Data Sanitization: A forensic look at used hard drives

Amy Maskiewicz
Lewis University
May2009

ABSTRACT

The purpose of my project is to examine the misuse and improper disposal of old or used hard drives which in the wrong hands can expose sensitive information which can be used for fraud, identity theft and other cyber crimes. Many of today's cyber crimes occur from a cyber attack on a "live" personal or business network. Most people don't think that when they are giving or throwing away an old PC that they have to worry about their personal information being stolen because in their minds they have wiped their hard drive clean. Or so they think.

The goal of my project is to buy several used hard drives from different venues and then analyze the drives forensically using AccessData's Forensic Toolkit® (FTK®). The data retrieved from the hard drives may contain sensitive information that can be used by identity thieves. I will also use my own old hard drive and analyze it with FTK to document the amount of information that is on the drive. After the initial analysis I will perform a format on the drive. After the first format I will analyze the drive again to see how much personal data remains on the drive. I will continue this process until the drive is completely clean of any personal information to determine how many formats it actually takes to wipe a drive clean.

My project will also cover security measures to completely remove data from hard drives before disposing of them. It will address the legal requirements that organizations must follow and the penalties for not following the law. Furthermore, it will explore how digital data is being used in crimes and as evidence against criminals.

Introduction:

Computers contain more valuable personal information today than ever before. In the business world, data protection has become an increasingly important task. Certain steps should also be taken by individuals with their personal computers. With the increasing number of people who use computers to do on-line shopping, banking, posting on social networking sites and storing digital photos, the more their personal information is at risk. Organizations must provide sufficient protection for their confidential information about their company and its employees. Today there are stronger legal requirements that exist to protect user data from unauthorized use. Not only should protection be in place on working networks, but organizations must also take the proper procedures when disposing, reselling or donating used or old hard drives. Organizations are subject to certain legal obligations in terms of data sanitization. Failure to comply with these laws can result in legal fines, civil lawsuits and possible jail time.

Used disk drive case studies:

The consequences of confidential data being made public or falling into the wrong hands can be devastating to the owner of that information. Loss of such sensitive information can cause organizational embarrassment, disruption and lead to various identity theft crimes. Although data security seems to be a main concern to most organizations, in a November 2005 Gartner Inc. survey it was reported that 80% of companies stated "managing data security and privacy risks' were very important or most important when disposing obsolete hardware." However, 30% of those surveyed admitted to not having any type of data disposal policy for securing retired media (Hildreth, 2006).

Several studies have been conducted by university students as well as IT researchers on the subject of used hard drives being resold or resurfacing on the second hand market still containing confidential, sensitive information that is retrievable.

A well cited study conducted in 2003 by two Massachusetts Institute of Technology (MIT) students proved this problem exists by buying several used hard drives and then analyzing the drives. The two MIT students Simson Garfinkel and Abhi Shelat bought 158 hard drives from different sources such as, eBay, thrift stores and salvage companies. Out of the 158 drives, 129 drives were successfully imaged, 66 had recoverable files and 49 contained sensitive information including over 5,000 credit card numbers, medical data, e-mails, personal and corporate financial information and pornography. (Garfinkel & Shelat, 2003)

In April 2003, Tom Spring a senior reporter for *PC World Magazine* conducted his own experiment with used hard drives. Spring bought ten used hard drives in the Boston, MA. area. All but one of the drives contained personal information. He found data containing tax, medical and legal records, social security numbers, credit card and bank accounts, and pornography. From the information left on the drives Sprint was able to contact some of the original owners of the drives. All indicated that they had deleted or entrusted someone else to erase their hard drives. (Spring, 2003)

In February 2009 a New York based computer forensic firm, Kessler International, reported they bought 100 drives from eBay over a six month period. Out of the 100 drives 40 contained personal, confidential, and sensitive information. Kessler CEO, Michael Kessler stated " We expected most of the drives to be wiped -- to find one or two disks with data. But 40 drives out of 100 is a lot." (Mearian, 2009) Some of the data had to be retrieved with specific forensic software, but data on other drives was in the clear with no attempts to be erased or overwritten. Besides personal information, the drives also contained corporate financial records, e-mails, photos, DNS server information and one company's "secret" recipe for french fries. (Mearian, 2009)

The above studies are only a few. There are constantly new stories popping up in the news about confidential information being found on resold media. Usually this happens because people don't know how to erase a drive or they are doing it improperly. Often organizations will outsource to a third party company to have their drives wiped and entrust that the company hired is properly wiping the drives. That is not always the case. Idaho Power, a utility company based out of Boise, Idaho, found this out the hard way. In 2006 Idaho Power hired Grant Korth of Nampa, Idaho to recycle 230 SCSI drives. Grant Korth turned around and sold 84 of the drives on eBay to 12 different parties. It turned out that the drives still contained Idaho Power's proprietary company information and confidential employee information. Idaho Power was able to retrieve 146 unsold drives and got assurances from 10 of the 12 parties who bought the drives on eBay to erase the data. This incident led Idaho Power to establishing a new data sanitization policy allowing destruction as the only acceptable method. (Fisher, 2006)

No organization or individual should wait until their personal information has fallen into the wrong hands. The above case studies indicate that despite the availability of effective and easy to use tools many organizations and individuals are failing to effectively remove data from their storage devices before disposing of them.

Legal Requirements:

The California Senate Bill 1386 implemented in 2003 was one of the first major bills passed addressing the issue of security breaches involving electronic data. The bill mandated that any organization whose database consisted of California residents must notify the customers that the organization suffered an electronic security breach and that their information may have been jeopardized. (Privacy Rights, 2003). In the years to follow, several data brokerage firms, which collected and maintained personal information had suffered security breaches, putting customers' sensitive data at risk. This increase in publicized security breaches resulted in new federal laws and regulations regarding security standards for safeguarding customer information.
(Stevens, 2006)

These new federal laws relating to data retention and data sanitization were most prevalent in the financial, government, health-care and internet sectors. Some of the principal regulations are listed below:

- Health Information Portability and Accountability Act of 1996 (HIPAA)
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- Sarbanes-Oxley Act of 2002 (SOX)
- SEC Rule 17a-4

The above federal regulations all contain privacy rules and/or security safeguards to ensure the proper procedures are followed by organizations to protect electronic data through its' lifecycle from unauthorized use.

HIPAA Privacy and Security Rule:

HIPAA is the Health Information Portability and Accountability Act of 1996. There are two sections to the ACT. HIPAA Title I refers to protecting health insurance coverage for people who lose or change jobs. Title II includes an administration simplification section which covers the standardization of healthcare related information systems. The Privacy Rule in this section regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (health plans, health care clearinghouses, health insurers and Medicare sponsors). PHI is any health related information being linked to an individual either orally, written or electronic. The Security Rule requires covered entities to provide confidentiality, integrity and availability of electronic protected health information (EPHI). The Security Rule consists of administrative, physical and technical standards. Covered entities must meet these standards by protecting any EPHI which it creates, receives, maintains or transmits by assessing risks, reasonably anticipated threats, hazards and any unauthorized uses or disclosures (NIST 800-66, 2008).

Gramm-Leach-Bliley Act Safeguards Rule:

The GLBA allowed commercial and investment banks to consolidate.
The Safeguards Rule of the GLBA was enforced by the Federal Trade Commission (FTC) in May 2002. In order for a financial institution to comply with the Safeguards Rule it must develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards'' (Federal Register, 2002). These standards of a security program must address the safeguards as to how a financial institution accesses, collects, processes, maintains, transmits, stores, disposes of or otherwise handles customer information (Federal Register, 2002).

Sarbanes-Oxley Act of 2002:

The Sarbanes-Oxley Act of 2002 was enacted in response, to the high-end corporate and accounting scandals involving major companies like Enron and WorldCom, to protect shareholders and the public from fraudulent practices. The Act is administered by the Security and Exchange Commission (SEC). The basis of this Act defines how information is stored and for how long information should be kept. Title VIII section 802 defines three rules that affect the management of electronic records. The first rule deals with the destruction, altercation or falsification of records. The second rule defines the retention period for storing records. The third rule defines what type of business records need to be retained including business and electronic communications (Spurzem, 2009).

SEC Rule 17a-4:

SEC Rule 17a-4 is an amendment to the Securities Exchange Act of 1934. The rule requires specific record keeping for certain exchange members, brokers and dealers in the securities industry. The Rule allows for the storage, retention, and reproduction of records on electronic storage media under certain conditions. Records must be kept no less than three years. Records must be kept exclusively on a non-rewritable, non-erasable format. Records must be kept for a period not less than 3 years. All records kept electronically by broker-dealers must be made readily accessible for SEC review at all times (Securities and Exchange Commission, 2003)

Data Sanitization Methods:

If not erased properly data remains on a hard drive. Even if an organization or individual deletes or formats a drive data can still be recovered. Data needs to be destroyed beyond recovery to provide complete security of sensitive information.
"Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed" (Kissel, Scholl, Skolochenko, & Li, 2006).

There are several different approved methods for data sanitization in which organizations can use to comply with federal requirements. The National Institute of Standards and Technology (NIST) has published **NIST 800-88, Guidelines for Media Sanitization** which provides a comprehensive guide to assist organizations in making sanitization decisions according to their needs.

Different types of sanitization methods exist for different types of media and the information contained on that media. When choosing a sanitization method it is important to determine the security category of the information and then the media type (Kissel, Scholl, Skolochenko, & Li, 2006).

The methods discussed here will refer to hard disk and storage media. The NIST 800-88 outlines four categories of data sanitization:

- **Disposal** - discarding media by throwing it out, but only if it contains no confidential information.

- **Clearing** - involves overwriting the data so that it is unreadable and irretrievable by keyboard strokes or other data recovery utilities.

- **Purging** - More robust data removal and protects removed data from laboratory attacks. Using firmware Secure Erase command and degaussing are examples of purging.

- **Destroying** - Physical destruction of media. Media cannot be reused as original intention. Disintegration, Incineration, pulverization and melting are all methods of destroying.

Another method that deserves mentioning but not included in the NIST 800-88 guidelines is encryption. Encryption allows leaving the data in place and only allowing those who have the key to view the data. However, the encryption level must be strong and the key should be kept in a secure place and not on the same system.

Using FDISK, FORMAT or DELETE commands is not enough for data removal. By only running basic operating system commands leaves a chance of data being recovered. FDISK is a MS-DOS based utility tool that creates partitions on a hard drive. When you run the FDISK command on existing drives it only clears the partition table leaving the data in tact at the sector level. The FORMAT command only clears the address tables and checks to make sure all sectors are reliable, marks bad sectors and prepares the disk to be writable. The DELETE command does not remove files from the disk, but only removes the reference from the file system table. The data will remain on the disk until another file is written over it.

Clearing Method:

Sanitizing hard drives or other storage media using the clearing method, also referred to as overwriting or wiping, should be sufficient for most organizations or individuals. If highly sensitive or TOP SECRET information is involved then purging or destruction methods may be needed.

Overwriting overwrites all addressable locations usually with binary or random characters making data unreadable by recovery software. Usually at least three wipes are recommended to render data completely unrecoverable (Webopedia). There are consumer products as well as freeware programs available to assist in making the task a lot easier. Disk wiping software will generally overwrite the master boot record, partition table, and every sector of the hard drive. Some of the popular products are listed below:

Name	Cost	Platform
Active@Killdisk www.killdisk.com	freeware	PC bootable disk
Darik's Nuke and Boot www.dban.org	freeware	PC bootable disk
Eraser www.heidi.ie/eraser	freeware	Windows
Free DiskWipe 2.6.3 www.un-delete.com	freeware	Windows
WipeDrive Pro 5.0 www.whitecanyon.com	$99.99	Windows & MAC versions
DriveScrubber 3.5.3.0 www.iolo.com	$29.95	Windows, Linux, Unix, MAC
Data Destroyer 7.0 www.braintwist-studios.com	$32.00	Windows
Shredit 5.7 www.mireth.com	$19.95	Windows

Table 1: Examples of Disk Wiping Software

One of the biggest advantages of using freeware software is the cost. All of the freeware programs listed in the above table claim to effectively remove data from a hard drive by overwriting making it completely unrecoverable. Although they have a lot of features, they are limited and not as powerful as the consumer products. The consumer products are faster and offer more robust, customizable features. For example, WipeDrive Pro 5.0 can run simultaneous wiping, supports several wiping patterns, and has the ability to wipe an entire hard drive. The freeware programs do not include these features. For the individual user freeware programs may be sufficient. For an organization with multiple computer systems it would be worth the investment to purchase a product that has ease of use, speed and power.

Purging Method:

The purging method is usually used on proprietary and confidential data. If there is a significant risk to an organization of confidential data being lost then the media should be purged. Degaussing qualifies as a purging method. Degaussing is a process that utilizes a machine to produce a strong electromagnetic field that erases all magnetic recordings on a hard disk drive. A degausser will erase all sector head information, including track and disk motor magnets. Once a hard drive has been degaussed it is no longer operable (Hughes & Coughlin, 2006).

Data Categorization:

It is important for an organization to determine and develop a data sanitization policy. Several factors must be taken into consideration when developing a policy. The security level of data, what types of media are used, cost and environmental issues are all factors in the policy developing process (Stevens, 2006).

Data sensitivity can be divided into three different levels: low, moderate, and high. It is up to the organization or individual to determine the level of sensitivity of its data. A low level data security breach could cause minor damage or financial loss to an organization and minor harm to individuals, including their privacy. A moderate level loss would cause a significant degradation in an organizations primary functions. A significant damage to assets and financial loss, as well as, significant harm to individuals, not involving loss of life or serious life threatening injuries. A high level data loss could cause severe degradation in the ability of an organization to perform one or more of its primary functions. There could be major damage or financial loss, or cause catastrophic harm to individuals including loss of life or life threatening injuries. Regardless the level of sensitivity, data should always be protected in terms of confidentiality, integrity and availability (Kissel, Scholl, Skolochenko, & Li, 2006).

Cost is another important factor in choosing a sanitization process. Depending on the type of media used a cost effective sanitization method should be chosen. For example, the most cost effective data sanitization method for floppy disks, CD's and DVD's may be destruction. The actual value of these types of media are low so clearing or purging methods may be too costly and time consuming.

Once developed, the organization must make sure that the process and proper resources are available to support the policy. Organizations should also record and maintain documentation on what, when and how media is sanitized to protect themselves legally. Proper documentation is necessary to help maintain accountability of all equipment. Organization name, description of item, make and model, date, method of sanitization, serial numbers and reason for sanitizing should all be documented when sanitization of media occurs(Kissel, Scholl, Skolochenko, & Li, 2006).

My Case Study:

I purchased 5 different hard drives from various sources such as, eBay, Craig's List, and a local flea market. The drives ranged in size from 15 Gigabyte (GB) to 40GB. I took each drive and connected it to my own pc through an IDE/SATA to USB cable.

Before analyzing a drive an image has to be created. The program I used to create images of the drives was AccessData's Forensic Toolkit Imager (FTK Imager). AccessData is a leading provider of forensic software and training to law enforcement, government agencies and corporations. AccessData's Forensic Toolkit (FTK) software allows organizations to preview, search, analyze, process and forensically preserve electronic evidence for investigations. (AccessData, 2008)

When FTK Imager is finished with creating an image of the original drive it produces a MD5 hash checksum which verifies that the image is identical to the original drive and the original drive has not been altered. This is a critical feature in legal investigations. I imaged all 5 drives and they all produced a matching hash value. After the image is created then it is added and processed in FTK Toolkit. Figures 1 and 2 show screen shots of the results of these two processes. The figures show the results from the first drive, Drive #1, which I imaged and purchased from Craig's List . A 15GB IDE hard drive. The same screen shots were created for the four remaining hard drives except the actual hash and file number results are specific to each hard drive.

⊟ General	
Name	Clist15GB.E01
Sector count	30003120
⊟ MD5 Hash	
Computed hash	55c6718f87772be5126f8d55bbfee2e2
Stored verification hash	55c6718f87772be5126f8d55bbfee2e2
Report Hash	55c6718f87772be5126f8d55bbfee2e2
Verify result	Match
⊟ SHA1 Hash	
Computed hash	65d818159cabdcd81a3b6af6ebd674556f37502b
Report Hash	65d818159cabdcd81a3b6af6ebd674556f37502b
Verify result	Match
⊟ Bad Sector List	
No bad sectors found	

Figure 1: Drive #1 results of MD5 Hash checksum

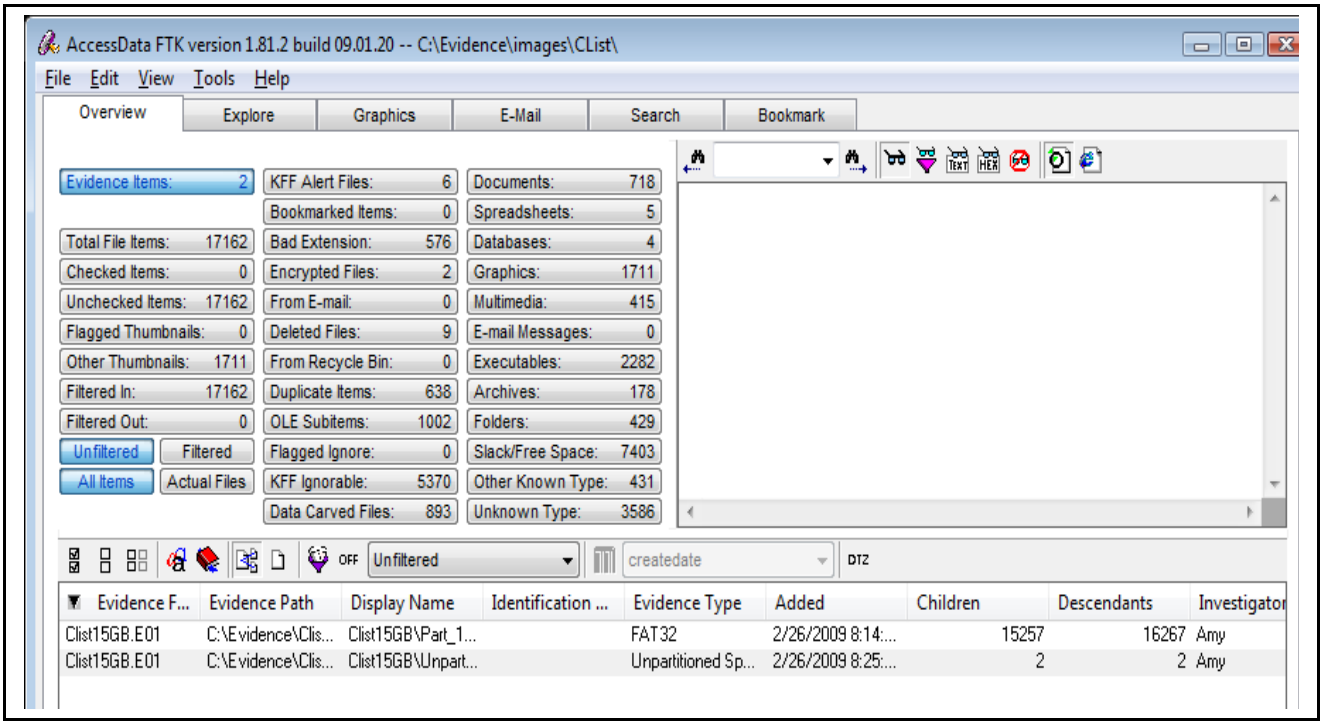

Figure 2: Drive #1 processed imaged in FTK

Figure 2 shows the main window after FTK is finished cataloging and indexing the image. In the lower window pane in the above Figure 2 you can see there are two evidence file names representing the partitioned and unpartitioned sections of the hard drive. FTK processed 17,162 items from the 15 GB hard drive. FTK separates the file types into their respective categories which make viewing and analyzing easier.

From this particular drive the previous owner did make an attempt to clean the drive. I found a configuration file from Norton CleanSweep with a recent creation date of 12/07/2008 on the drive. I purchased the drive in February 2009. Norton CleanSweep claims to delete unwanted programs from your drive along with unneeded internet files. There were no emails or user profiles found on this drive. The only remanence of data found to indicate that the drive was a used drive were about 25-30 pornographic pictures. All other files were Windows or program files.

The second drive that I analyzed was a 40GB hard drive I purchased from eBay. This drive was clean of any sensitive data. The only files on the drive were Windows program files. The third drive was a 20GB hard drive I purchased from a local flea market. The drive had been completely wiped clean with no software loaded on it. Figures 3 & 4 show the snap shots of how drive #3 appeared in FTK.

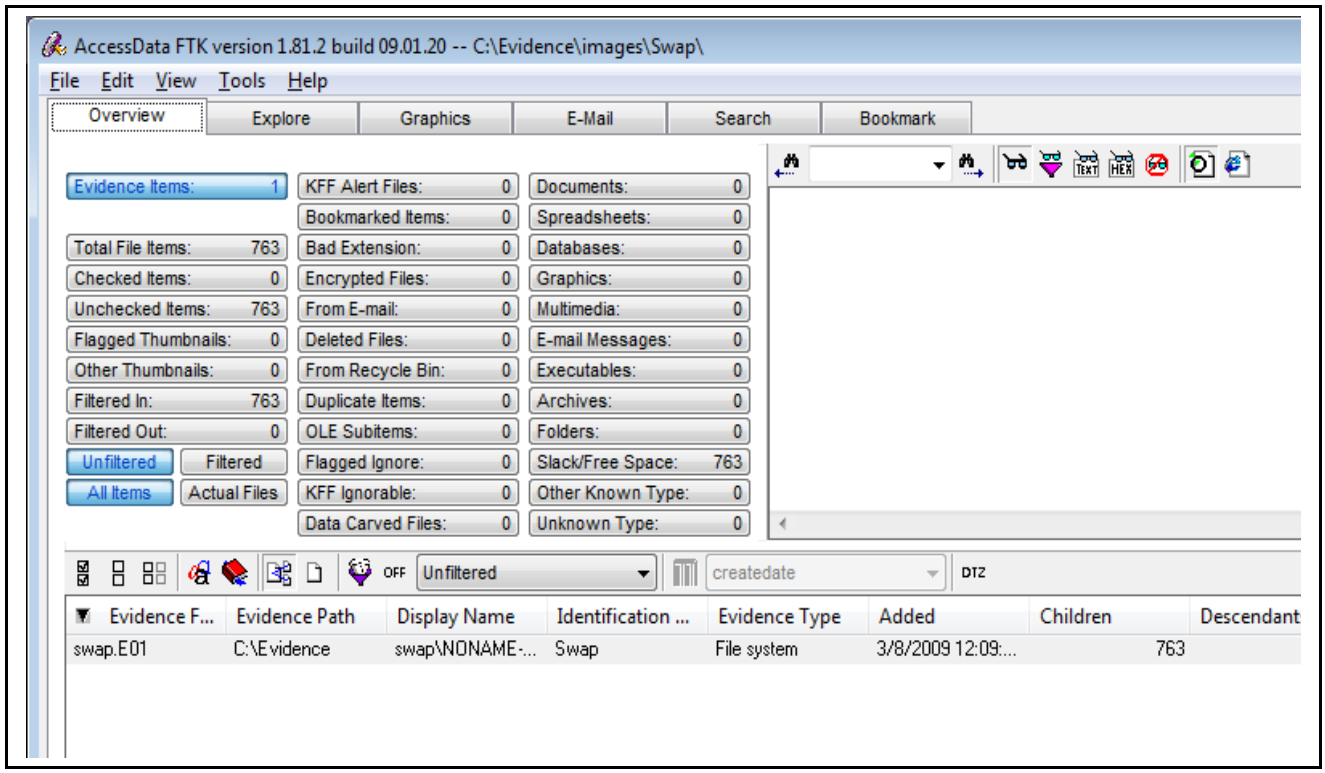

Figure 3: Drive #3 FTK Overview

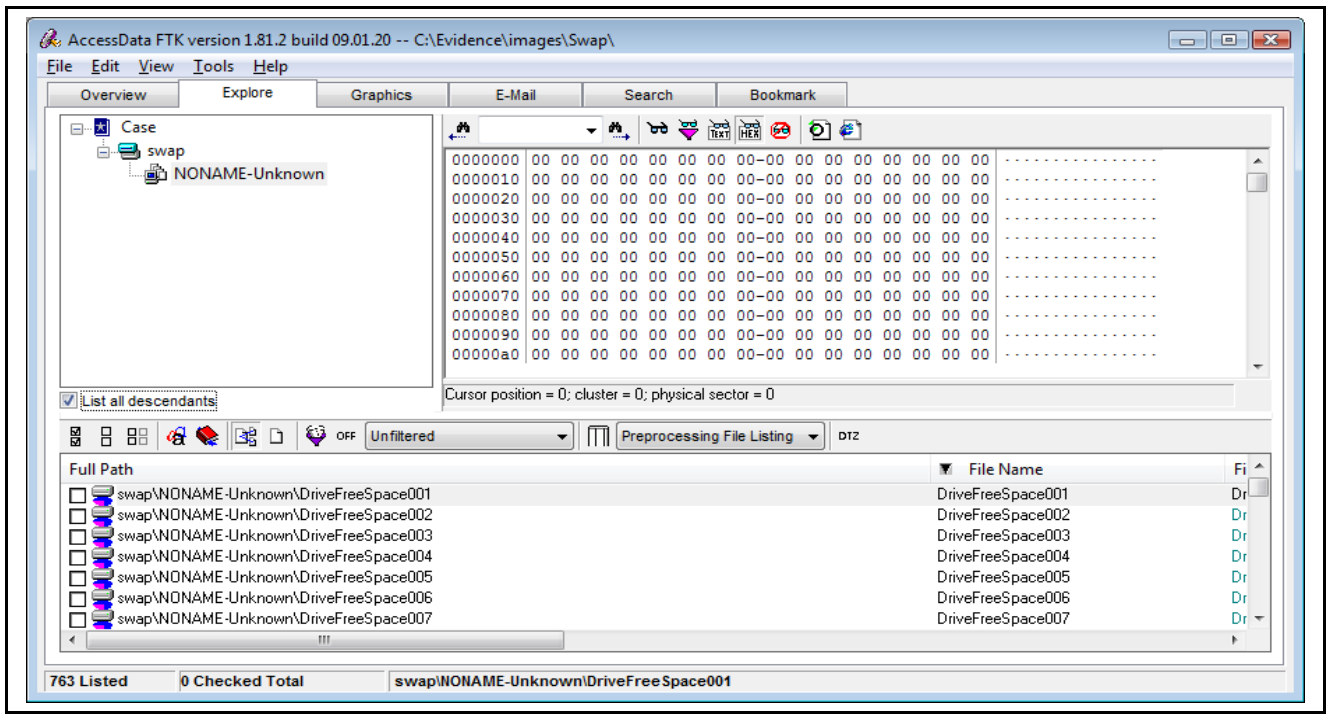

Figure 4: Drive #3 No files on drive.

The fourth and fifth drives I analyzed were a 30GB laptop hard drive and a 40GB hard drive that were purchased from different individuals from Craig's List. The results were similar to drive #2. Both drives had no personal or confidential information. There were general graphics from websites found in the drive free space along with Windows and program files on the drives.

My Hard Drive:

Part of my research was to look at a drive where no type of data sanitization had been performed to show just how much personal data exists and how it can be harmful if that information should fall into the wrong hands. I took a hard drive from an old computer I had and analyzed it with FTK. I was quite surprised to see just how much information was there that the average person may not think about when getting rid of an old hard drive. Figure 5 below shows the statistics from the first analysis.

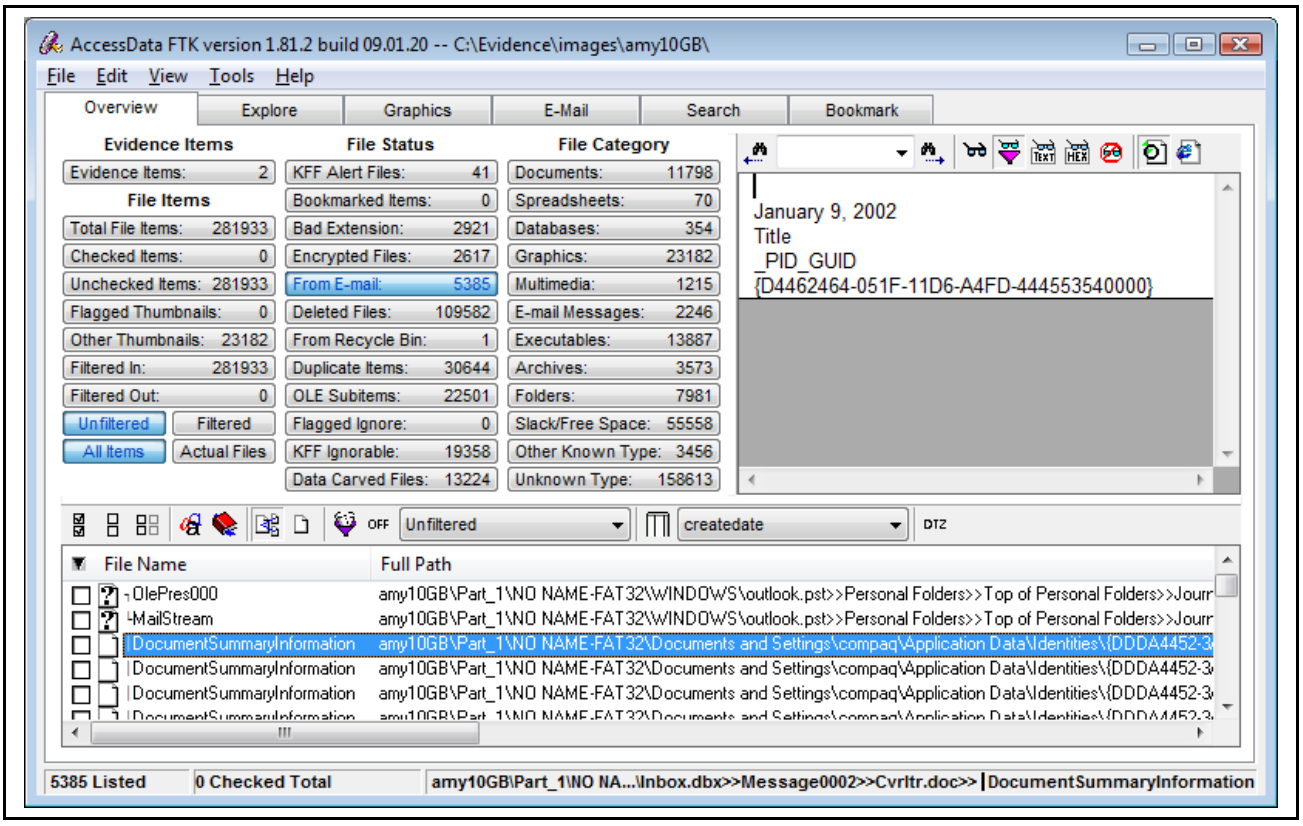

Figure 5: 10GB drive 1st analysis

There were a total of 281,933 files found on the drive. Over 5,000 emails and 55,558 items found in drive slack space. In the top right pane in Figure 5 it shows an email dated back to 2002. Information that you thought was deleted a long time ago still may exist if it has not been overwritten by another file and can still be recovered. I then performed a quick format on the drive and analyzed it again in FTK. Figure 6 shows the file results.

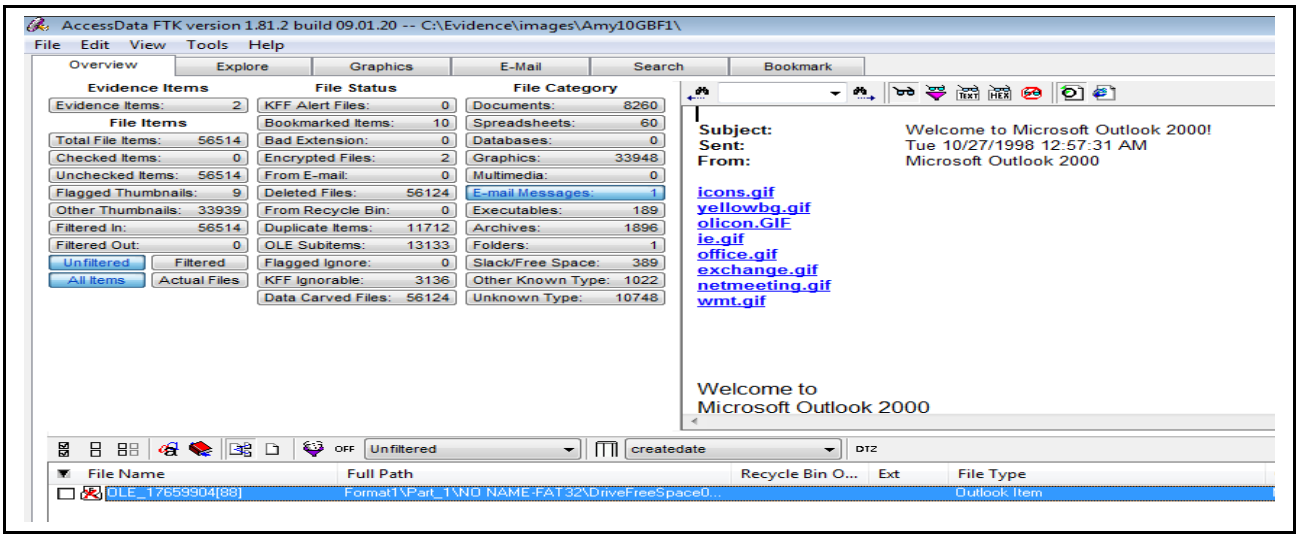

Figure 6: 10 GB HDD drive after 1st format

As you can see from Figure 6 the total file items are now only 56,514 a big difference from the original 281,933 files. FTK only detected one email and it was dated back to 1998. There was still a large number of items listed in the documents category so I went through them to see what was still viewable. All the documents listed had red X's on them which FTK signifies as a deleted file. The majority of the files listed were html, jpeg exif files, and pdf's. Almost all the html files were still viewable and in tact. The jpeg's were not viewable as graphics only the file information associated with the graphic was listed. Only a few of the pdf files were viewable, the rest contained no information. I was still able to fully view some emails listed as html files that contained my name and email address as shown in Figure 7. The email was junk email that I know I didn't save but it still existed in the drive free space since 2002.

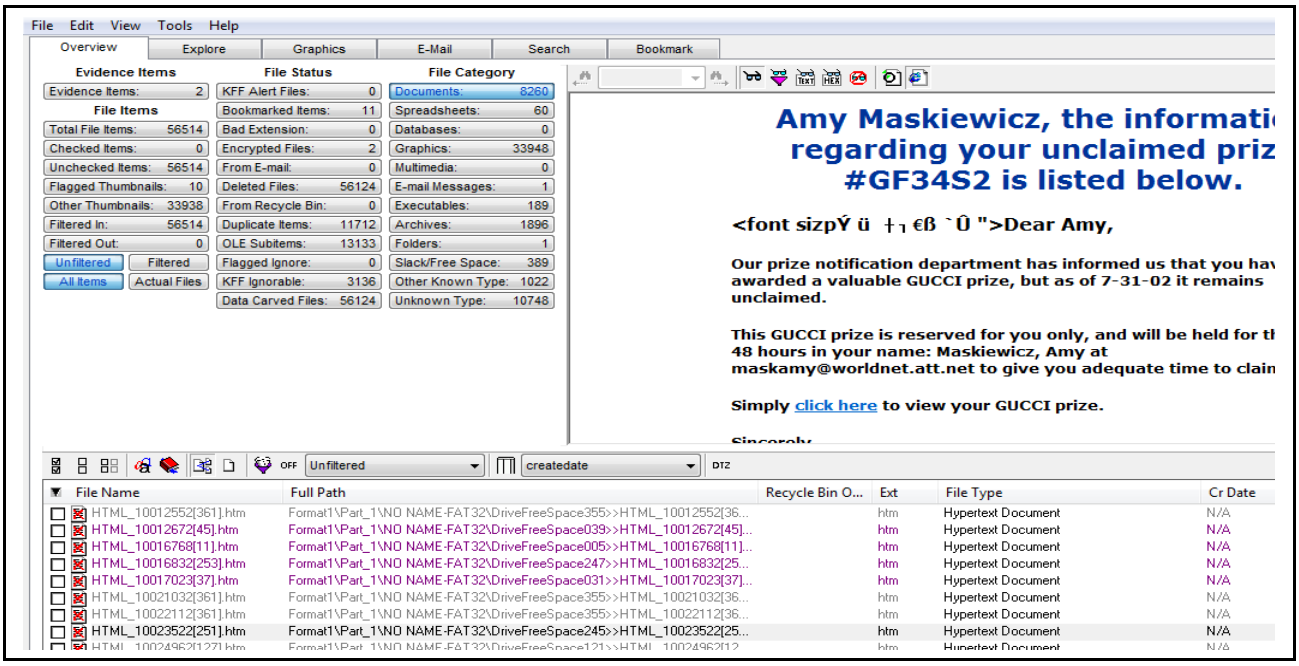

Figure 7: Deleted email file

A format on the drive did not erase all files, it only erases the address table information so that the operating system will see the space as available. After the first quick format, there were no personal emails or registry files, a majority of the graphics are still available but they are listed under drive free space. Some graphics are not visible and some are partially visible. With forensic software, even if the graphic is not visible, information about the file is still obtainable. Figure 8 highlights a graphic that has a display error where the actual graphic is not viewable, but FTK allows you to look at the hexadecimal values of the file. From reading the header information you can still see the file name. This is important because this proves that, that file existed on your system. This is important in criminal investigations by law enforcement. Also in Figure 8, on the right side of the middle pane is where you see the file header information:

Messier Image\Part_1\FAT32-FAT32\Solar System\Asteroid Belt\Web Pages\433 Eros_files\host.gif

This gives the full path and file name of where the file once existed. Because this image was after the format the new file path in FTK is different:

Format1\Part_1\NO NAME-FAT32\DriveFreeSpace272>>GIF_7216392[278].gif .

All files are now seen as drive free space and this is shown in Figure 8 on the left hand side of the middle pane.

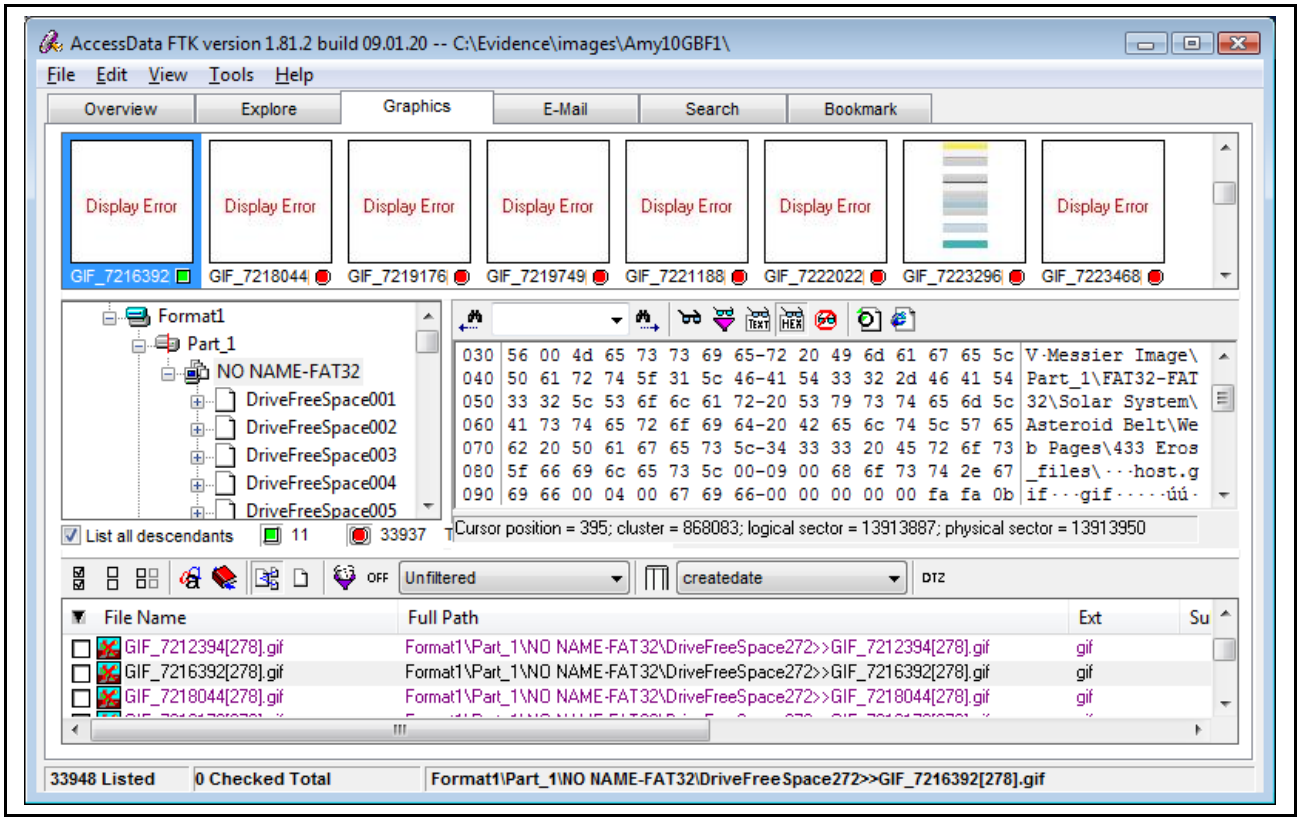

Figure 8: File header information

Figure 9 shows the screen shot after performing the second quick format on the 10 GB HDD. The file count is exactly the same as after the first format. This proves that formatting does

not clear or erase files from the drive but only clears the file allocation tables. The files still remain on the drive but are seen as drive free space.

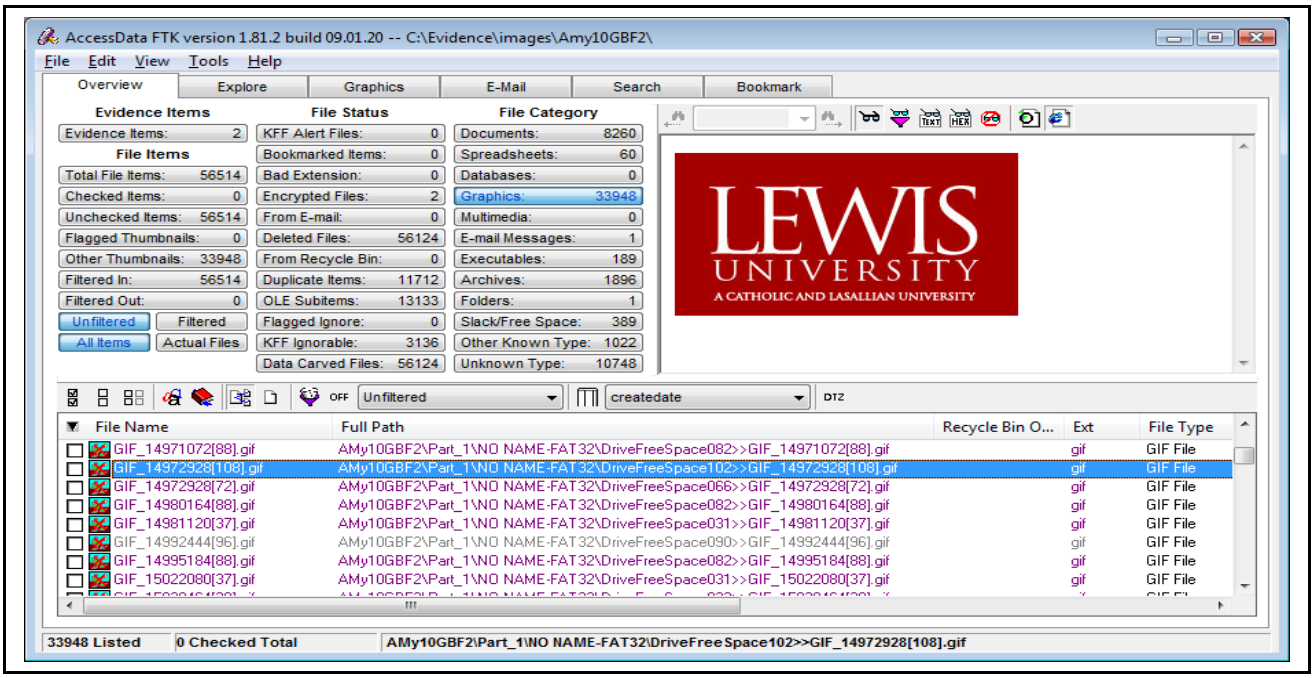

Figure 9: File totals after 2nd format

Since formatting is not a secure method of clearing a hard drive I resulted to a freeware drive wiping software program called CopyWipe 1.14 by Terabyte Unlimited. Using the CopyWipe 1.14 I ran a one-pass wipe process and then analyzed the drive again in FTK.
Figure 10 shows the results.

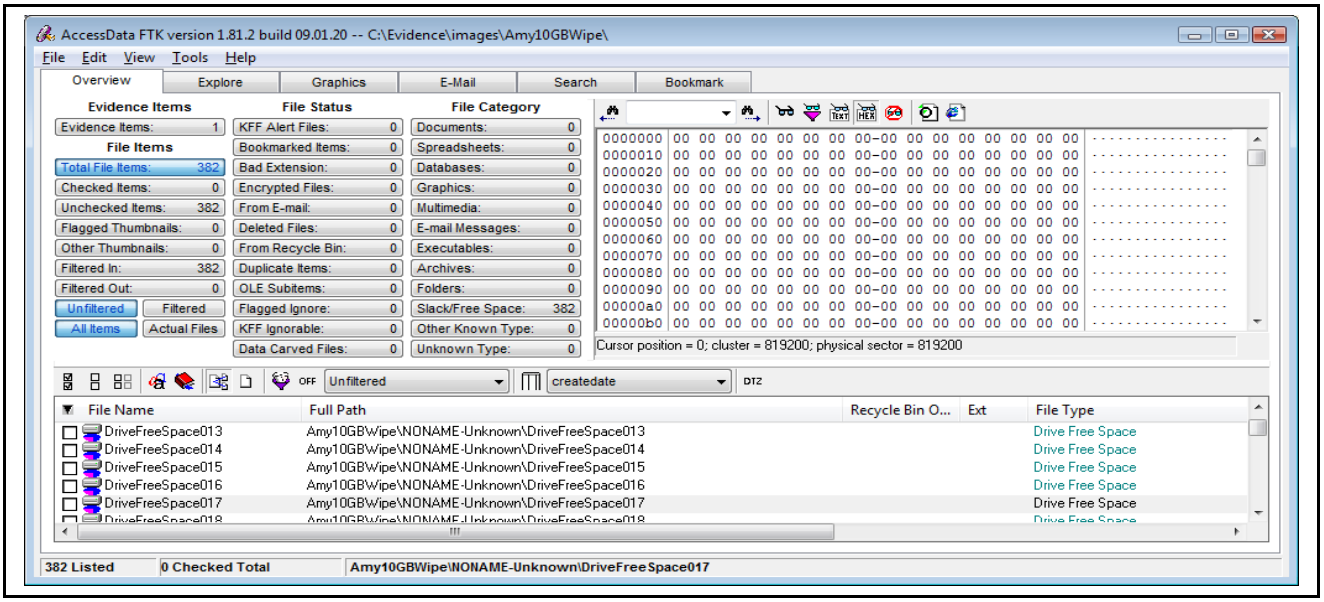

Figure 10: 10 GB HDD after using CopyWipe 1.14

The drive is completely overwritten with only using a one-pass wipe process with CopyWipe 1.14. There are no files. The only items detected by FTK is the drive free space and you can

see from Figure 10 the drive free space is zeroed out. In this example the freeware software was sufficient for wiping the drive, but it was a very small drive. The process took less than five minutes. Organizations with multiple systems or hard drives that are much larger may need a faster more flexible program.

The results of my study only produced a minimal amount of data on the hard drives that were examined. Compared to the case studies mentioned earlier in this paper my study was done on a much smaller scale. The majority of the studies conducted bought a larger amount of hard drives stretched over a longer period of time. Even with the tougher laws on organizations and the heightened media attention of security breaches and identity theft there are some organizations and individuals that fail to take the proper precautions in protecting their data.

Digital data and crimes:

Theft of sensitive information from individuals and business organizations computing systems is one of the fastest growing crimes in the United States. (National Crime Prevention Council, 2009). Whether a criminal obtains your confidential information from stolen laptops, disposed media, or security breaches he can use that information to commit various crimes of identity theft and fraud. According to the Consumer Sentinel Network (CSN) identity theft and fraud were the number one reported crimes to the Federal Trade Commission (FTC) reaching over 1.2 million complaints in 2008. (Federal Trade Commission, 2009).

Data loss or theft occurs almost every day. The Open Security Foundation is an open source community project which currently maintains the Data Loss Database (DataLossDB). DataLossDB is a recognized leader in the categorization of data loss incidents. Its main objective is to maintain the loss of personally identifying information in the United States and throughout the world (Attrition.org, 2008). Not all data loss incidents receive widespread attention in the media. In fact some breaches go unreported. The website www.datalossdb.org is a great resource to obtain current information on data loss incidents. Figure 11 shows reported data loss incidents from 2000 through 2009. (Datalossdb, 2009)

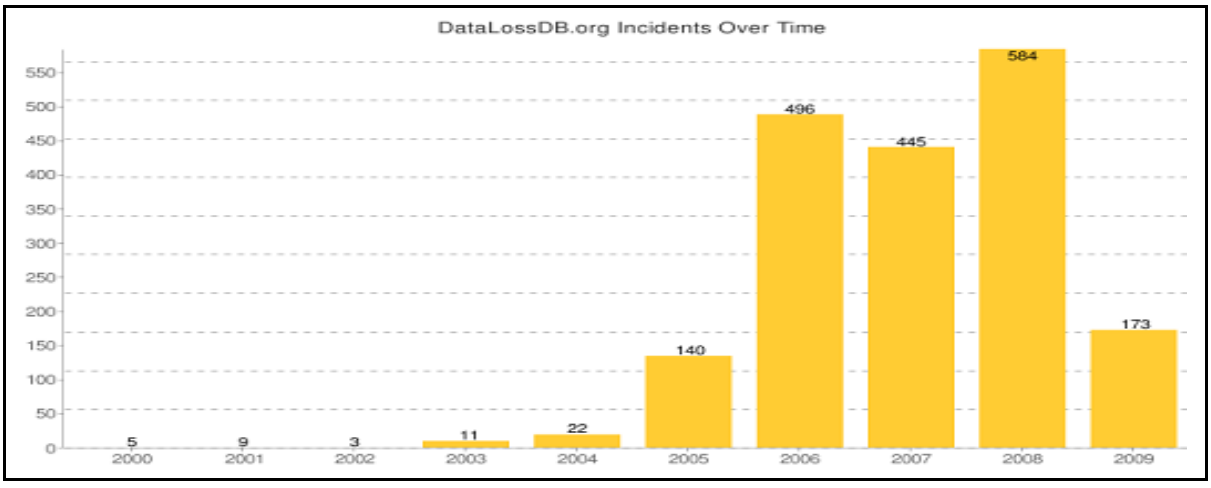

Figure 11: Reported Incidents from 2000 - 2009

Figure 12 illustrates the reported public data breaches gathered by Datalossdb divided by breach type involving personally identifying information for the year 2009.

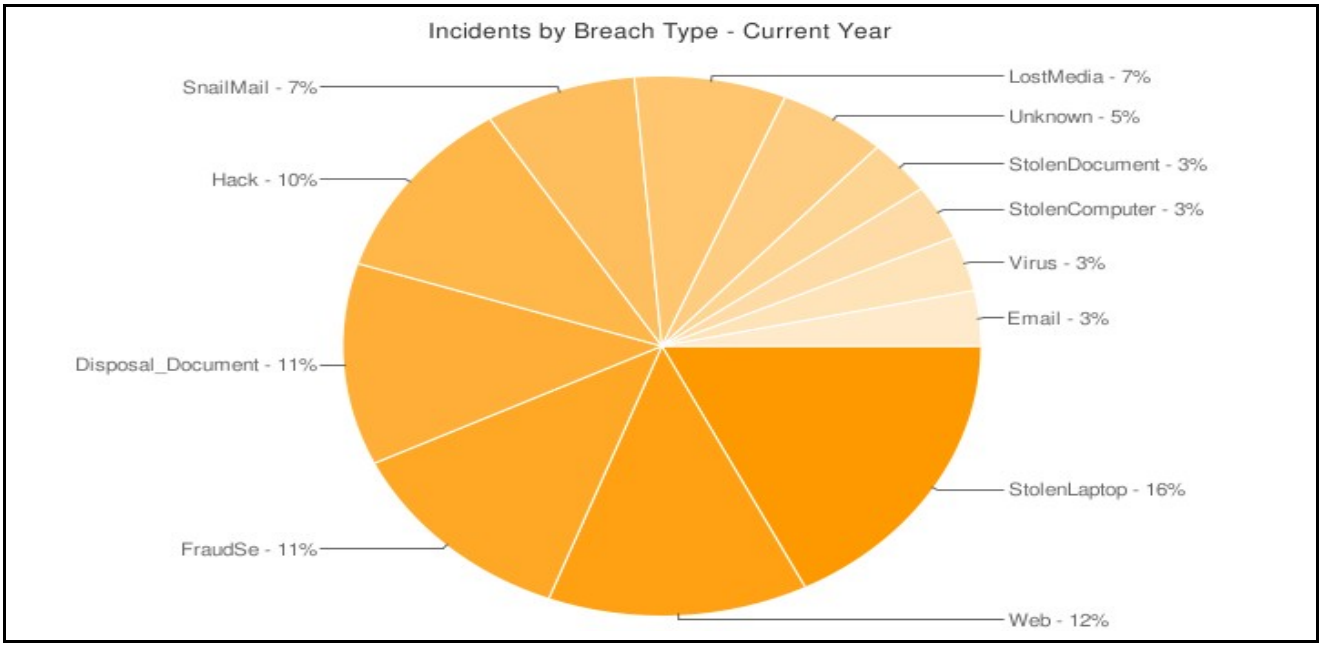

Figure 12: Incidents by breach type for 2009

Of the 173 data loss incidents reported so far for 2009 the business sector has had the most breaches. Name and/or Addresses (NAA) and Social Security Numbers (SSN) are the two most type of data being reported as lost. Figure 13 displays the breakdown of the different business types and data types by percentages for 2009 (Datalossdb, 2009).

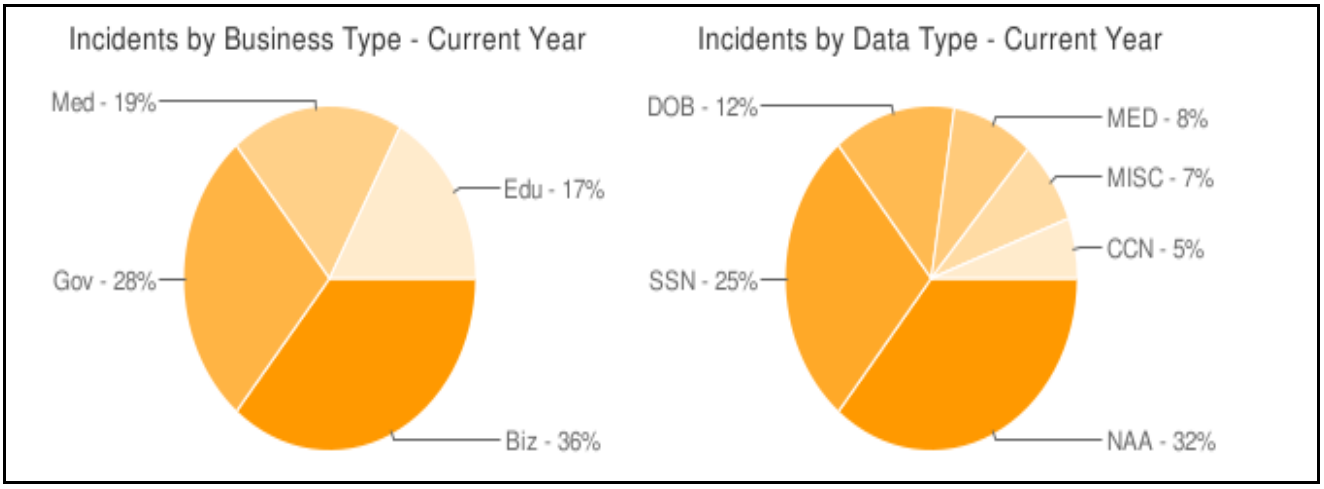

Figure 13: Incident by Business and Data type for 2009

As technology continues to advance so do the skills of cyber criminals. Because so much of what we do as individuals and businesses in our every day lives is done through some form of electronic means, criminals have learned to use technology to their advantage to commit more sophisticated cyber crimes. Digital data does not always favor on the side of the criminal. Digital data, referred to as digital evidence, has come to play a large part in today's criminal investigations.

Computer technology and computer systems can be used to commit crime, be a target of crime and contain evidence of a crime. Identity theft, terrorism, counterfeiting, online brokerage schemes, child exploitation, embezzlement, theft and distribution of credit card numbers are all types of crimes that criminals are committing with the use of computers. (Gallegos, 2005).

A criminal can use a computer as a database to maintain lists and records of acquired information. For instance, if a criminal is stealing credit card or social security numbers they can create a text or spreadsheet file to maintain it for retrieval at a later time. Child pornographers maintain thousands of graphic and movie files on their computers. Financial fraud and embezzlement records have also been found and used as digital evidence against criminals (Zucker, 2007).

Criminals also use computers as a tool to conduct criminal activity. With access to the internet anyone can target or access other computer or network systems. Network systems or users can be directly targeted by someone with malicious code, viruses or Denial of Service (DoS) attacks causing damage or outages to a system. Once a hacker has access to a system there is no limit to the damage that can be done. A criminal can try and hide his tracks by taking over a machine that doesn't belong to him and then conduct criminal activities from that machine so any evidence would be tracked back to the compromised machine and not the criminal. A business system being hacked to steal confidential, proprietary information is another example of a computer being targeted (Carter 1995).

Digital evidence is becoming more prominent in today's criminal cases. The development of the Internet and the continuing advancement of technology has contributed to the enormous growth of cyber crimes. To help combat the cyber criminal and the increasing rise in cyber crimes the field of computer forensics was developed. Computer forensics is the science of collecting, preserving, examining, analyzing, reporting and being able to provide an expert opinion in a court of law. (Hailey, 2002)

In 1984 the Federal Bureau of Investigations (FBI) and other law enforcement agencies began developing programs and laboratories to examine computer evidence. For practically any type of crime that is committed using a computer, or electronic device with media storage, a computer forensic specialist can investigate and gather digital evidence against the criminal (Gallegos, 2005). Specialized computer forensic software has been developed to assist in the examination of electronic media in legal investigations.

Guidance Software's EnCase® is one of the most widely used forensic programs used by law enforcement agencies (Guidance Software, 2002). Access Data's Forensic Toolkit is another popular program. Both programs are designed to allow investigators to make an exact image copy of the original piece of evidence. Once an image has been made the software is used to search for hidden folders and unallocated disk space for copies of deleted, encrypted or damaged files. Any evidence found can be generated into a report and

used in legal proceedings.

Forensic Software was used by law enforcement agencies to catch the Wichita, Kansas BTK killer, Dennis Rader in February 2005. Digital evidence was obtained from a floppy disk sent to police by the BTK killer. The floppy disk was examined using forensic software. Retrieved from the disk was a Microsoft Word document. The metadata of the file revealed that the disk was created by a computer belonging to the Christ Lutheran Church. Metadata is data about data. Metadata can indicate the name, size, data type, or ownership of a file. The name of the person to last save the file on the disk was "Dennis". Dennis Rader was a member on the council of the Christ Lutheran Church. This evidence allowed law enforcement to obtain a warrant to test a DNA sample from Rader's daughter. The DNA produced a positive match to DNA taken from underneath the fingernails of one of the BTK victims (National White Collar Crime, 2006).

Forensic software was also used to help convict Scott Peterson for killing his wife Laci. Using forensic software investigators examined Peterson's computer which contained a map of the island where Laci's body was found. Digital evidence also revealed that he had shopped online for a boat and studied water currents in the San Francisco Bay area.

In December 2004, Bobby Jo Stinnett, was found dead in her kitchen in Skidmore, Missouri. Stinnett who was eight months pregnant was found strangled, stabbed, and her unborn child removed from her womb. Internet chat sessions found on the victim's computer lead investigators to the killer - Lisa Montgomery. Montgomery contacted Stinnett through the internet pretending to be interested in puppies which Stinnett had for sale. Examination of the suspect's computer revealed internet searches on c-sections, a purchase of a birthing kit, and information proving that Montgomery knew Stinnett was pregnant. Montgomery was sentenced to death (National White Collar Crime, 2006).

In July 2007, three Jihad network terrorist pleaded guilty to using the Internet to incite murder. In 2003, Lisa Spence received an e-mail urging her to verify her eBay account information. By responding to the email the link took her to a phony eBay site where she entered her personal financial information. Spence's information was sold on the black market to a 21 yr. old student, Tariq al-Daour, living in the United Kingdom. al-Daour used stolen identities and credit card accounts to purchase a range of web sites where extreme propaganda and material produced by Al-qaeda was published to incite murder to innocent people. (Krebs, 2007)

Jason Hawkins a 30 year old Kentucky man was arrested and charged with transporting, receiving, possessing and creating child pornography. The suspect was arrested as part of an investigation being conducted by agents of the U.S. Immigrations and Customs Enforcement (ICE). An undercover agent logged onto an Internet chat room and was shortly contacted by Hawkins. During the conversation Hawkins sent the agent several items of child pornography. A search warrant was obtained for Hawkins's computer and digital cameras. A forensic examination of the computer's hard drive revealed over 6,900 images and 456 movies files that were identified as child pornography. From the digital cameras several home made movies were found that showed children ranging in ages from 3 to 5 years involved in sexual positions and acts (U.S. Immigrations and Customs Enforcement, 2007).

Conclusion:

Personal, sensitive, confidential data existing on any type of media storage should be protected throughout its lifecycle. It is the responsibility of the owner of that information, whether it's an organization or an individual to take all necessary precautions to provide data security. Sensitive documents and data containing personally identifiable information can be stored electronically in multiple formats and locations on storage media. Organizations and individuals must be aware of what their storage devices contain. Understanding the importance of knowing what is being stored and where will allow you to identify the need and proper procedures for data media protection and disposal.

Several examples and facts have been pointed out in this paper to heighten the awareness and importance of having a documented data sanitization and disposal policy. The consequences of not properly protecting and safeguarding personal, sensitive, and confidential information can result in legal fines, civil lawsuits and embarrassment. Tougher legal requirements have been enforced due to overwhelming statistics of data loss and theft. HIPAA, GLBA, SOX, and SEC Rule 17a-4 have all played a significant role in implementing stronger federal regulations in order to ensure the confidentiality, integrity, and availability of sensitive, personally identifiable information stored electronically.

Regardless of how secure an organization or individual believes their system is protected there is always risk involved with the human element. Whether deliberate or unintentional, data loss or theft is a constant factor.

There is no such thing as a completely secure system. Providing sufficient and constant up to date security measures is time consuming and costly. Unfortunately, because providing security is so costly organizations and individuals only implement safeguards after they have been victimized or found legally liable for a data loss incident.

As long as security vulnerabilities exist there is a criminal waiting to exploit that vulnerability for his own gain. With the continued advancement in technology, widespread use of the Internet, and the growing number of hand held portable devices used personally and for business, the number of possibilities for criminal activity increases. Computer related crimes have become a top priority nationwide with law enforcement agencies. Computer forensics and digital evidence are tools that aid in the fight against cyber criminals. As technology becomes more sophisticated so do the criminals and the crimes they commit. To effectively respond to the increase in computer related crimes national and local law enforcement, as well as private organizations, need to constantly develop their technical skills to keep up with the criminals.

References

(2003, July, 01). California Notification Security Breach Notification Law. *Privacy Right's Clearinghouse*, Retrieved April, 2009, from http://www.privacyrights.org/ar/SecurityBreach.htm

(2006). Computer Forensic Solutions with EnCase Software. Retrieved May 8, 2009, from Guideance Software Web site: http://www.guidancesoftware.com/law_enforcement/index.aspx

(2006). Identifying & Seizing Electronic Evidence. *Cyber Investigation 100*, Retrieved May 7, 2009, from http://www.nw3c.org/

(2006). Two Witchita police detectives use skills taught by NW3C. *Informant*, *1*, Retrieved May 7, 2009, from http://www.nw3c.org/resources/docs/informant_NOV05.pdf

(2007, April 23). Kentucky child pornographer sentenced to 60 years in prison. Retrieved May 8, 2009, from U.S. Immigration and Customs Enforcement Web site: http://www.ice.gov/pi/news/newsreleases/articles/080424bowlinggreen.htm

(2008, October 17). Formatting a Hard Disk Drive. Retrieved April, 2009, from Webobedia Web site: http://webopedia.com/DidYouKnow/Hardware_Software/2005/harddrive_format.asp

(2009). Evolving With Technology. Retrieved May 8, 2009, from National Crime Prevention Council Web site: http://www.ncpc.org/topics/fraud-and-identity-theft/fraud-and-identity-theft/evolving-with-technology

AccessData's Forensic Toolkit. Retrieved April, 2009, from AccessData A Pioneer in Digital Investigations Since 1987 Web site: http://www.accessdata.com/forensictoolkit.html

Carter , David (1995). Computer Crime Categories: How Techno -criminals Operate. *National Security Institute*, Retrieved May 7, 2009, from http://nsi.org/Library/Compsec/crimecom.html

Couglin,Tom & , Hughes, Gordon (2006, September). Tutorital on Disk Drive Sanitization. Retrieved April, 2009, from http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf

Datalossdb. Retrieved May 07, 2009, from DatalossDB Open Security Foundation Web site: http://datalossdb.org/

Federal Trade Commission. Consumer Sentinel Network Data Book (2009) Retrieved May 08, 2009 From http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf

Federal Trade Commission. Standards for Safeguarding Customer Information; Final Rule. 67 Fed. Reg. 36484 (2002) (to be codified at 16 CFR Part 314)

Fisher, Sharon (0006, May 08). Used Hard Drives Retain Data in eBay Sale. *PC World Magazine*, Retrieved March, 2009, from http://www.pcworld.com/article/125662/used_hard_drives_retain_data_in_ebay_sale.html

References Continued

Gallegos, Frederick (2005). Computer Forensics: An Overview. *Information Systems Audit Control Journal*, *6*, Retrieved May, 2009, from http://www.isaca.org/Template.cfm?Section=home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=27782

Garfinkel S. &, Shelat A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices. *IEEE Computer Society*, Retrieved March, 2009, from http://www.computer.org/portal/cms_docs_security/security/v1n1/garfinkel.pdf

Hailey, Steve (2002, April 2). What is Computer Forensics?. *Cyber Security Institute*, Retrieved May 7, 2009, from http://www.cybersecurityinstitute.biz/forensics.htm

Hildreth, Sue (2006, May, 04). Where hard drives go to die, or do they?. *Information Security Magazine*, Retrieved March, 2009, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1186300,00.html#

Kissel, R., Scholl, M., Skolochenko, S., Li, X. (2006). *Guidelines for Media Sanitization.* (NIST Special Publication 800-88) Gaithersburg, MD. National Institute of Standards and Technology.

Krebs, Brian (2007, July 5). Terrorism's Hook Into your Inbox. *Washington Post*, Retrieved May 7, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html

Mearian, Lucas (2009, February, 10). Survey: 40% of hard drives bought on eBay hold personal, corporate data. *Computer World Magazine*, Retrieved March, 2009, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=912771

Securities and Exchange Commission (2007). *SEC Interpretation: Electronic Storage of Broker-Dealer Records.* (to be codified at 17 CFR Part 241) Retrieved April, 2009, From http://www.sec.gov/rules/interp/34-47806.htm

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C.D., & Steinberg, D.I. (2008). *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (NIST Special Publication 800-66 Revision 1) Gaithersburg, MD. National Institute of Standards and Technology.

Spring, Tom (2003, April, 03). Hard Drives Exposed. *PC World Magazine*, Retrieved March, 2009, from http://www.pcworld.com/article/110012-2/hard_drives_exposed.html

References Continued

Spurzem, Bob (2009). *Sarbanes-Oxley Act*. Retrieved May 9, 2009,. From SearchCIO.com Web Site: http://searchcio.techtarget.com/sDefinition/0,,sid182_gci920030,00.html

Stevens, G. (2006) Data Security: Federal and State Laws. Congressional Research Service, Retrieved April, 2009, from http://www.asisonline.org/newsroom/crisisResponse/CRS_report0807.pdf

Zucker, Dr. Susan (2006). Cyber Forencis: Part I. *National Clearing House for Science, Technology and Law*, Retrieved May 7, 2009, from http://www.ncstl.org/news/ZuckerJan07