Computer Forensics – In Layman's Terms.

By

Simon Gibbons

About the author: Simon Gibbons has over 20 years of investigative experience in both a law enforcement and corporate environment. He has conducted countless investigations across Asia and has a wealth of experience in Computer Forensics. He has provided expert witness testimony in a number of different jurisdictions. Simon provides the computer forensic support and advice to LBG in Thailand. When he is not on assignment, Simon is busy building the first online community for Security Professionals. For more information please see www.clearviewsolutions.org/paladin.html.

Introduction - Invariably these days whenever there is a corporate investigation, especially fraud or intellectual property theft, it is only a matter of time before someone says, "Well, we better get those computer forensic guys in." When the forensic expert arrives, he removes a tool kit from his briefcase, lays it out carefully on the desk and then sets about surgically removing the hard drive from computer. Once it's removed, he holds it aloft to the heavens, letting out a maniacal laugh as the storm clouds circle and electricity fills the air. The forensics gods are once again appeased.....Whoa, hold on a sec - I got a little Harry Potter on you!!

Having said that though, to the non-tech savvy, computer forensics is shrouded in mystery and is regarded by many as a black box. In this article, I'd like to unmask the truths and reveal (some of) the magicians secrets. I'll spell out in layman's terms a few of the steps we take when we conduct a forensic investigation.

Imaging a Hard Drive - This is more often than not the first thing a computer forensic expert will do when they arrive at a job. Imaging a hard drive is more than making a copy of the files and folders that exist on a drive. Rather, it is a bit-for-bit transfer of data from one drive to the other creating an exact replica. It includes all the partition information, boot sectors, file allocation tables and the free space. (Hey, I thought we were going to use any geekspeak!!) Basically, when we image we get ALL the data, not just the files created by the user.

There is more than one way to skin a cat and the same goes for imaging a hard drive. Generally and where possible the drive is removed and placed in a portable imaging device. If that is not possible, then it is imaged whilst it is still in the computer. Each way has its purpose and its own set of advantages and disadvantages.

One of the first questions I am always asked is "How long will it take?" Well, let me explain.....

First some maths: A bit is the smallest area on a hard drive where data can be stored (remember we are imaging every single bit on a drive) 1 byte equals 8 bits and a kilobyte (KB) is a 1000 bytes[1]. For megabytes (MB) multiply by another thousand and for a gigabyte (GB) multiple yet again by another thousand. For Terabytes (TB), multiply.... Ok, I think you get the picture. Whew, we need to crack our knuckles after that one so here is a nice cheat sheet.

8 bits = 1 byte 1000 bytes = 1 kilobyte 1000 kilobytes = 1 megabyte 1000 megabytes = 1 gigabyte 1000 gigabytes = 1 terabyte etc, etc ,etc

"Yes, but I don't care about that. I just want to know how long will it take?"

Hmm, I thought I just answered that.... Well, suffice to say though that in today's laptops a 250GB hard drive can hold a mind-boggling amount of data. A 1GB USB thumbdrive can store approximately 20,000 typical word document pages, 640 photos or 64 MP3 audio files. On a 250GB drive that equates to 5 million pages which is about 22,000 copies of Aarons book "And Then one Morning" published by Big Wave Productions (A shameless plug!)

But how long?? In God's name, please just tell me how long it will take??!!!

I think you get my point by now. There are far too many variables including the size of the drive, the imaging method used and the amount of data stored on the original drive. Generally, when pushed for an answer, I say anything between 1 and 4 hours per computer, so it's important to bring a packed lunch.

[1] Ok, technically its 1024 bytes but unless you are a mathematician suffering from OCD, I'll spare you the exact formula. For now, lets just say 1000 and move on….

Sometimes, it can even be an overnight affair so a toothbrush is an essential piece of kit I also carry in my toolbag.

Verifying an image - Once the hard drive is imaged its important that the forensic expert ensures that they have obtained an EXACT replica (bit for bit) of the original drive. There is a whole plethora of complex mathematical computations behind this process that will make your head swim so I'll cut straight to the chase. It is the equivalent of taking a “digital fingerprint” of the two hard drives to prove that they are identical. Verifying can take time as well - anything from 1-2 hours is not unusual.

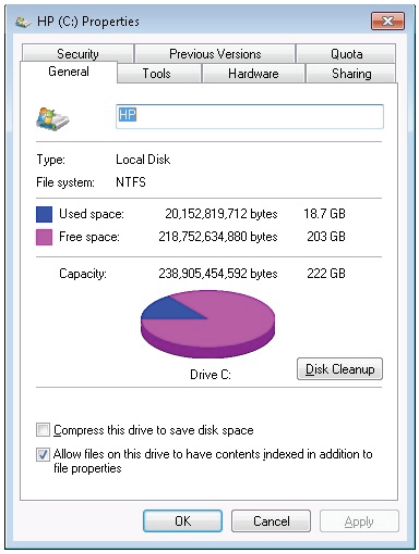
Obtaining the image in a “forensically sound” manner - this means that the data on the original drive has not been changed during the imaging process. Many people don't realise that whenever a hard drive is connected to a computer, depending on the operating system, data is written to the drive to prepare it for use. Forensic experts should always image a drive in a forensically sound method by using a write-blocking device. This is to negate any legal disputes that may arise where an astute lawyer may argue that the data was altered somehow and therefore not admissible as evidence.

Now that the hard drive has been imaged, its time to look at the analysis:

Recovering Deleted Files - One of the things I like to brag about to girls at parties (not that computer forensic experts get invited to many parties where there are girls!) is recovering files that have been "deleted". How do we do that? Well, here's the secret.... *When you delete a file from your computer it's not really deleted.*

Here is an analogy (did I mention Aaron wrote a book? – here comes plug number two!): I read "And Then One Morning" but didn’t like Chapter Ten and want to “delete” it. Rather than tearing the pages from the book, I simply erase Chapter 10 from the Table of Contents. Now, anyone who looks at the TOC no longer see Chapter 10 listed and will therefore assume that the chapter doesn’t exist. In its simplest form, this is the same concept of how an operating system deletes a file on your computer. Us clever computer forensics techies though, have software that allows us to flip through each and every page in the book bypassing the TOC. And guess what we find at page 45? Exactly, Chapter 10, in all its glory.

Free Space/Unallocated Clusters - The free space (sometimes called unallocated clusters) on a hard is the area that the operating system sees as being available to store more files and folders.



Free Space: the area that is available to store data on a hard drive

This is the Alladins cave of computer forensics and all sorts of previously existing files can be found here. No-one can say for sure exactly how the different operating systems and software applications use this free space, but needless to say there is a lot of files being temporarily stored there along with files you thought you had deleted years ago. Going back to the book analogy, even though you had deleted Chapter Two from the TOC, it would still remain in the free space until such time as the operating system decided to use those pages in the book to write new data.

How do we find data in free space? Every type of file (a word document, an email message, a spreadsheet, etc) has a signature that the operating system uses to determine which application should be used to open the file. With a little know-how, forensic experts can trawl through all the free space searching for those signatures and with a little trickery can recreate those files.

Conducting Keyword Searches - These days, forensic software can easily search through data for keywords in almost any language. People however sometimes fall into the trap of searching every conceivable word they can think of that may be related to the investigation. This normally ends up returning thousands of hits. Whilst this may be a thorough approach, the issue remains that someone with intimate knowledge of the case will need to review those results, particularly if it’s a technical matter. I’ve investigated cases

in the past where the keywords returned more than 5,000 files. A staff member of the client had to manually review each file to determine whether it was relevant to the case or not. So, be thoughtful of the keywords you use and work towards a shorter unique list rather than a generic one.

Alternatively, I prefer to take a more targeted approach. I will spend some time with the client to learn more about the investigation and what they suspect has occurred. For example, if it were a case where they think the offender was passing confidential information via an online chat program, I would begin with a keyword search focusing on areas where I would expect to find chat-room conversations. This effectively reduces the amount of data returned for review and can significantly save the clients time and money.

The Technical Report - I was brought up old school in the police where a forensic report was to contain enough technical mumbo-jumbo to confuse the defense attorney (read enemy) into not asking any questions in fear they may look like a fool. In a corporate environment this is counter productive. I learnt this the hard way when a lawyer once described my report as "technical and containing many esoteric terms difficult to comprehend." – and they were on MY side!!

Now, I still provide the technical details as it's important that the methodology stands up to scrutiny, however I distinctly separate these from the findings. The result, I hope, is a much easier to understand document. After all, in a corporate world all the client wants to know is what the offender did and how they did it. No-one really cares that the hard drives spins at 7200RPM or that BIOS clock settings were 0.06 seconds slower than GMT. That may only become relevant if any of the evidence is contested. The information is still important to collect but not necessary information that a corporate client needs to be aware of.

In summary, computer forensics is becoming more and more mainstream in corporate investigations and should be considered early to avoid loosing valuable evidence. Forensics experts have a few tricks up our sleeve to unearth information that may well turn out to be the smoking gun of the investigation. There are many different ways to conduct an investigation and each practitioner has their own style. There is no absolute right way. And how long does it take to image a hard drive? Pass me that ball of string will you and let me explain……