful in the classroom, and realistic.

Conclusion

In conclusion, digital forensics is a dynamic and continuously evolving process. Rules and guidelines are provided for involved personnel in order to help assure the integrity of an investigation and the admissibility of the evidence recovered. The importance of procedure cannot be stressed enough. Armed with the proper tools and knowledge, the forensic examiner can provide an increasingly useful service for both companies and law enforcement. While digital evidence rarely provides the "smoking gun," it can provide critical information that helps in solving an otherwise unsolvable puzzle.

The difficulty of the examiner's job can vary greatly from case to case. In addition to adequate training, a well-tested set of forensic tools that comply with industry standards is necessary when dealing with digital evidence. Access Data provides a suite of tools that fit that description. From cell phone analyzers to large-scale network tools, the reputation of their products is acknowledged worldwide.

Access Data's products were successfully used in the creation and analysis of the images discussed in this project. The image files will now be available for use in the MSIS Computer Forensics class. It is my hope that the image files will be instrumental in igniting a spark of interest in the minds of curious students for years to come.

References

1. Nelson, Bill, Amelia Phillips, and Frank Steuart. *Guide to Computer Forensics and Investigations*. 2nd edition. Canada: Course Technology, 2006. 2. Print.

2. Cummings, Tucker. "The History of Computer Forensics." *eHow*. N.p., n.d. Web. 5 Mar 2010. <http://www.ehow.com/about_5813564_history-computer-forensics.html>.

3. Nelson, Bill, Amelia Phillips, and Frank Steuart. *Guide to Computer Forensics and Investigations*. 2nd edition. Canada: Course Technology, 2006. 2. Print.

4. "NIJ Special Report, Electronic Crime Scene Investigation: A Guide to First Responders." *NCJRS*. U.S Department of Justice, Apr 2008. Web. 5 Mar 2010. <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

5. "Guidelines for Searching and Seizing Computers." *Computer Crime and Intellectual Property Section (CCIPS)*. Art Power Database, Oct 1997. Web. 25 Apr 2010. <http://www.irational.org/APD/CCIPS/sect3.htm#C.2>.

6. "Guidelines for Searching and Seizing Computers." *Computer Crime and Property Section (CCIPS)*. Art Power Database, Oct 1997. Web. 25 Apr 2010. <http://www.irational.org/APD/CCIPS/ssgsup.htm#_1_16>.

7. "Recognizing Potential Evidence." *Computer Forensics World*. N.p., 27 Aug 2004. Web. 10 Mar 2010. <http://www.computerforensicsworld.com/modules.php?name=Content&pa=showpage&pid=1>.

8. Ibid.

9. "Digital evidence - its true value." *TechBeat* 01 Apr 2009: n. pag. Web. 02 Mar 2010. <http://www.policeone.com/pc_print.asp?vid=1805790>.

10. Ibid.

11. Ibid.

12. Volonino, Linda. "Electronic Evidence in Small Cases and Private Litigation." *.docstoc Documents for Small Business & Professionals*. N.p., n.d. Web. 10 Mar 2010. <http://www.docstoc.com/docs/26035924/Electronic-Evidence-in-Small-Cases-and-Private-Litigation---Robson>.

13. "Electronic Crime Scene Investigation, A Guide for First Responders." *NCJRS*. U.S. Department of Justice, Jul 2001. Web. 02 Mar 2010.<http://www.ncjrs.gov/pdffiles1/nij/187736.pdf>.

14. Sanchez, Julian. "Court: self-incrimination privilige won't protect password." *ars technica*. N.p., 02 Mar 2009. Web. 15 Mar 2010. <http://arstechnica.com/tech-policy/news/2009/03/court-self-incrimination-privilege-stops-with-passwords.ars>.

15. "NIJ Special Report, Electronic Crime Scene Investigation: A Guide to First Responders." *NCJRS*. U.S Department of Justice, Apr 2008. Web. 5 Mar 2010. <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

16. Nelson, Bill, Amelia Phillips, and Frank Steuart. *Guide to Computer Forensics and Investigations*. 2nd edition. Canada: Course Technology, 2006. 203-204. Print.

17. "BitLocker Drive Encryption." *Wikipedia*. Web. <http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption>.

18. "NIJ Special Report, Electronic Crime Scene Investigation: A Guide to First Responders." *NCJRS*. U.S Department of Justice, Apr 2008. Web. 5 Mar 2010. <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

19. Ibid.

20. Nelson, Bill, Amelia Phillips, and Frank Steuart. *Guide to Computer Forensics and Investigations*. 2nd edition. Canada: Course Technology, 2006. 36-38. Print.

21. "User Guide, Password Recovery Toolkit." *AccessData*. AccessData Corp, 2008. Web. 15 Mar 2010. <http://www.accessdata.com/downloads/media/PRTK_DNA%20User%20Guide.pdf>.

22. "Hardware Write Blocker Device (HWB) Specification." *Computer Forensics Tool Testing Program*. NIST, 19 May 2004. Web. 15 Mar 2010. <http://www.cftt.nist.gov/HWB-v2-post-19-may-04.pdf>.

23. "Disk Imaging Tool Specifications." *Computer Forensics Tool Testing Program*. NIST, 12 Oct 2001. Web. 15 Mar 2010. <http://www.cftt.nist.gov/archived_documents.htm>.

24. "Keyword Searching explained." *Norcross Group, Digital Discovery Services*. N.p., n.d. Web. 15 Mar 2010. <http://www.tng-access.com/searching_information.htm#PROCESS>.

25. Gupta, Chetan. "File Slack Vs RAM Slack Vs Drive Slack." *Network Intelligence*. N.p., 21 Jun 2006. Web. 25 Apr 2010. <http://niiconsulting.com/checkmate/2006/06/21/file-slack-vs-ram-slack-vs-drive-slack/>.

26. "File Slack Defined." *NTI*. N.p., n.d. Web. 15 Mar 2010. <http://www.forensics-intl.com/def6.html>.

27. "Keyword Searching explained." *Norcross Group, Digital Discovery Services*. N.p., n.d. Web. 15 Mar 2010. <http://www.tng-access.com/searching_information.htm#PROCESS>.

28. *Merriam-Webster OnLine*. N.p., n.d. Web. 15 Mar 2010. <http://www.merriam-webster.com/dictionary/steganography>.

29. "AccessData Overview." *AccessData*. AccessData Corp, 2010. Web. 15 Mar 2010. <http://www.accessdata.com/overview.html>.

30. "CART Examiner Training." *FedBizOpps.gov*. Federal Bureau of Investigation, 12 Nov 2009. Web. 15 Mar 2010. <https://www.fbo.gov/index?s=opportunity&mode=form&id=1d1394477e55320502f1935913a47920&tab=core&_cview=0>.

31. "Forensic Toolkit User Guide, Ver 1.80.0." *AccessData*. AccessData Corp, 22 May 2008. Web. 15 Mar 2010. <http://www.accessdata.com/downloads/media/FTK_1.80_Manual.pdf>.

32. Schneider Traylor, Polly. "Leading in a Regulatory Environment." *Microsoft Services*. Microsoft, 25 Mar 2009. Web. 15 Mar 2010. <http://www.microsoft.com/microsoftservices/en/us/article_Leading_in_a_Regulatory_Environment.aspx>.

33. Stiefel, Lynne. "Glenview double murder trial begins." *PioneerLocal*. Sun-Times Media, 04 June 2009. Web. 15 Mar 2010. <http://www.pioneerlocal.com/glenview/news/1605681,glenview-zirko-060409-s1.article>

34. "Former Musician Found Guilty of Murder." *RCFL Regional Computer Forensics Laboratory*. N.p., 13 Jul 2009. Web. 15 Mar 2010. <http://www.rcfl.gov/index.cfm?fuseAction=Public.N_CG003>.

35. "Manhattan U.S. Attorney Charges Former Goldman Sachs Computer Programmer for Theft of Trade Secrets." *Cyber Crime & Intellectual Property Section, U.S. Department of Justice*. U.S. Department of Justice, 11 Feb 2010. Web. 15 Mar 2010. <http://www.cybercrime.gov/aleynikovChar.pdf>.

36. "Case Studies, Computer Analysis - Internet History." *CCL Forensics*. N.p., n.d. Web. 15 Mar 2010. <http://www.ccl-forensics.com/Case_Studies-27.html&linkto=38#1>.