OVERVIEW & INTRODUCTION

SECTION A: RESEARCH, THEORY & METHODOLOGIES

SECTION B: PRACTICAL APPLICATION

OVERVIEW & INTRODUCTION

1.0 Document Overview

This document will examine computer forensics from both a theoretical and practical perspective. Section A will look at the former of these, researching and discussing the various aspects of computer forensics, including important methodologies, technical and practical considerations. Section B will document a series of live tests that I conducted in a virtualised environment, analysing the use of a variety of forensic tools and applications. While this document is primarily concerned with the technical side of computer forensics, the legalalities of the subject will be discussed briefly in Section C, as the legal considerations of the science are too significant an aspect to be ignored. Where relevant, reference has been drawn to examples of situations where various aspects of computer forensics have been applied.

2.0 What is Computer Forensics?

In order to properly examine any aspect of the digital world, it is important to fully understand what it is that you are examining. Essentially, computer forensics is the collection of means through which data can be found on a computer. By “means”, I am referring to a range of techniques, tools and applications, many of which will be discussed throughout the course of this document. The purpose of computer forensics usually comes down to a question of evidence, finding data that can prove some particular fact, usually pertaining to what a user has been doing on their computer. In this sense, this branch of forensic science is no different to that of its counterparts; it’s simply digital.

2.1 Uses of Computer Forensics

As was just noted, computer forensics are used to unconver proof of particular usage in digital environments. This is not always a question of criminal investigation; there are also civil, academic and professional reasons for using computer forensics. Dennis Lynn Rader, a notorious American serial killer, was convicted in 2005 after a lengthly investigation came to a head when disks he had sent to a police station were analysed. Contained on the disks were Microsoft Word documents taunting the authorities. By analysing the metadata contained in the documents, they were able to identify data created by a man named Dennis, and a link to the church at which Rader was a Deacon[1]. After a search that lasted three decades, it was the ability to analyse data that provided the critical piece of evidence. The use of computer forensics in criminal investigations such as the Rader case is commonplace. Cases involving the distribution and download of child pornography, for example. Through digital analysis of hardware, authorities can identify if an alleged offender has being viewing such material, even if the original data has been deleted from the hardware.

The ability to recover data spans across all fields. Civil disputes have often been dependent on the results of hardware analysis. One of the most famous civil actions in history was a consolidation of actions against Microsoft Corporation in the case, United States v Microsoft. Amongst the allegations against the software giant was numerous breaches of antitrust laws. Included in these were allegations that then Microsoft executive, Paul Maritz, now CEO of VMware, had claimed that the inclusion of a clone of the Netscape browser was an attempt at “cutting off the air” from their competitors[2]. While Maritz denied the allegations, subsequent analysis of deleted data uncovered an eMail suggesting the former vice president had in fact made such a statement.

Computer forensics, and the ability to recover data, also plays a part in academic and professional scenarios where legitimate data needs to be recovered, for example, from a corrupted HARD DISK . In summation, there are a vast number of reasons why we need computer forensics and its various applications, the aforementioned were just a taste of some examples of these.

SECTION A: RESEARCH, THEORY & METHODOLOGIES

The primary focus of this document will be an examination of technical aspects involved in the application of computer forensic techniques, as well as a practical demonstration of a selection of these. This section addresses the former of these two objectives; an examination of the technical aspects.

3.0 Computer Forensics Tools & Applications

[1] Douglas; Dodd, John. *Inside the Mind of BTK: The True Story Behind the Thirty-year Hunt for the Notorious Wichita Serial Killer.*
[2] US Dept. of Justice, Antitrust Case Filings. *United States v Microsoft. http://www.justice.gov/atr/cases/ms_index.htm*

The evolution of technology progresses at an immensely rapid pace; because of this computer forensics tools and applications must be constantly updated. The techniques involved in computer forensics are, in response to advancing methods of data destruction and concealment, becoming increasingly complex; the tools involved must facilitate this. There are a number of considerations to take into account when choosing which tools to opt for. Firstly, as computer forensics can often entail specifics, it is important to know exactly what it is that you are trying to achieve. Is the aim to uncover hidden or deleted data, or are you trying to reconstruct corrupted information? There are countless scenarios to be considered, such as the platform to be analysed, whether the file system is FAT, NTFS, ext4 or any other of the various file systems in use today; all of these considerations, and more, must be taken into account when choosing computer forensics tools.

The functions of computer forensics tools can be defined in five categories[3].

Acquisition
Validation and discrimination
Extraction
Reconstruction
Reporting

One of the primary functions of many computer forensics tools is data acquisition. Essentially, data acquisition is the process of copying digital evidence from disks, and while it sounds trivial, it does hold considerable importance in computer forensics, and with that carries a higher degree of complexity. With this in mind, data acquisition techniques will be is examined in more detail later in this document.

Validation and discrimination are two major concerns of analysts when it comes to computer forensics. Firstly, they must ensure validation; the integrity of data being copied. Secondly, there is the issue of discrimination; the process of filtering data. Without tools that offer validation, analysts may be facing issues of data loss and corruption, and as can often be the case, there may not be a second chance to acquire the necessary data. Many modern computer forensics tools ensure data integrity so as to avoid such issues through the use of various methods of validation, such as obtaining SHA-512 and MD5 hash values. Discrimination features within computer forensics tools provide a major convenience for analysts. When examining data, there

[3] Nelson, Bill; Phillips, Amelia; Enfinger, Frank; Steuart, Christopher. *Guide to Computer Forensics and Investigations (Second Edition).*

are large volumes that are irrelevant to the analysis or investigation. By utilising discrimination features in tools, analysts can avail of such processes as verification of header information, effectively allowing them to filter the data so that they are only provided with what it is that they are interested in.

Extraction of data is more difficult than the aforementioned functions, and so tools incorporating such features are usually more expensive. In computer forensics, extraction of data refers to the ability to recover data from some secure or corrupted location; think of the analogy of air lifting a crew from a stranded vessel. Most tools aid in the extraction of data by providing a number of features, particularly data viewing, and what is known in computer forensics as salvaging, or carving in some circles. Tools facilitate data viewing for extraction through a variety of means, but one popular method is to provide a view of a disk drive's logical configuration and a hexadecimal view of a drive's clusters and sectors. Salvaging is when tools analyse unallocated areas of disk space for file specific fragments, which in turn allow for the extraction of full structures and data streams. Extraction tools also feature a number of tools often found to be in use by malicious users. Computer forensic tools will offer their users functions such as brute-force attacks, in the event of an investigator having to overcome some form of encryption in order to get at the data that is required for analysis.

Tools which facilitate reconstruction have become more common with the emergence of more sophisticated methods of data corruption and deletion. Reconstruction tools provide the facility to do two things; copy and rebuild data. Essentially, a reconstruct function could be used to simply create an exact clone of a disk's partition. This is very helpful in computer forensics, particularly in criminal investigations, or in situations where several investigators or analysts all need individual original copies of the hard disk for examination. While comparable to acquisition, reconstruction features within tools are slightly different, and not to be confused. Acquisition is specific to data bytes and streams, while reconstruction is effectively copying an entire configuration, inclusive of data. It is essentially the same as cloning. More advanced tools will offer the secondary reconstruction feature of combining; allowing various acquisitions and clones to be reconstructed into a near exact replica of a corrupted system, often beneficial in situations where the hardware involved has been damaged to the extent that the data can be extracted, but the configuration itself is beyond repair.

Then, of course, there is always reporting. Because of the nature of the situations in which computer forensics is used, strict reporting is often required. To facilitate this, many tools will offer integrated reporting features, which will create logs of what was found through the analysis, what steps the investigator took during the analysis, as well as translate and create representations of non readable data so that they can be displayed and viewed for reporting purposes.

3.1 Hardware

The hardware used in computer forensics varies greatly dependent on the type and complexity of the analysis in question. Several vendors offer a variety of standalone devices, while other's provide integrated configurations; essentially complete computer forensics hardware suites for investigators and analysts.

3.1.1 Standalone Devices

Password Decryption Device

Data needed for analysis, particularly when indictable, will more than likely be, if the user of that data is any way computer competent, encrypted. Developed by Digital Intelligence, the Rack-A-TACC[4] is a typical example of a hardware device used in computer forensics for decryption; often a necessary step before the successful retrieval of data can occur. The device is comprised of four TACC1441 accelerators. Designed by Tableau, the TACC1441 is a hardware accelerator whose use increases decryption speeds by a multiple of 60[5]. Let's just take a few simple examples to illustrate how this can aid a forensic investigation. Forcefully decrypting information can be extremely difficult, and without sufficient hardware, effectively impossible. There are also certain types of encryption that can only be cracked with extremely powerful machines, which are themselves often beyond the budget of national agencies and law enforcement. For example, the US National Security Agency (NSA) is the cryptologic intelligence unit to the US Government, which controls one of the world's most powerful supercomputers, requiring 8000 tonnes of water just to keep it cooled. This computer, referred to as "the Thinking Machine", can decrypt 70 quadrillion keys in a few seconds[6]. "Roadrunner", stationed within the NSA controlled Los Alamos National Laboratory, can do 1,000 trillion calculations per second. But resources

[4] Forensic Devices, Digital Intelligence. *http://www.digitalintelligence.com/products/rack-a-tacc/*

[5] Forensic Computers, Inc. Tableau TACC1441 Hardware Accelerator. *http://www.forensic-computers.com/TACC1441.php*

[6] Discovery Channel production entitled *Super Computer*.

offered by such mammoth configurations found within the Thinking Machine and Roadrunner aren't available to law enforcement agencies, even in larger countries, but that is not to say that they are stranded. With the likes of Racc-A-TACC and TACC accelerators, data won't be decrypted in seconds, but it will be decrypted. Take for example, 128-bit encryption. In 128-bit encryption, which simply computes as 2^128, there are a possible 3.39×10^{35} different keys. To a normal computer, that would require an immense amount of calculation. But a computer forensics systems, with say, 10 Rack-a-TACCs, which would in turn contain 40 TACC1441 accelerators. That would improve the speed of the system's ability to decrypt by $1.33674945 \times 10^{71}$. Vendor specifications claim that the device can retrieve 105,000 Microsoft Office passwords per second, and WinZip passwords at 2,500,000 passwords a second. This is effectively a gain of 180 times that of what one would get from an average quad core processor, per single TACC[7]. Of course, decryption requirements will vary from situation to situation, but this is just an example of the power afforded to computer forensic investigators by decryption devices currently on the market.

Forensic Duplicator

There is a range of forensic duplicators on the market at the moment, each being offered by various vendors. Examples of such are the ImageMASSter Solo 3 Forensic Duplicator[8], and the TD1 Forensic Duplicator[9]. Forensic duplicators are designed to aid in data acquisition. They are essentially portable imaging tools that can both acquire and replicate data at very high rates. The TD1, for example, can sustain rates of up to 6GB/min, meaning that it could replicate 600GB of data in approximately 10 minutes. Most forensic duplicators, particularly the newer models, would support data acquisition from a variety of differing drives types, the most common of which would usually be either IDE, SATA or SCSI. They can also replicate across drive types, for example, from IDE to SATA, so investigators and analysts needn't worry about the specific drive to be examined. Forensic duplicators come with a range of additional features to aid in computer forensics. Data can be hashed and verified during the acquisition process to ensure integrity, audit logs can be automatically generated, and newer models also have the capability to overcome edited HPA and DCO configurations on

[7] Forensic Devices, Digital Intelligence. *http://www.digitalintelligence.com/products/rack-a-tacc/*

[8] MetaRescue.com, Hard Drive Forensic Duplicators. *http://www.metarescue.com/servlet/Detail?no=2*

[9] Tableau.com, Products, Forensic Duplicators *http://www.tableau.com/index.php?pageid=products&category=duplicators#galBottom0*

disks. Altering a disk's HPA (Host Protected Area) and DCO (Device Configuration Overlay) are two methods through which data can be hidden on a hard drive[10]. The majority of hardware manufacturers incorporate both of these into their disks. HPA sets a hidden partition, or in the case of some vendors, like Dell for example, a recovery partition, which is present in case there is a need to restore the system to its factory settings. DCO is used to limit available space on disks, but being somewhat more vendor dependent than HPA, is not as common. Using either of these, an advanced user can hide data from detection. While this method of hiding data does involve some level of advanced computing skills, it is essentially a simple complex. As both the HPA and DCO are system specific protected partitions, by altering the configuration so that the user can store data within them, this data will be hidden from even the most thorough of hard disk analysis. Most new forensic duplicators take this into account, and include functionality to overcome such configurations and acquire relevant data even from the HPA and DCO.

Read / Write Blockers

Also referred to as forensic bridges, read / write blockers are essential to data acquisition as they ensure that data is not damaged during the process. As their name would suggest, they do this by ensuring data cannot be altered, by allowing only read commands to pass through them, hence the comparison with a bridge. They can be either set to accept all of the user-specified commands, or block all write commands. When in write mode, all writes are prevented from reaching the attached device. Either way the end result will be similar; the specific scenario itself will usually dictate which method is best. An example of a popular read / write blocker used in computer forensics at present would be the T35e-RW Forensic SATA/IDE Bridge[11]. Not all forensic bridges would be both read and write blockers. Many of them would be just write blockers, with the added read blocking functionality, which isn't always completely necessary, being sacrificed to save on cost. More expensive write blockers will include integrated USB and Firewire write blockers.

[10] Data Destruction Topics, Accessing HPA and DCO Areas on Hard Drives. *www.destructdata.com*

[11] Tableau.com, Products, Forensic Bridges, Forensic SATA/IDE Bridge. *http://www.tableau.com/index.php?pageid=products&model=T35e-RW*

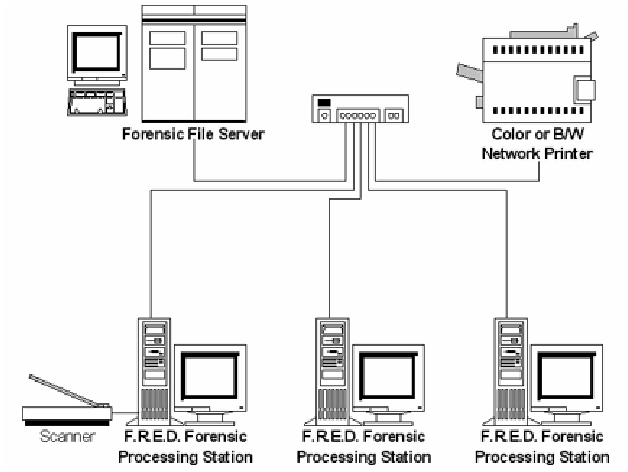
3.1.2 Integrated Configurations (Forensic Workstations)

FRED (Forensic Recovery of Evidence Device)

For the purpose of discussing integrated hardware configurations used in computer forensics, I will be taking the Digital Information's line of devices known as FRED, as an example case study. As already noted, integrated configurations take all of the standalone devices required in computer forensics and bring them together into a single complete hardware configuration. Essentially, integrated configurations are the workstations of computer forensics. FRED, and its many incarnations, is a typical example of one of these, produced by Digital Intelligence, a US corporation who are currently one of the world's largest providers of computer forensics hardware. As seen in the above imagery, FRED comes in numerous different configurations, each one designed to address differing levels of forensic complexity. Each system is essentially comprised of the same components, and as one goes up the scale, all that really occurs is an increase in the hardware capabilities and the volume of devices incorporated into the unit. For example, FRED, the base unit, will have one removable SATA hard drive bay, while FRED SR, the highest model, will have multiple bays for this drive type. Processing speeds and hardware specifications will also differ accordingly, similar to any workstation. Typically, FRED, and all similar integrated computer forensic systems by under vendors, will incorporate all of the aforementioned standalone devices (decryption, forensic duplicator, write block), a number of removable hard drive bays and both HPA and DCO support as discussed. FRED also has a portable solution, called FREDDIE.

The choice between opting for standalone devices or an integrated computer forensic workstation like FRED is dependent on the needs of the investigator. While standalone devices offer portability and cost, integrated configurations offer a more complete package and superior forensic power. However, they may also have more than is required by an investigator or analyst, who by opting for standalone devices, can ensure they are only paying for what they need.

3.1.3 Forensic Networks



In scenarios where computer forensics forms part of a major operation, for example, in some law enforcement operations, the forensic capabilities of standalone devices and integrated systems alone may not be sufficient to meet the technical requirements. With this in mind, forensic investigators and data analysts, looking to combine and share forensic resources to increase productivity, have developed forensic networks[12]. A forensic network would be comprised of a number of systems like FRED, all joined together over a high speed network. They would also be connected to a server, so that all of the investigators and analysts involved in the forensic process could share resources and data, such as imagery and disk replications.

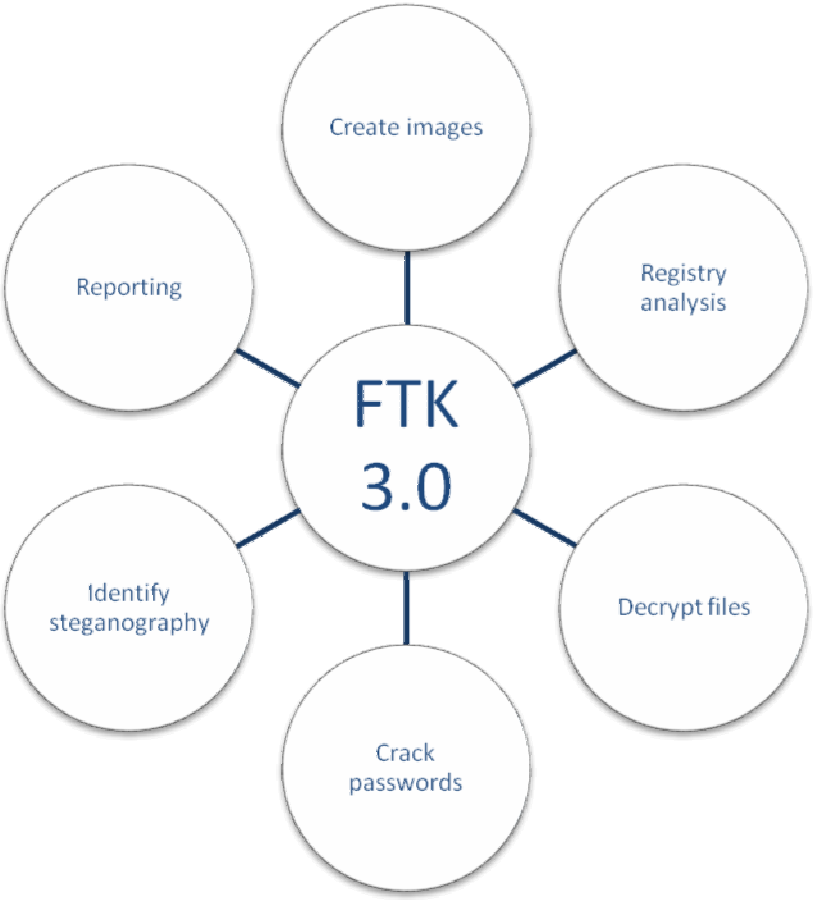
3.2 Software

As was the case with hardware, there is a whole range of software tools available for use throughout the various aspects of computer forensics. There are considerably more vendors offering computer forensics software solutions as opposed to hardware. Market leaders include Digital Intelligence, already mentioned as a chief computer forensics hardware provider, Nuix, AccessData, Paraben, Guidance Software and Technology Pathways.

Differing software applications will provide varying features and functions, but AccessData's FTK (Forensic Toolkit) is typical of what one can expect from computer forensics software, so provides a valid case study for examination. The application's latest release, FTK 3.0, can be

[12] Forensic Network, Digital Intelligence. *http://www.digitalintelligence.com/products/forensic_network/*

used to achieve both acquisition and analysis of data, offers decryption and password cracking features, and is court-validated, so appeals to investigators and analysts involved in the computer forensics of both criminal and civil actions[13]. FTK integrates all of the base requirements of any computer forensics investigation, as illustrated in the following diagram.



From this diagram, it is plain to see that FTK, and other software tools like it, offer a completed integration of all the necessary functions of computer forensics. The importance of creating images has already been discussed, while registry analysis is key to the locating of sensitive data when dealing with a Windows environment. Decrypting files and passwords is a chief consideration when looking at the question of gaining access to data, while the ability of such tools to identify steganography takes considerable strides against the ability of users to masquerade and hide the data that the investigator or analyst may be looking to recover. The reporting feature, as already noted, is hugely beneficial in this field of computing, as due to its

[13] AccessData.com, Forensic Toolkit 3.0. *http://www.accessdata.com/forensictoolkit.html*

frequently high legal nature, proper procedures, methods of documentation and reporting regulations must be adhered to.

Computer forensics software also offers an advantage in relation to power, similar to the forensic network mentioned in Section 4.1.3. Using such software as FTK, investigators and analysts are able to draw on idle CPUs across networks when performing decryption or brute force attacks. By harnessing resources across a network like this, the chances of success are significantly increased. Computer forensic labs can use this to deploy a shared resource approach known as distributed processing, as well as collaborative analysis. With the advent of more sophisticated methods of masquerading data, the need for such a combined effort is increasing.

Many of the features offered by computer forensics hardware devices would also be offered by software solutions, such as write blocking and the inclusion of large collection of hashes to ensure integrity. However there are other features that cannot be offered by hardware, such as PDE (Physical Disk Emulator), available on Guidance Software’s EnCase, a popular forensic application very similar to FTK in functionality, that provides the ability to emulate an exact hard drive replication in a read-only environment and mount hard drives in virtual environments[14].

Computer forensic software tools offer their users the ability to “carve”, an industry term for filtering. The ability to carve makes a huge difference to any digital analysis, simply because it allow the investigator to focus specifically on the data they are concerned with, saving valuable time and resources. Computer forensic software allows users to carve allocated and unallocated data, as well as set parameters such as data type and size. Most applications will also feature an increased rate of indexing so that searches and results are presented to the user as quickly as possible.

For specific in-depth analysis of data, computer forensics software is a must. Conducting RAM dump analysis for example, would not be possible without it. RAM dump analysis is the process of capturing data from memory, providing a whole range of information valuable within computer forensics, such as passwords. FTK’s RAM dump analysis analytics also offer the enumeration of all running processes, including those hidden by rootkits[15].

[14] Encase Forensic Total Offering, PDF available from Guidance Software. www.guidancesoftware.com

[15] AccessData.com, Forensic Toolkit 3.0. *http://www.accessdata.com/forensictoolkit.html*

Computer forensics software applications have had to evolve with the devices on which data can be processed. In the past, computer forensics was concerned chiefly with desktops and workstations, but now, there are mobile phones, PDAs and other portable devices to consider. Most MP3 players can even store general data now. The leading software suites have taken this into account. EnCase has modules that allow it to be used on mobile and smart phones, as well as several other portable device types.

3.2.1 NIST CFTT, FS-TST & NSRL

NIST (National Institute of Standards and Technology) is a US Department of Commerce body responsible for the measurement of standards in relation to advances in technology. It is a non regulatory body, but its high levels of funding and quality scientists and engineers has made NIST one of the world's most respected standards institutes.

Due to the nature of computer forensics, it is imperative that errors are avoided in its operation. With this in mind, NIST have developed their CFTT (Computer Forensics Tool Testing) project with an aim to ensure an appropriate standard against which computer forensics tools, primarily software, can be measured. Essentially, the CFTT project has provided a method with which we can sufficiently test computer forensic tools. This methodology was outlined in 2001, in a document entitled "General Test Methodology for Computer Forensic Tools"[16]. The short document outlines the approach to testing computer forensics tools as follows[17];

1. Establish categories of forensic requirements
2. Identify requirements for a specific category
3. Develop test assertions based on requirements
4. Develop test code for assertions
5. Identify relevant test cases
6. Develop testing procedures and method
7. Report test results

[16] Tool Testing Documents, NIST CFFT. *http://www.cftt.nist.gov/testdocs.html*

[17] NIST, *General Test Methodology for Computer Forensic Tools*, Version 1.9, Section 3.0: Approach.

Testing computer forensics tools is paramount to the success of the field. As it is such an exact science, and one whose success often carries with it serious criminal and civil consequences, simply opting for the most popular suite is not sufficient. The NIST CFTT has been developed so that those engaging in computer forensics, particularly law enforcement authorities, can test each application to ensure that it meets their requirements. By getting several demos of differing tools, and applying CFTT to each of these, a far more informed decision can be made. Computer forensics software is not like selecting an eMail client. Failure to choose the right one may see a criminal walk free, or a large corporation's data stolen and destroyed.

NIST has also developed FS-TST (Forensic Software Testing Support Tools) which looks to evaluate disk drive imaging tools, available from the same location as their CFTT, entitled FS-TST: Forensic Software Testing Support Tools. After downloading the tool, users can issue a number of commands that will automate the evaluation process of imaging process on computer forensics applications. Once again, through using this tool, those engaged in computer forensics can ensure that the software they are using for their investigations and analysis are performing to the required level.

Finally, NIST have developed NSRL (National Software Reference Library). NSRL uses what an RDS (Reference Data Set), which is a collection of hash values from known software applications, to help analyse the files on a computer by matching profiles based on these hashes[18]. Version 2.14 of the NSRL's RDS has over 11 million unique hash values. Being freely available, like all of the NIST projects, NSRL has been provided the foundation for many of the hash functions within today's most widely-used computer forensics applications. However, the project does have its failings; for example, it cannot help in the detection of certain illicit data, such as pornographic material featuring minors, as such data does not contain hash values.

4.0 Locating Sensitive Data

Before looking at more complex forensic analysis techniques, one must consider the more simple question; where are the default locations in which you can find sensitive data? Oftentimes, complex methods of analysis are not required to find the necessary data, but a

[18] National Software Reference Library, Project Overview. *http://www.nsrl.nist.gov/Project_Overview.htm*

knowledge of where to look for such data is. If the user has not attempted to properly erradicate the data, it will most likely be in one of the following locations[19].

- **Cluster tips**

  Hard disks are divided into small 512 byte physical storage segments called sectors. Sectors are then group consecutively to form clusters, usually consisting of 2^3 (8) sectors. Clusters are, essentially, where a system's data is stored. On many platforms, depending on the filesystem and allocation method, clusters will be dedicated to data from a single file, raising issues of fragmentation. If a file is 3.2 kilobytes (3,276.8 bytes) in size, and stored within a 4 kilobyte (4096 bytes) cluster, then 819.2 bytes will be left unused within that cluster. The problem that this raises in relation to the location of sensitive data, is the way in which operating systems, particularly Windows, will use this space. On systems where sufficient RAM is not present for maximised efficiency of operation, the remaining cluster space will be utilised for the storage of data that does not need to be in volatile memory. The idea behind this is that increased RAM will be released for use elsewhere, and that the data stored within the cluster will be overwritten as necessary. However, this is not the case, as most platforms will not attempt to store data in this unused cluster space if it isn't sufficient in size. Instead, they will opt for the next block, which in turn, leaves the original piece of sensitive data residing in the cluster. For a forensic investigator, this presents an opportunity to locate sensitive data on a machine, with such a configuration, without the need for complex analysis.

- **Free space**

  A common misconception amongst those who aren't very technically competent is that placing a file in the Recycle Bin will delete the data. It won't. By the same token, several alternative methods of deletion, for example, issuing the `del` command in DOS-based platforms, also do not delete a file. Rather, they simply mark the file as no longer needed and flag the section of the disk that the data occupies as available for use by other data in the future, allocating it as "free space". By looking in this free space, a forensic investigator could uncover a significant amount of data that an unsuspecting user may have considered to have been deleted. More advanced users will know that to truly delete a file, put it beyond the bounds of less complex methods such as this, the space on which that data once resided must be overwritten with data of any form, even

[19] Caloyannides, Michael A. *Privacy Protection and Computer Forensics (Second Edition).*

nonsensical (which is the method adopted by many of today's most widely used file removal toolkits).

- **Swap file**

  The opportunity that the swap file presents for the location of sensitive data is not unlike that of the aforementioned cluster tips. The difference is that, in the case of the clusters, the data in question did not need to reside specifically in volatile memory. In this case, the data does require volatile memory. However, situations will arise on systems where the amount of RAM available is insufficient to the requirements of the current tasks. A swap file addresses this issue, by allocating space on the hard disk as virtual memory. Essentially, this is the operating system pretending that the system has more RAM than it actually does. An effective solution to the problem that it seeks to address, the use of a swap file gives rise to a similar issue as with the cluster tips; data that was never intended to be stored on the hard disk is. This method of data recovery is becoming less prevelant as volatile memory becomes increasingly inexpensive and greater volumes are being install in systems. As the amount of RAM available to users increases, the need for a swap file will decrease in congruence. The installation of Windows Vista on many under resourced systems did give rise to a resurgence in the use of swap files, but the advent of Windows 7 has lessened this trend somewhat. Nonetheless, it still remains a very effective way for a forensic analysis to locate sensitive data on a system without the need for any of the more complex techniques.

- **Non-magnetic disks**

  The rise in popularity of non-magnetic disks has led increased need for forensic analysis to be carried on such storage devices as USB memory keys and flash memory cards found in electronics such as digital cameras. Non-magnetic disks suffer from the same issue as that of their magnetic counterparts. The data from deleted files continues to reside on the disk until such time as new data rewrites it. The chief difference between this type of storage and traditional magnetic hard disks found in most computer systems is that their lower levels of storage space usually mean that deleted data is overwritten within a shorter period of time.

- **History files**

One of the simplest means of conducting an investigation in computer forensics is the analysis of history files. A lot of current software packages and applications will create history files of the data and actions traversed by the user, sometimes over a considerable length of time. Once again, the opportunity that this presents for a forensic investigator to conduct an analysis without the need for complex techniques is dependent on the competency and precautions of the user in question, as simply disabling such functions is not a difficult task for anyone with even a modest knowledge of computers.

- **Spool files**

  Before a file is printed, they undergo a process known as spooling. This essentially puts the file to be printed within a spool file, that is used to queue the file for printing. If the user deletes the file from the hard disk after printing is complete, a simple forensic analysis will still be able to uncover the data, as it will still exist within the spool, unless removed by the user or specific system configuration. This is a popular method within computer forensics used in the pursuit of individuals downloading child pornography. Posessing limited knowledge of computers, they print off the illicit images, before then deleting the soft copies, thinking that they have covered their activity.

5.0 Computer Forensic Techniques

Having looked at both the hardware and software that can be put to use in computer forensics, as well as their functionality and reasons for using such, this section will look at three more of the primary issues that computer forensics is concerned with. These are recovering deleted data, string searching and registry reconstruction.

5.1 Recovering Deleted Data

Recovering deleted files is a major part of computer forensics, as it is relevant to all branches of the science. The need to recove data that has previously been deleted, intentionally or otherwise, is a requirement in criminal, civil, corporate and academic situations. There may be malicious reasons behind the destruction of data, such as a person facing a criminal charge for the possession of illicit material attempting to destroy evidence, or legitimate reasons, or more accurately mistakes, like a secretary or a student accidentally deleting some important files. But why data needs to be recovered is irrelevant, whether it be for criminal or corporate chargse makes little odds to this examination, the important thing is that it *can* be recovered. Various tools that allow for the recovering of data after more “permanent deletes” will be demonstrated in Section B, the practical examination, of this document, but here it is important to fully understand why it is that files can be recovered in the first place. Combined, Windows and Unix pretty much make up 99.9% of the world’s operating systems. There are of course others, but they aren’t widely used. Windows-based systems are hugely popular amongst both personal and corporate users, while all of the remaining platforms, namely the numerous Linux distributions, Solaris, and the Macintosh operating systems, are all Unix-based. In both Windows and Unix-based platforms, when you delete a file, depending on your current location within the operating system, it will do either one of two things; it will either move the file to the recycle bin, or it will delete the file. If it is the former of these two steps, recovering the data is hardly and act of overly complex data recovery; you simply have to restore it from the desktop. However, if the file is deleted directly, which happens in the case of all files deleted from the DOS prompt, Unix terminal or any files on removable media, or if the recycle bin, or trash in the case of most Unix-based systems, is emptied, then the recovery becomes somewhat more complex, particularly if the aforementioned spooling technique doesn’t suffice. When a file is deleted, it is not destroyed, it is simply removed, in its entirety, from its current location and placed in a hidden folder, in some unoccupied space on the hard disk. It is then issued with a new filename, usually based on an alphanumeric sequence, and its indexing erased. However, added to the data will be a byte of information, recording in which will be the original name and path of the file. It will then reside at this location until it is overwritten by some new data, even if the operating system is completely wiped. As will be seen in Section B of this document, it is possible to locate and recover deleted data based on this premise.

Recovering image files can be complex, but is an important part of computer forensics, particularly with the advent of broadband and a rise in the distribution of such contrabands as illicit pornographic material. For the purposes of computer forensics, it is important to understand the categorisation of imaging formats into bitmap, vector and metafiles. Bitmaps are images that are made up of pixels, while vector images are mathematically based definitions of geometric shapes. Metafiles are a combination of the two. You need to understand the differing types of image files for the purpose of salvaging. If trying to recover a deleted image file, you may need to salvage, which means recover pieces, of that file, and identifying file fragments is easier when you understand the data pattern of the file that is fragmented. This is where the ability to distinguish between pixellated and geometric shapes proves useful. Recovering data fragments will be demonstrated in Section B. Once this has been done, the image file can be recovered. However, it will more than likely have a damaged header due to the fragmentation. Repairing damaged headers is the final step in recovering deleted image files, and can be done by comparing hexidecimal values between the damaged header and that of a similar image of the same format. Take JPEG for example; all images in this format will have a header value of FF D8 FF E0 00 10, so know this allows for the header to be fixed, as well as provides a way of identifying what kind of format an image is. JPEG images will also contain the hex value 4A 46 49 46, which is represented by ASCII as JFIF, which in turn, allows us to identify any fragments containing JFIF as JPEG files[20], allowing for more efficient recovery.

5.2 String Searching

Using the string searching technique, forensic investigators and analysts will be able to search for data, even when they don’t know what it is that they are looking for. Take for example, a stolen credit card number. When analysing the suspect’s hard drive, there is no way of knowing what kind of format the data was stored in. Did the suspect keep the credit card number in an eMail, or a Microsoft Word document, or a .txt file? The list of possibilities is numerous. Through the use of string searching, data can be searched for on the basis of a tiny stipend of information, in this case the credit card number. Essentially, you are filtering based on key words and phrases, not unlike how Windows conducts a search for indexed files, but in this case, the data may be deleted or hidden. String searching works off the premise of complex algorithms. The Boyer-Moore Fast String Searching Algorithm is one example of an algorithm that is widely utilised amongst computer forensics circles. Developed by Bob Boyer and J Strother Moore in the late 70s, essentially finds one string of characters in another[21]. The algorithim works off of the concept of pattern alignment, which is why it has proved so succesfull in computer forensics, where oftentimes data fragments and recovered bytes are so small and seemingly irrlevant. But with this algorithm, even the smallest of data fragments can be used to string search and find other pieces of relevant data. Sticking with the example of the credit card, I have devised the following example to demonstrate the use of the Boyer-Moore algorithm in string searching.

[20] Nelson, Bill; Phillips, Amelia; Enfinger, Frank; Steuart, Christopher. *Guide to Computer Forensics and Investigations (Second Edition).*

[21] RS Boyer, A Fast String Search Algorithm, *Communications of the Association for Computing Machinery, 1977*.

1. Take this random sequence of 16-digits as a representation of a typical credit card number: 6983 3476 9603 2184. All we have to go on is this number; no other knowledge of where the relevant data might be or what format it is in. All we have is this 16-digit string of characters.
2. The algorithm will take the credit card, and treat it as a single entity within a data pattern. As the credit card number doesn't change regardless of where it is stored, it will remain a constant throughout all of the data on the hard disk.

3. The binary sequence 11011 will represent the credit card number's 16-digits as a single constant character string.

4. The algorithm will apply 11011 to the data found on the hard drive. Say for example, the following is representative of a .txt file;
   101011100101000101001001011101001100101010**11011**00101011101000111101011

5. Within the data, the algorithm will match the string, providing the investigator with a file in which the data string is contained. However, in this case, the entire data was available. Say that only a fragment of the data is available, as is often the case when recovering data that has been destroyed. In this scenario, only the green fragment may be available;
   101011100101000101001001011101001100101010**11011**00101011101000111101011

6. Even though the data is fragmented, the algorithm will work on the premise that it is searching for a known pattern in an unknown string. Firstly, it will move toward the end of the string, in this case, producing the following pattern;
   01100101 **x**
   This is not a match, so it will move in the other direction, searching through the other data for a pattern that will fit. Even though it is not contaiend within the fragment; all it cares about is searching for the string. This will match the pattern and the string.
   0101010**11011**00101
   This in turn provides the other part of the fragmented file, and the data in which the incriminating evidence containing the credit card is found.

5.3 Registry Reconstruction

The ability to reconstruct data in computer forensics allows investigators to prove beyond doubt that a certain action was taken on a computer. Because of the popularity of the Windows operating system, one of the chief concerns in computer forensics is recontructing the platform's registry, the files required for the system to function properly.

Windows stores its registry files in a binary format that is propriatory to Microsoft. Because of this, registry files cannot be simply opened and viewed with a text editor or any other type of application for that matter. The system critical registry files are located in the system32 directory, and include user.dat files which contain information on a user's actions, as well as the files that they have used. Reconstructing this data, so as to avail of the valuable forensic information that it contains, is complex, and involves software such as the aforementioned FTK or EnCase, but worth the while from an analytic perspective. With these, identifying programs that have been uninstalled is possible through parsing, as they leave uninstallation information within one of the registry keys. It is also possible to determine most recently used documents. This comes from the functionality within most software to recall "most recently opened" files for user convenience. Even after software is uninstalled, the entry that this feature makes into the registry remains in existence. By using both of these techniques, a forensic investigator could prove a lot about the programs and files that a user has or had on their system.

6.0 Overcoming Forensic Techniques

If one is to understand how to perform a success forensic analysis of a system, they must understand more than the techniques and the tools involved. They must understand how it is that both of these will be avoided, so that that very purpose can not be fulfilled. This document has already established that deleting a file will not erradicate the data and put it beyond the reach of a recovery. But their are methods that can be taken to do so. Obviously, the best way to put data beyond recovery is to physically destroy the disk on which it is stored beyond all repair. This does not just include mechanically, it is crucial that the sectors themselves, the plates in the disk, are physically destroyed. Simply smashing a hard drive with a hammer may leave the disk intact. By destroying the surface of the disk however, data will be destroyed beyond all repair. Wiping a disk does not destroy data, it can still be recovered, the principles of why having already been discused. There are a number of disk wiping software solutions out there that claim to wipe disk completely clean. While they may succeed in erradicating most of the data, because of the fact that most modern hard drive hold sectors in reserve, which they can't touch, they won't destroy all data, just some.

Hiding data can be, at times, as effective as destroying it, particularly if a user doesn't want to do physical damage to costly hardware. Here there are three options; making a file invisible, disguised or unreadable. Making a file invisible hides its very existence, while disguising it hides it in plain site, as would be the case in steganography. The best example of making a file unreadable would be to use encryption, though the ability of computer forensic tools to overcome this has already been examined. Compression is a technique often ignored by users that wish to hide data, but can prove effective, as shrinking a file will make it unrecogniseable from its original form or expected parameters.

Other techniques that can be used would be to intentionally change file extensions. For example, change a .jpeg file to a .xls file. Forensic analsysts looking for illicit imagery may not concern themselves with files in .xls format. After the examination the format can be reverted back to its original. However, while this technique may fool a novice investigator, more experienced analysts may deploy the string search technique discussed in Section 5.2, which would overcome this precaution.

SECTION B: PRACTICAL APPLICATION

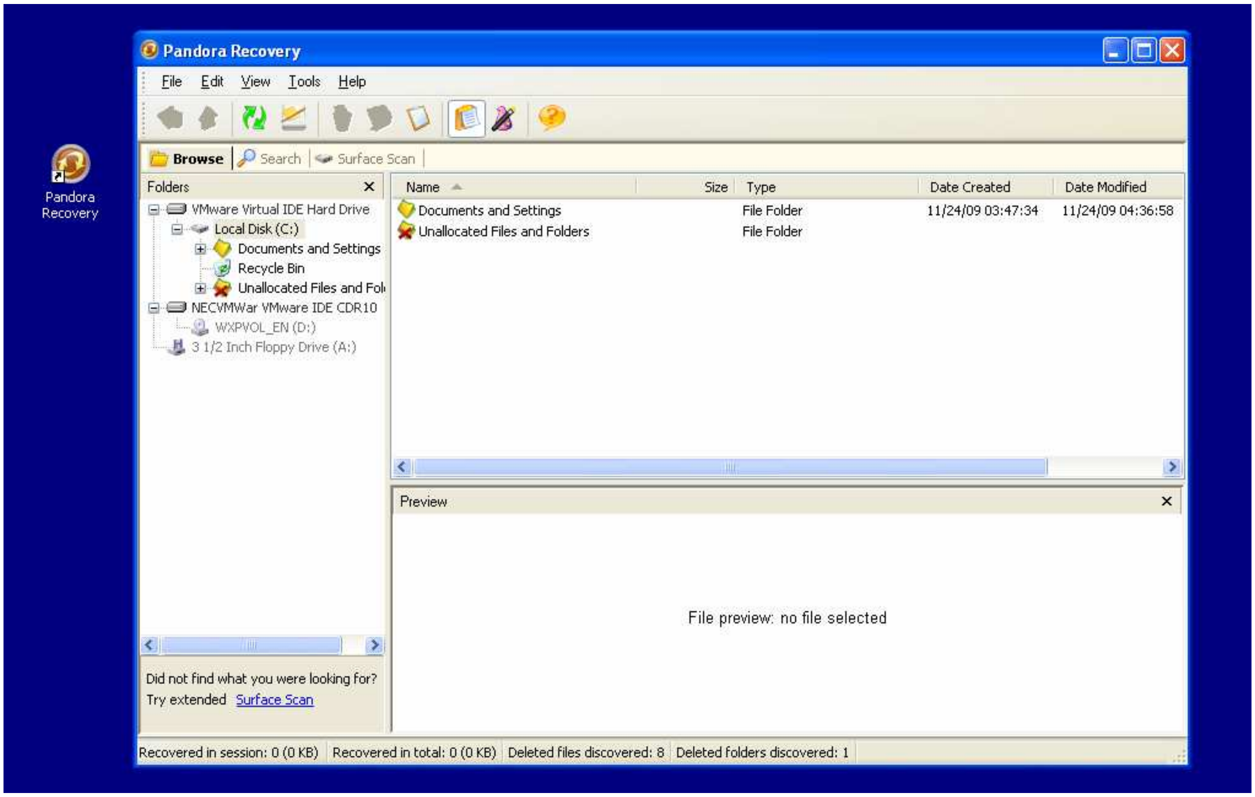
This section will take a more practical approach to the examination of computer forensics. Many of the aforementioned theories and methodologies will become clearer when demonstrated in a practical sense. Computer forensics is a "hands-on" science, and so this section will afford a better opportunity for a more in-depth technical analysis and demonstration of the various processes involved in computer forensics.

This practical examination took place in a virtualised environment, using Windows XP Professional and Debian 5.0. While FTK and EnCase are the most widely-used applications in computer forensics, the commercial nature of these has prompted me to opt for open source alternatives.

7.0 Recovering Deleted Data

At this point, we have discussed several times the importance of being able to recover deleted data through the use of various computer forensic tools and techniques. For the purposes of this particular practical application, I opted for the use of Pandora Recovery on Windows XP.

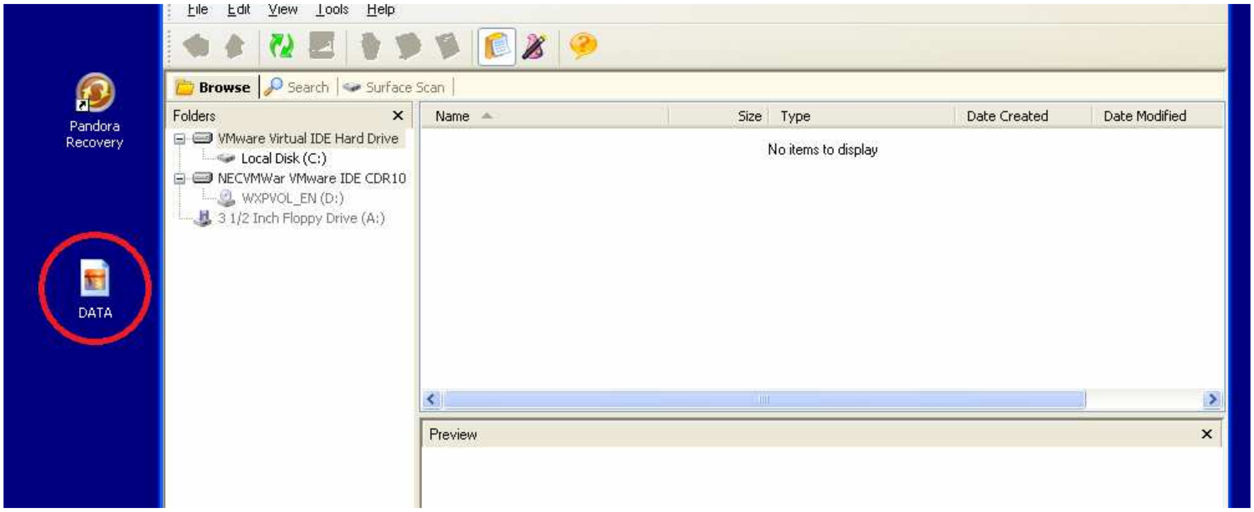
Pandora Recovery is compatible with all Windows NT-based operating systems, which includes XP and Vista. Able to recover data on fat16, fat32, ntfs, ntfs5 and efs file systems, Pandora even boasts the ability to recover some files even after they have been overwritten in memory. The following image shows Pandora's main dialog box after the software has been launched.


Pandora Recovery
Pandora Recovery
File
Edit
View
Tools
Help
Browse
Search
Surface Scan
Folders
VMware Virtual IDE Hard Drive
Local Disk (C:)
Documents and Settings
Recycle Bin
Unallocated Files and Fol
NECVMWar VMware IDE CDR10
WXPVOL_EN (D:)
3 1/2 Inch Floppy Drive (A:)
Did not find what you were looking for?
Try extended Surface Scan
Preview
File preview: no file selected

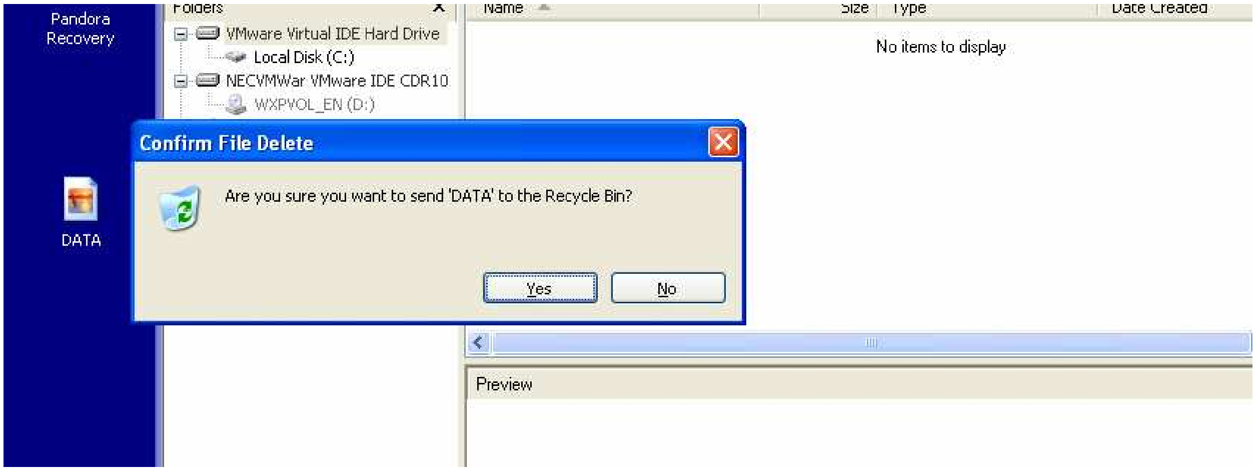
Name	Size	Type	Date Created	Date Modified
Documents and Settings		File Folder	11/24/09 03:47:34	11/24/09 04:36:58
Unallocated Files and Folders		File Folder		

Recovered in session: 0 (0 KB) | Recovered in total: 0 (0 KB) | Deleted files discovered: 8 | Deleted folders discovered: 1

For the purposes of this demonstration, I have created a file called DATA, as seen in the following image. It is simply an image in .jpeg format, of the CIT crest. Having created the file, I deleted it, and then deleted it from the recycle bin, "permanently" removing it as far as the user is concerned. The first thing that Pandora Recovery will do is check to see if data is in the recycle bin, which will not be the case here; the file has been completely deleted.

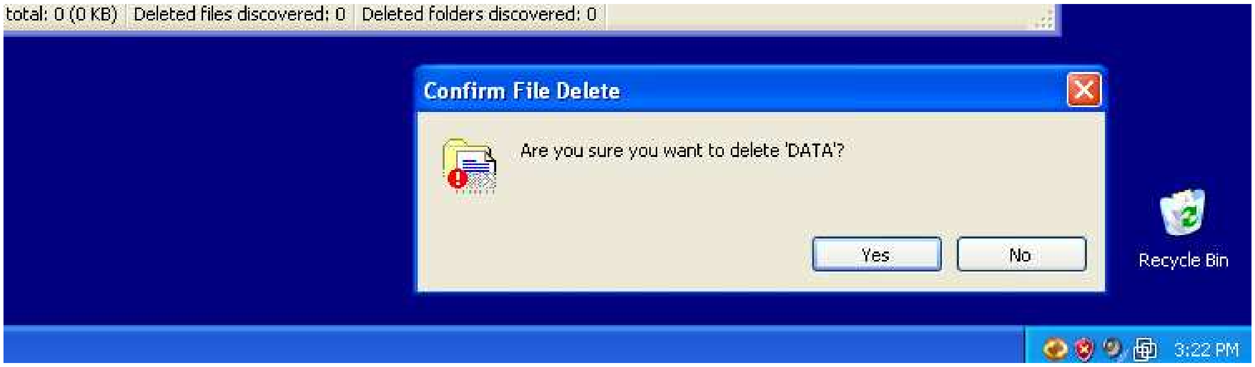


No items to display



No items to display

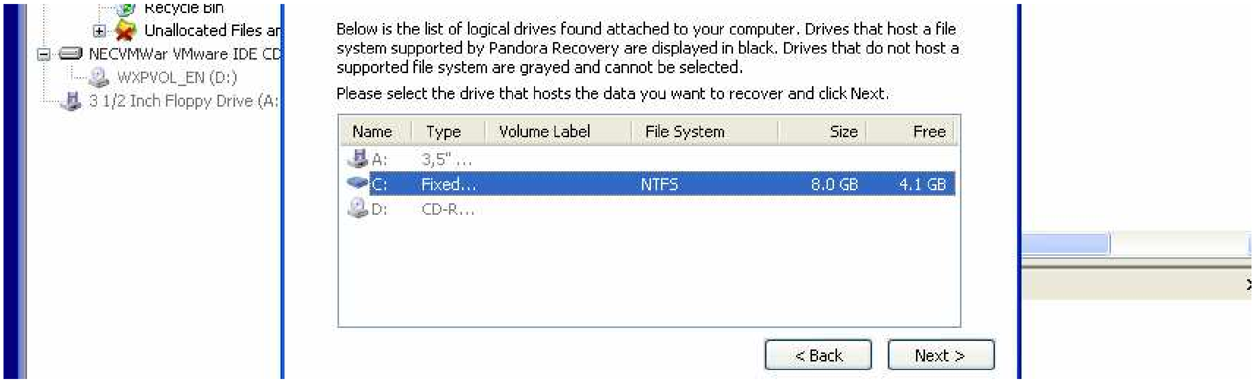
Are you sure you want to send 'DATA' to the Recycle Bin?



total: 0 (0 KB) | Deleted files discovered: 0 | Deleted folders discovered: 0

Are you sure you want to delete 'DATA'?

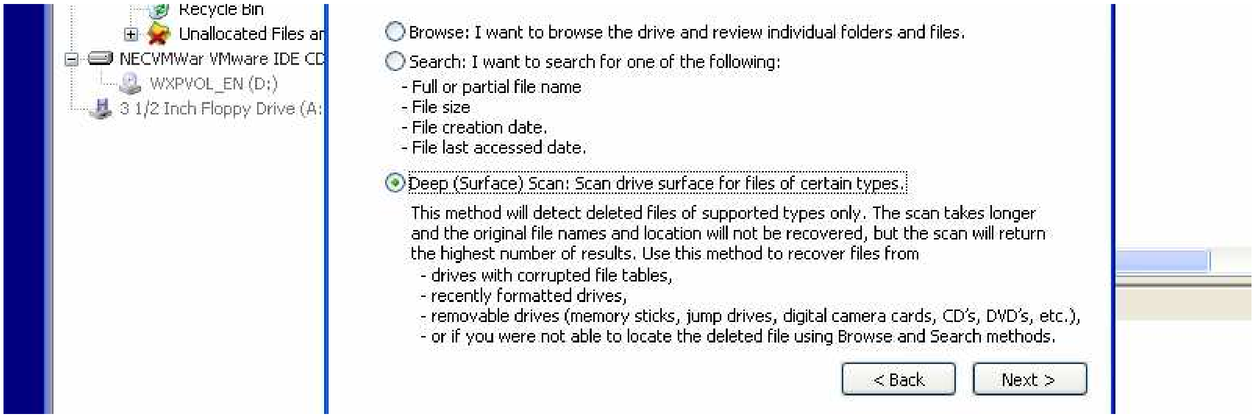
Once this has been done, I went to Pandora to start a deep scan of my disk. Pandora's deep scans take into account reserve clusters, so can recover data even after a drive and has been formatted and an operating system reinstalled over the original data. The first thing to do when starting a scan is to select the drive in question, in this case the C: drive, which being Windows is using the NTFS file system, which Pandora supports. Having selected the drive, you then have a number of scanning options, but as the DATA file was permanently deleted, I opted for the deep scan.



Below is the list of logical drives found attached to your computer. Drives that host a file system supported by Pandora Recovery are displayed in black. Drives that do not host a supported file system are grayed and cannot be selected.

Please select the drive that hosts the data you want to recover and click Next.

Name	Type	Volume Label	File System	Size	Free
A:	3,5" ...				
C:	Fixed...		NTFS	8.0 GB	4.1 GB
D:	CD-R...				



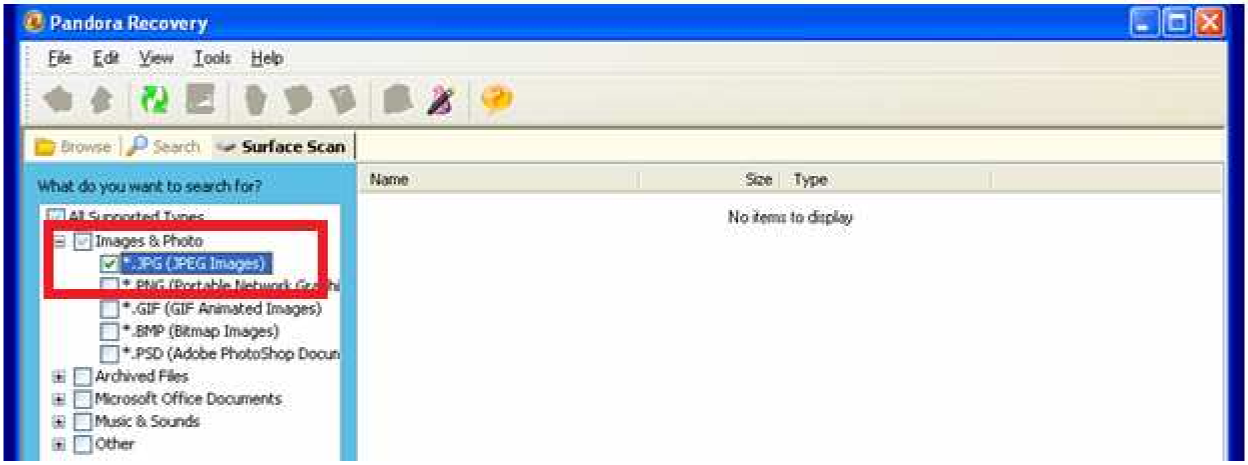
○ Browse: I want to browse the drive and review individual folders and files.

○ Search: I want to search for one of the following:
- Full or partial file name
- File size
- File creation date.
- File last accessed date.

● Deep (Surface) Scan: Scan drive surface for files of certain types.

This method will detect deleted files of supported types only. The scan takes longer and the original file names and location will not be recovered, but the scan will return the highest number of results. Use this method to recover files from
- drives with corrupted file tables,
- recently formatted drives,
- removable drives (memory sticks, jump drives, digital camera cards, CD's, DVD's, etc.),
- or if you were not able to locate the deleted file using Browse and Search methods.

If you want, Pandora then allows you to narrow the recovery parameters. As I knew the format of the file that I was truying to recover, I was able to narrow the criteria to save time.

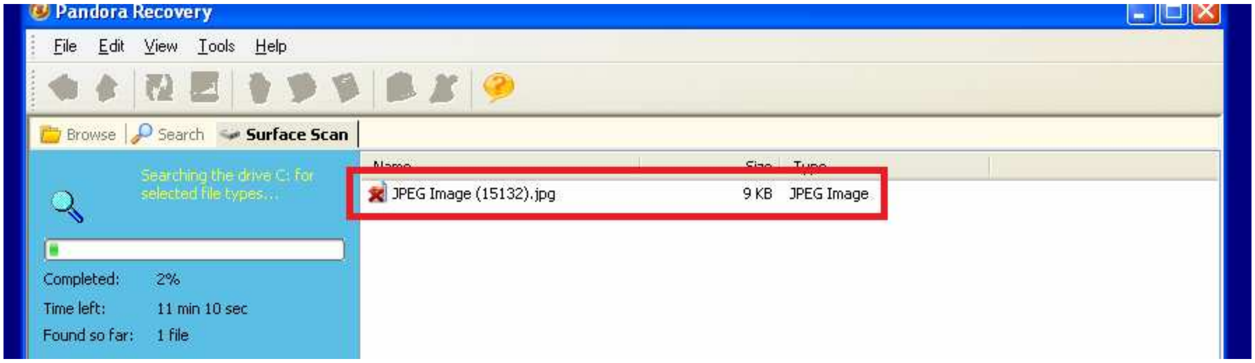


What do you want to search for?

- □ All Supported Types
  - ⊟ □ Images & Photo
    - ☑ *.JPG (JPEG Images)
    - □ *.PNG (Portable Network Graphi
    - □ *.GIF (GIF Animated Images)
    - □ *.BMP (Bitmap Images)
    - □ *.PSD (Adobe PhotoShop Docun
  - ⊞ □ Archived Files
  - ⊞ □ Microsoft Office Documents
  - ⊞ □ Music & Sounds
  - ⊞ □ Other

Name	Size	Type
No items to display		

This returned a 9KB JPEG image. The name of the image is not visible, which demonstrates the process by which files are stored when deleted using the INFO byte, as discussed in Section A of the document.



Searching the drive C: for selected file types...

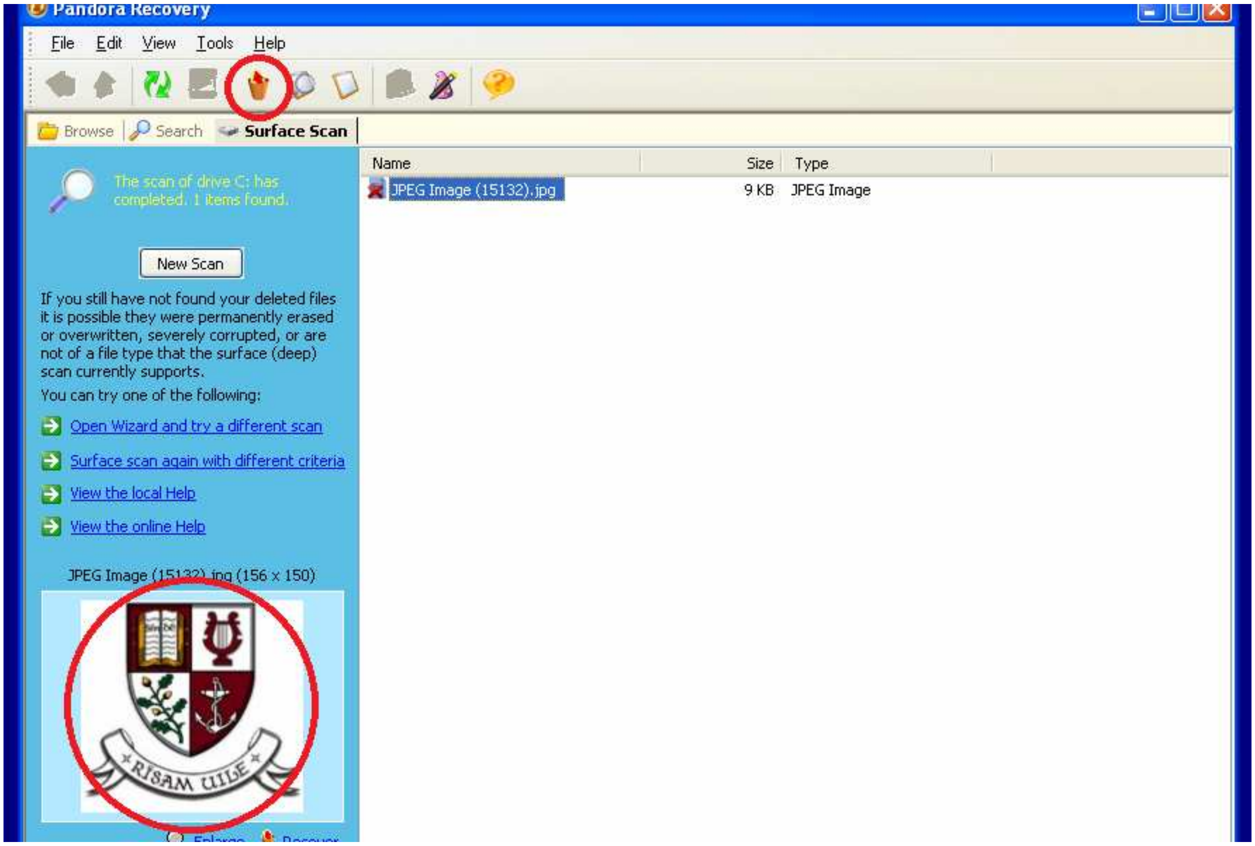
Completed: 2%

Time left: 11 min 10 sec

Found so far: 1 file

Name	Size	Type
JPEG Image (15132).jpg	9 KB	JPEG Image

However, Pandora does offer a preview of the file, so it is possible to identify, at least as far as imagery is concerned, what the data contains. Having identified this file as the correct one, I click recover, as highlighted in the following image, and Pandora attempts to recover the data.



The scan of drive C: has completed. 1 items found.

Name	Size	Type
JPEG Image (15132).jpg	9 KB	JPEG Image

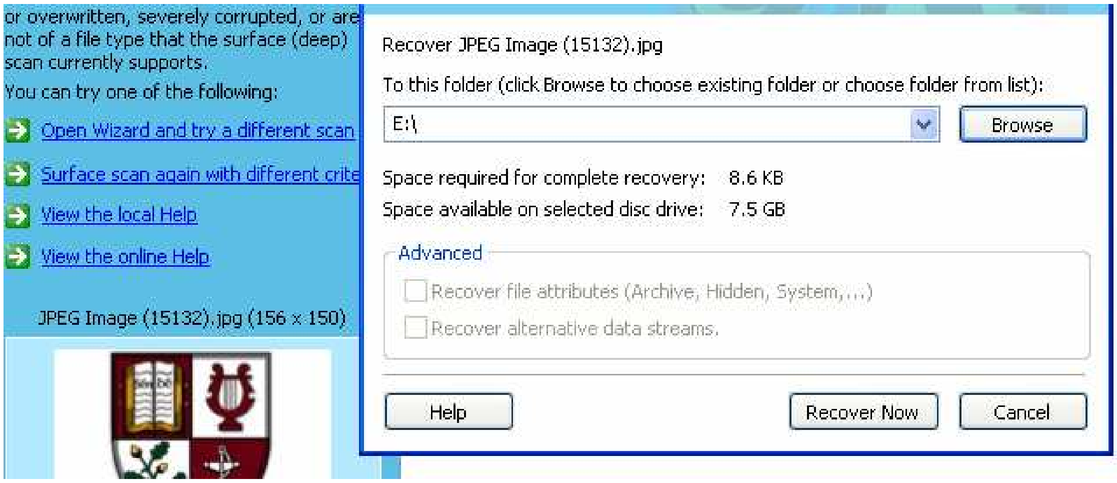
If you still have not found your deleted files it is possible they were permanently erased or overwritten, severely corrupted, or are not of a file type that the surface (deep) scan currently supports.

You can try one of the following:

- Open Wizard and try a different scan
- Surface scan again with different criteria
- View the local Help
- View the online Help

JPEG Image (15132).jpg (156 x 150)

When recovering data, it is worthwhile remembering that deleted data's worst enemy is new data being written to the same drive. This applies to recovery in the sense that, when recovering data, you run the risk of overwritting the data you want to recover with that same data during the recovery. To negate this risk, recovery of data should be done to a different drive to that of where the original data resided. With this in mind, when recovering data, Pandora offers the option to select the destination for the recovered data. As can be seen in the following image, to avoid the aforementioned risk I have chosen to recover the data to a portable USB drive.



or overwritten, severely corrupted, or are not of a file type that the surface (deep) scan currently supports.

You can try one of the following:

JPEG Image (15132).jpg (156 x 150)

Recover JPEG Image (15132).jpg

To this folder (click Browse to choose existing folder or choose folder from list): E:\

Space required for complete recovery: 8.6 KB

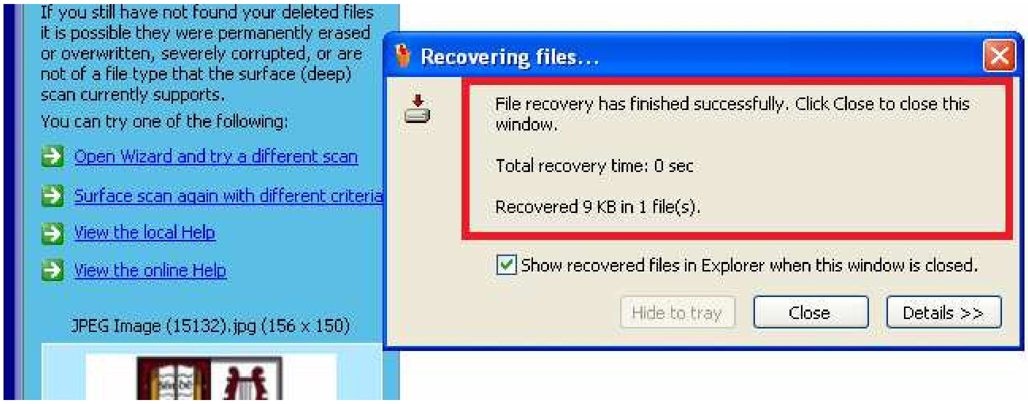
Space available on selected disc drive: 7.5 GB

Advanced

□ Recover file attributes (Archive, Hidden, System,...)

□ Recover alternative data streams.

Open Wizard and try a different scan
Surface scan again with different crite
View the local Help
View the online Help
Browse
Help
Recover Now
Cancel



If you still have not found your deleted files it is possible they were permanently erased or overwritten, severely corrupted, or are not of a file type that the surface (deep) scan currently supports.

You can try one of the following:

JPEG Image (15132).jpg (156 x 150)

Recovering files...

File recovery has finished successfully. Click Close to close this window.

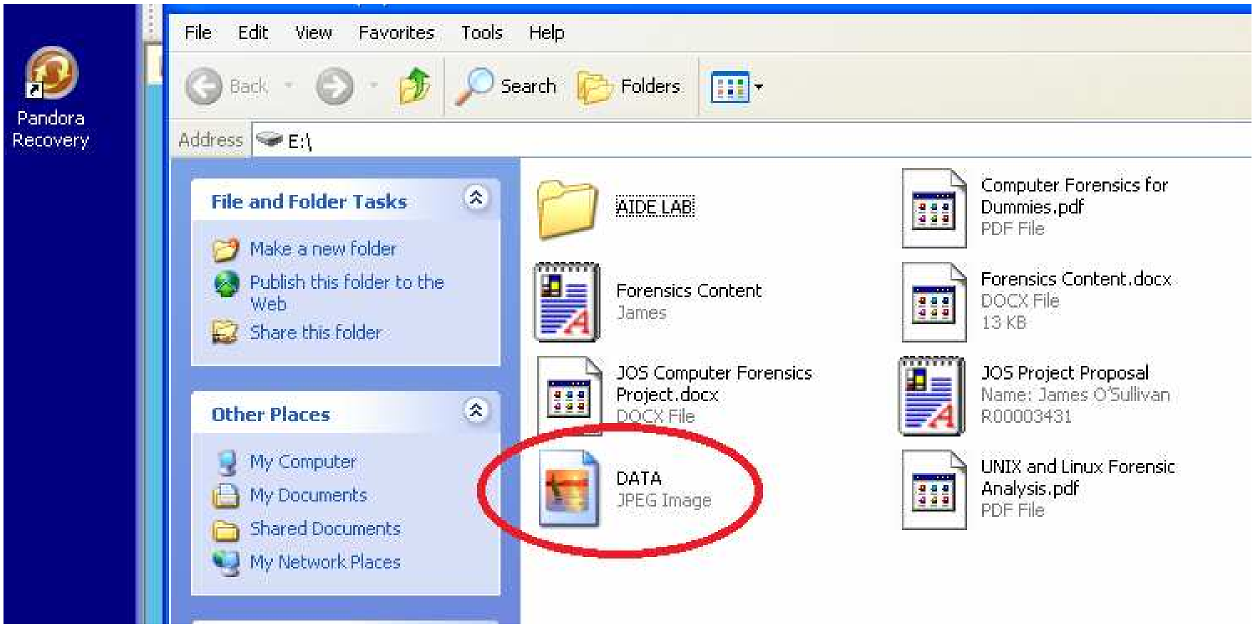
Total recovery time: 0 sec

Recovered 9 KB in 1 file(s).

☑ Show recovered files in Explorer when this window is closed.

Open Wizard and try a different scan
Surface scan again with different criteria
View the local Help
View the online Help
Hide to tray
Close
Details >>

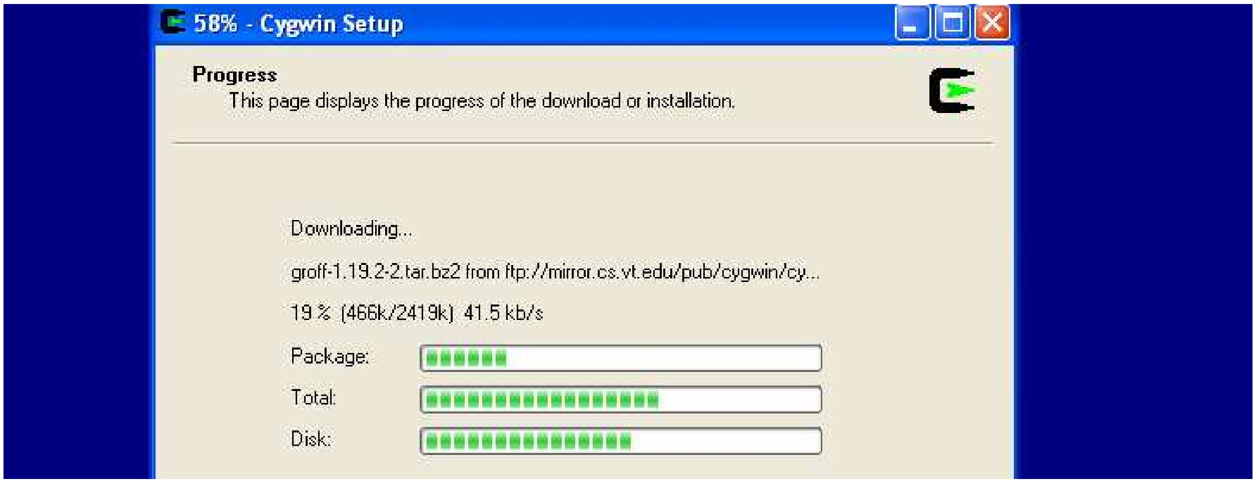
As can be seen from the following image of the E: drive, the file has been sucessfully recovered, even though it was “permanently” deleted.



8.0 Web Browser Activity Reconstruction

The ability to reconstruct data in computer forensics allows investigators to prove beyond doubt that a certain action was taken on a computer. The volume of illegal and unauthorised activity that involves use of the Internet is incredibly high, and it increases every day. In many cases, regardless of whether they be criminal, civil or corporate, the alleged offence will have in some way involved browsing the web. With this in mind, being able to reconstruct web browsing activity is a must for those operating in the field of computer forensics. There are a number of computer forensic tools which can be utilised in reconstructing web browsing activity; I have chosen to use two of the more popular open source forensic web activity reconstruction and analysis tools, Pasco and Galleta. There is a reason for using both tools in conjunction; Pasco will be used to parse the information in the index.dat file, while Galleta will handle the cookies. I have also chosen to use the Internet Explorer browser for the demonstration. I have chosen this over other browsers as Internet Explorer saves a lot of the files that we want to analyse in Microsoft propretry format, making the task of analysis that bit more challenging. Internet Explorer's .dat files contain much of the information on a user's web activity, and so will be a focus of the analysis. Cookies are small files placed on the local system by a web server for various reasons. Analysis of cookies can also shed light on a user's web browsing activity, as will be seen.

Using Pasco and Galleta in a Windows-based environment presents a problem; they are recommended for use on Unix-based systems. The lack of other effective opensource reconstruct tools prevents simply turning to an alternative. However, it is possible to using Cygwin to run the files in Windows. Cygwn is Unix-based environment that runs in Windows by emulating a Linux API[22]. Within this emulated layer, applications that require Unix-based platforms, can run. So the first step in this demonstration was to install Cygwin in XP, and emulate the Unix-based environment.



Progress
This page displays the progress of the download or installation.

Downloading...

groff-1.19.2-2.tar.bz2 from ftp://mirror.cs.vt.edu/pub/cygwin/cy...

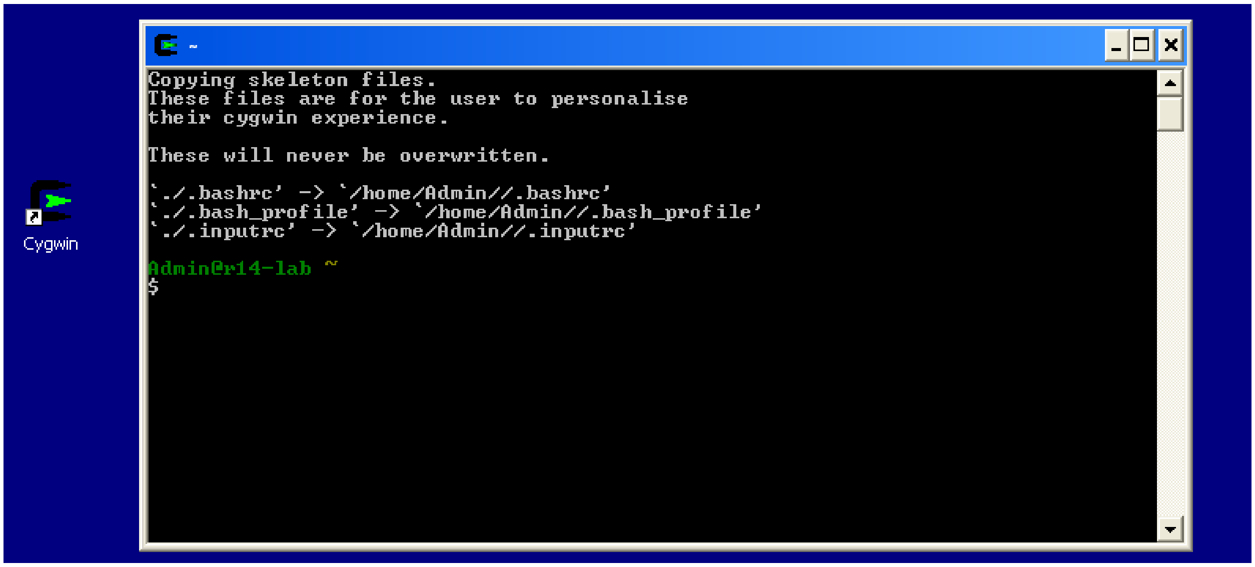
19 % (466k/2419k) 41.5 kb/s

Package:

Total:

Disk:

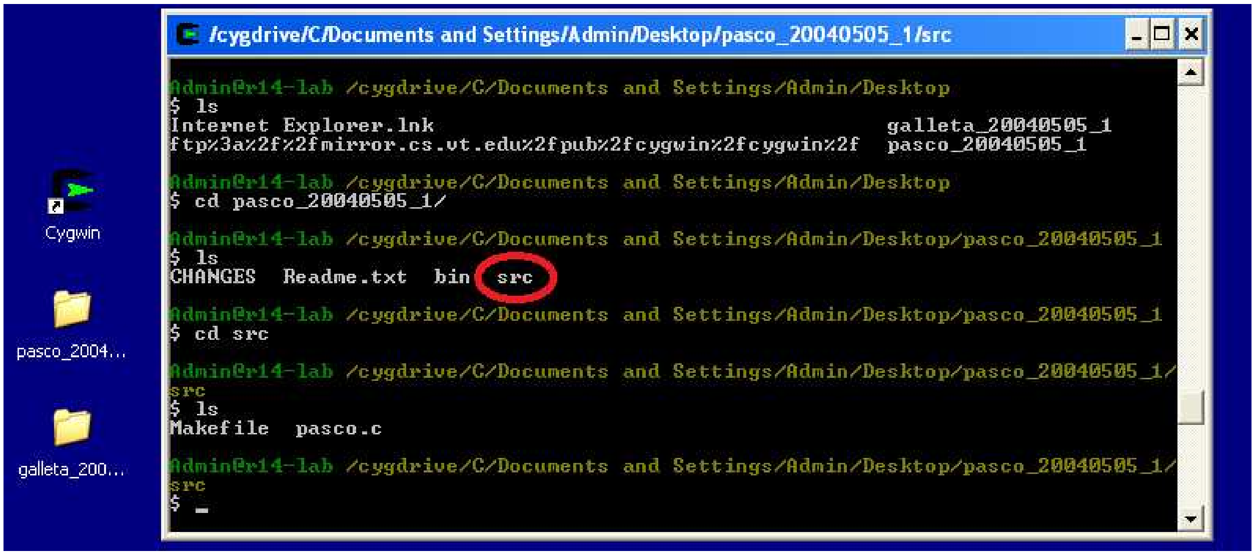
Once installed, Cygwin can then be run from within Windows, providing an emulated Linux API on which Pasco and Galleta will be able to function.



```
Copying skeleton files.
These files are for the user to personalise
their cygwin experience.

These will never be overwritten.

`./.bashrc' -> `/home/Admin//.bashrc'
`./.bash_profile' -> `/home/Admin//.bash_profile'
`./.inputrc' -> `/home/Admin//.inputrc'

Admin@r14-lab ~
$
```

[22] *http://www.cygwin.com/*

Once this has been done, Pasco and Galleta must be installed. The first step here is to download them to Windows. They can be downloaded individually as part of the Odessa beta[23]. Unzip, and then, from within Cygwin, navigate to Pasco' src directory so that it the program can be compiled as if it were functioning on a Unix-based platform.



/cygdrive/C/Documents and Settings/Admin/Desktop/pasco_20040505_1/src
Cygwin
pasco_2004...
galleta_200...

```
Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop
$ ls
Internet Explorer.lnk                                  galleta_20040505_1
ftp%3a%2f%2fmirror.cs.vt.edu%2fpub%2fcygwin%2fcygwin%2f  pasco_20040505_1

Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop
$ cd pasco_20040505_1/

Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop/pasco_20040505_1
$ ls
CHANGES  Readme.txt  bin  src

Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop/pasco_20040505_1
$ cd src

Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop/pasco_20040505_1/
src
$ ls
Makefile  pasco.c

Admin@r14-lab /cygdrive/C/Documents and Settings/Admin/Desktop/pasco_20040505_1/
src
$ _
```

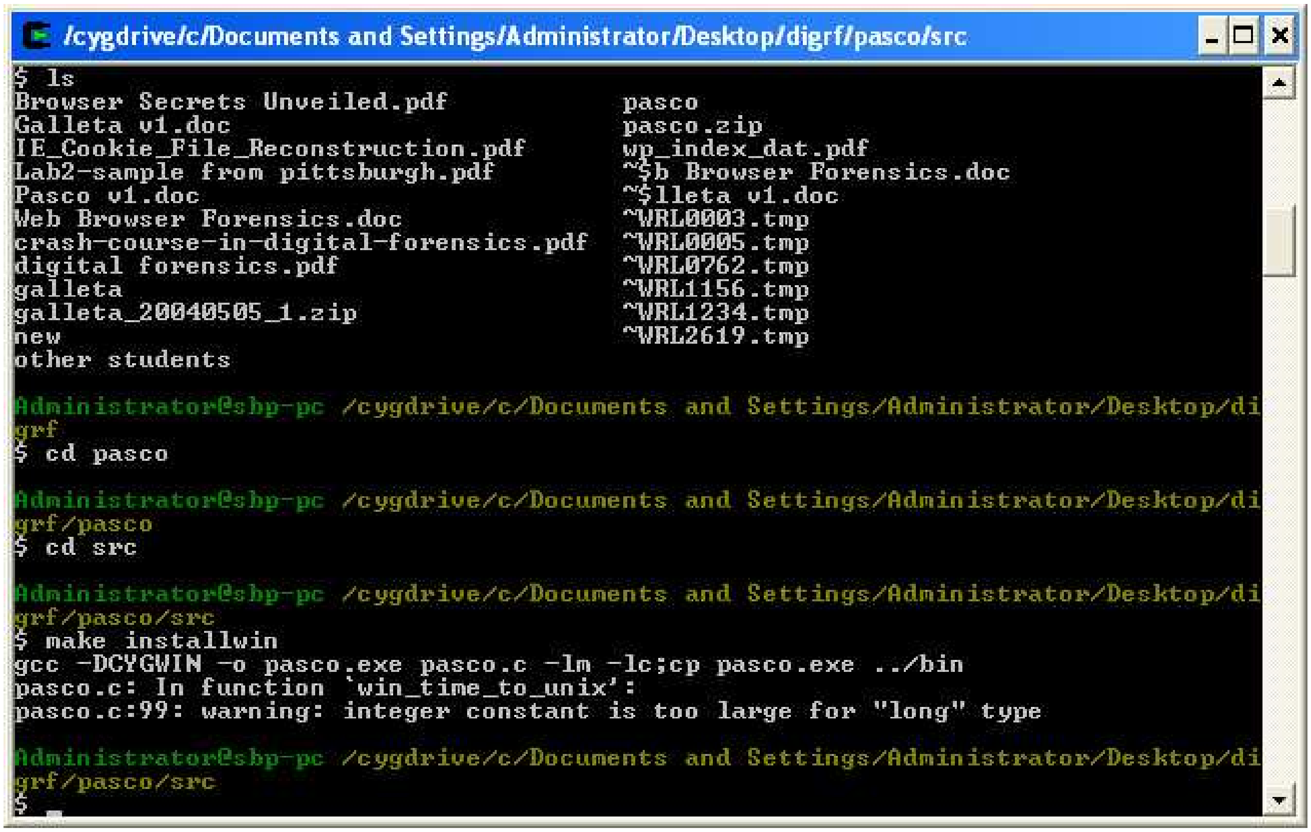
Before using, Pasco has to be recompiled from source.
To recompile from source:

- Enter the "src" directory.
- Type "make installwin" within Cygwin to make Pasco for Windows.

OR

- Type "make install" to make Pasco for Unix.

[23] *http://sourceforge.net/projects/odessa/files/*


/cygdrive/c/Documents and Settings/Administrator/Desktop/digrf/pasco/src

```
$ ls
Browser Secrets Unveiled.pdf           pasco
Galleta v1.doc                         pasco.zip
IE_Cookie_File_Reconstruction.pdf      wp_index_dat.pdf
Lab2-sample from pittsburgh.pdf        ~$b Browser Forensics.doc
Pasco v1.doc                           ~$lleta v1.doc
Web Browser Forensics.doc              ~WRL0003.tmp
crash-course-in-digital-forensics.pdf  ~WRL0005.tmp
digital forensics.pdf                  ~WRL0762.tmp
galleta                                ~WRL1156.tmp
galleta_20040505_1.zip                 ~WRL1234.tmp
new                                    ~WRL2619.tmp
other students

Administrator@sbp-pc /cygdrive/c/Documents and Settings/Administrator/Desktop/di
grf
$ cd pasco

Administrator@sbp-pc /cygdrive/c/Documents and Settings/Administrator/Desktop/di
grf/pasco
$ cd src

Administrator@sbp-pc /cygdrive/c/Documents and Settings/Administrator/Desktop/di
grf/pasco/src
$ make installwin
gcc -DCYGWIN -o pasco.exe pasco.c -lm -lc;cp pasco.exe ../bin
pasco.c: In function `win_time_to_unix':
pasco.c:99: warning: integer constant is too large for "long" type

Administrator@sbp-pc /cygdrive/c/Documents and Settings/Administrator/Desktop/di
grf/pasco/src
$ _
```

Figure 5 – Compiling Pasco from Source

The binaries will be located in the "bin" directory.

Using Pasco

The commands for using Pasco is relatively simple:

./pasco index.dat > index.txt

Once index.txt is created, the results can be imported into a spreadsheet like Microsoft Excel for further viewing, sorting, and formatting:

Installing Galleta

Before using, Galleta also has to be recompiled from source.
To recompile from source the procedure is similar to that for Pasco:

- Enter the "src" directory.
- Type "make installwin" within Cygwin to make Galleta for Windows.

OR

- Type "make install" to make Galleta for Unix.

Using Galleta

The commands for using Galleta are also relatively simple:

```
./galleta administrator@arstechnica.txt > arstechnica_galleta.txt
```

It is important to note that Galleta's output can be also be easily imported into your favorite spreadsheet program so that you may sort, search, and filter the data. Furthermore, a spreadsheet will allow you to format the data so that it is appropriate for a report.

Conclusion and Scope for Further Research:

Pasco and Galleta are both powerful tools that are indispensable to a forensic investigator tracking Internet activity. These tools automate the analysis of the Index.dat as well as cookie files generated by Internet Explorer. The main shortcoming of both tools are their lack of support for Internet Explorer 7 as well as Opera, Firefox and other non-IE browsers. Future research to develop both tools to work with other browser as well as Internet Explorer would extend their capabilities immensely. Extending the capabilities of both tools in this respect is is quite feasible given the open source nature of the source code. However, extending the tools to utilize native windows support would be beyond the scope of this project

BIBLIOGRAPHY

Literary Sources

Jones, Keith J.; Bejtlich, Richard; Curtis, Rose W. Real Digital Forensics: Computer Security and Incident Response. Addison – Wesley, 2006. ISBN: 0321240693.

Nelson, Bill; Phillips, Amelia; Enfinger, Frank; Steuart, Christopher. Guide to Computer Forensics and Investigations (Second Edition). Thomson Course Technology, 2005.
ISBN: 0619217065.

Caloyannides, Michael A. Privacy Protection and Computer Forensics (Second Edition). Artech House, 2004. ISBN: 1580538304.

Image Sources
http://www.digitalintelligence.com/products/rack-a-tacc/
http://toys4techies.com/images/solo3largeforensic.jpg
http://www.tableau.com/index.php?pageid=products&model=T35e-RW
http://www.digitalintelligence.com/preview.php?pic=/products/fred/images/fred_ubii_med.jpg&title=FRED
http://www.digitalintelligence.com/preview.php?pic=/products/freddx/images/freddx_ubii_med.jpg&title=FRED%20DX
http://www.digitalintelligence.com/preview.php?pic=/products/freddie/images/freddie_angle_med.jpg&title=FREDDIE
http://www.digitalintelligence.com/preview.php?pic=/products/fredsr/images/fredsr_med.jpg&title=FRED%20SR
http://www.digitalintelligence.com/products/forensic_network/