

“A discussion of the legality of creating and storing forensic images for  
prosecution in the United Kingdom”

By **Michael Bright** (bs901229)

**ABSTRACT**

In recent years there has been a dramatic increase in the use of computer systems. Tied in with this is the increase in computer crime. Because of this increase a new breed of digital forensic investigator has flourished. The digital forensic investigator is tasked with copying and analysing suspect machines, and when required, making copies which are known as forensic images. A question which still remains unanswered is how legal these forensic images are. The process of copying systems and software has received a large amount of interest in recent years. This has resulted in high profile cases involving the suspension of software sales and the prosecution of people who have used Peer-to-Peer software to infringe on copyright. This paper provides an insight into the process of forensic imaging and its use as evidence in prosecution, providing a background to the legal system in the United Kingdom. It focuses on copyright legislation and when and how forensic images can be deemed legal and illegal.

**INTRODUCTION**

Over the last 10 years the area of digital forensics has expanded dramatically primarily due to the overall increase in computer systems usage. A survey carried out by the National Office of Statistics (2002) showed that more and more people are starting to use computer systems and the internet in their day to day life. The unfortunate downside to this is that as usage is rising, so is the proliferation of internet and electronic crime. Davies et al. (2005) identify that because of this growing figure, there is an ever developing need for qualified digital forensic investigators. The role of the digital forensic investigator has adapted over the years, which is a view supported by Ferraro (2005). With these ever developing job requirements, digital forensic investigators are constantly having to adapt and learn new skills. One of the key skills that any digital forensic investigator must master is that of being able to forensically image. The process of imaging is quite prevalent in terms of the controlled handling of evidence during investigations. Because the digital forensic investigator images many hard disk drives during their career, an interesting question is raised. What are the legal ramifications when a digital forensic investigator images a disk, and essentially makes a copy of its contents? This paper will outline the processes involved in forensic imaging and the different approaches and techniques used. There will be a discussion of the use of images and their handling in both the criminal and civil legal system, and a discussion of software copyright laws and what effects it may have on the process of forensic imaging.

**FORENSIC IMAGING, PROCESSES AND TECHNIQUES**

The term “*Forensic image*”, is a phrase everybody who is involved with digital forensics will come across from time to time. Firstly, it is important to identify that a “*Forensic image*” has nothing to do with pictorial images. In this context, the phrase ‘image’ as outlined by Dictionary.com (2006) is “*An exact replica of the contents of a storage device, such as a hard disk, stored on a second storage device,*

*such as a network server*". What this means is that when producing an image of a storage device such as a hard disk, flash card or USB pen drive, it is making an exact copy of it. This is a very important process because when handling evidence, one of the key objectives as outlined by Inman (2000) is to preserve the integrity of that evidence. If the image that is taken is not an exact copy then the evidence could be considered invalid and could be suppressed in any court proceedings. In relation to the context of this paper, it is important to be aware that when an exact image is taken, not only are all the files which a suspect may have on a system copied, but all of the software and operating system files are copied as well.

When discussing the process involved in forensic imaging, there are two main approaches as outlined by the National Institute for Standards and Testing (2001). The first approach to be considered is termed a "*full bit stream copy*". A full bit stream copy works by accessing the lowest possible denominator of the physical medium, in this case the 'bit'. These bits are then copied one by one from source to destination. This is considered a full exact copy because the process is done iteratively and in a forward only process. A full bit stream copy is the most common approach used within forensic investigation and is implemented in most of the main stream forensic tools. The second approach is termed a "*Qualified bit-stream copy*". A qualified bit stream copy is where the specific data which needs to be copied bit by bit is qualified before the copying process commences. In this context, it simply means that a specific portion of a disk or storage device is going to be copied. This has advantages in terms of storage, but it very much depends on the needs of a prosecutor and the investigation. A good example of this would be the need to copy just the boot record or BIOS Parameter Block as outlined by Microsoft (1999) from one device to another.

Once an exact copy of the source device has been made, the process of then creating a hash value of the data can commence. This process ensures the integrity of the data taken for the bit stream image. Carrier (2005), highlights that the most common implementation of generating a cryptographic hash from a source device, is to use either the MD5 (Messages Digest 5) algorithm or SHA1 algorithm. The process of producing a cryptographic hash involves applying a complex mathematical operation to all of the data on the source device, which will produce a unique value. If the same calculation is then carried out on the data which has been copied, the value should be the same. This is important because it helps ensure that the data is correctly copied and maintains the state of the evidence.

Many tools exist for a forensic investigator to use to produce bit stream and qualified bit stream copies of data. The National Institute for Standards and Testing (2001), is responsible for ensuring that the tools do exactly what they are required to do. It outlines a set of specific criteria to which any forensics imaging tool must comply;

- *"The tool shall make a bit-stream duplicate or an image of an original disk or partition on fixed or removable media."*
- *"The tool shall not alter the original disk."*
- *"The tool shall be able to access both IDE and SCSI disks."*
- *"The tool shall be able to verify the integrity of a disk image file."*
- *"The tool shall log I/O errors."*
- *"The tool's documentation shall be correct."*

Analysing these requirements provides good context to the discussion of the issues in this paper. By ensuring the forensic software development companies such as Encase (2006) and AccessData (2006) meet these standards from a legal point of view, they are clarifying that their software does in fact make an exact copy of the software and operating systems stored on the device which is being imaged. This is very important when discussing whether or not this copying process is in fact a breach of copyright law.

### LEGAL PROCESS IN THE UNITED KINGDOM

Martin (2005) outlines that “*law covers an enormous range of situations and the legal system of the United Kingdom has a variety of courts and methods for dealing with different types of cases*”. What is being stated here is that law is very complex and that different situations require different approaches. In the United Kingdom, the legal system can be split into two main sections as described by Keenan et al. (2004). The civil process, also termed private law, is generally responsible for legal issues between employers and employees, family law and anything which does not generally represent an offence against the countries legislation. The criminal process, also termed public law, represents prosecutions in cases where the suspect has committed an offence against the legislation of the country, such as Murder, Rape and the distribution of Child Pornography.

When discussing the different types of legal prosecution, it is important to remember that while private prosecutions are just as important as public ones, public prosecutions are carried out by the state and therefore may be shielded from prosecution when producing in court items which infringe upon legislation. Forensic cases can appear in both streams of prosecution, for example Ferraro (2005) outlines that *The Crown vs. Schofield Case (2003)* is an example of a public prosecution. In this case, the defendant was accused of accessing child pornography which is considered a crime against the state and therefore prosecuted in criminal law, however in this case the defendant was found not guilty. A good example of the private process is a case where an employee has been dismissed for perhaps breaking a company’s reasonable internet usage policy. This crime was committed against the company and not the state and is therefore a private civil matter. Civil proceedings are not as publicised as criminal proceedings and they are generally much lower key because negative publicity is not good for business.

As mentioned previously, digital forensics can appear in both the criminal and civil process. In the criminal process, digital forensics experts can be called upon to give expert testimony and to produce forensic images to prove cases such as hacking, blackmail and accessing child pornography. In these types of case, it is almost guaranteed that forensic imaging will have taken place. This is primarily because the rules of evidence state that a device must not be altered from its original state. Working on a copy of the evidence ensures that the digital forensic investigator does not damage or alter the state of the evidence. The use of forensic images also allows the digital forensic investigator to take a forensic image off site and analyse the contents in order to make their report to the police or the court. In a civil case, the role of the investigator is somewhat different. Generally, the digital forensic investigator will enter the situation in a paid position for the company wanting the investigation to be carried out. In this context, the investigator has no shielding or protection as expected if working for the Crown as discussed earlier. The digital forensic investigator is likely to carry out qualified bit stream imaging, but it is very

much dependent on the crime or breach of contract which has taken place. The relevance of this scenario is that the investigator is being paid by the company and is therefore in no legal context associated with the Crown. This may have certain legal implications when considering whether or not the use of bit stream imaging can be considered legal.

At this point, it is important to discuss the handling of this evidence and where such evidence may be stored. When considering a criminal prosecution, it is likely that the evidence will be stored at a police station, or held within a Crown approved facility. Again this brings up the point that if the evidence being held is in breach of copyright it is likely that such evidence would be shielded from legal implications. In the instance of a private forensic investigation, it is highly probable that the individual carrying out the investigation on behalf of the company will hold any evidence that they obtain at their offices. This is not an approved storage facility of the Crown and therefore is likely not to have shielding or special privileges in terms of copyright infringement.

Most forensic evidence used in both private and public cases, is held securely for a long period of time, from original acquisition right through to the court case and then for a period of years afterwards in case of appeal. Primarily, the use of forensic images is not related to the software or operating system installed on the source system. These forensic images are used to provide evidence in the shape of files and explanations of any activities which an individual may have carried out on a set system. Very rarely will an investigator be interested in making use of any of the software which they may have extracted from a system. However, there are occasions where an investigator may be required to identify what a specific application does. For example, if the suspect was using what Ferraro (2005) describes as the “*Trojan horse defence*”, the investigator may need to copy and extract executable applications from the suspects system and run them in a safe environment in an attempt to identify what those applications do. The question raised here is if that specific application was in fact not a Trojan and was a company’s intellectual property, has the forensic investigator broken copyright laws by copying the application and running it?

#### **COPYRIGHT LAW IN THE UNITED KINGDOM**

Copyright law is the foundation of protection for developers and authors alike. It provides a fundamental element to ensure that the work of individuals and companies, be it hardware, software or written work, is not copied or misused. Copyright is a long standing concern for many authors, as it provides the fundamental backbone to keeping their work their own. Copyright law has very clearly defined avenues and has been the focus of a number of legal actions in the United Kingdom in recent years. In this day and age, copyright infringement is related in some way to the world of digital technology. A good example of this is the recent actions being carried out by the Record Industry Association of America (RIAA) (2005) and British Phonographic Industry (BPI) (2006). An article by the British Broadcasting Corporation (BBC) (2005) outlines that as many as 750 people are being pursued through the British courts for breaching copyright law, by downloading protected content from Peer-to-Peer file sharing services such as Sharman’s Kazaa software (2005). Bainbridge (2005) outlines that it is only within the last 10 years or so that the use of copyright in information technology has started to be prevalent and legal precedents set, which is a view supported by Rowland et al. (2000). This means that

up until that point, the legislation was not really applied to digital media, by virtue that no cases had been tested. Merkin (1989) identifies that the primary piece of legislation in the United Kingdom which is associated with Copyright protection, is the Copyright, Designs and Patents Act 1988. This is a view supported by Bainbridge (2005) and Rowland et al. (2000). This Act provides the fundamental structure to all British copyright laws, and gives scope as to what is illegal and legal copying. A point for discussion is whether or not the Act needs to be rewritten. This is due to the fact that technology is constantly changing and an Act written over 20 years ago may not be able to handle all possible outcomes of the future. In the context of this paper, it is important to identify the relevance of the Copyright, Designs and Patents Act because it provides the framework against which forensic imaging can be tested to see whether or not it is in fact in breach of the Act.

Bainbridge (2005) outlines the key points from section 16 of the Act stating that copyright is infringed when a person other than the owner of the work carries out any of the following;

- “*Copying the work*”
- “*Issue copies of the work to the public*”
- “*To rent or lend copies of the work to the public*”
- “*To perform or play the work in public*”

These key points draw together the main basis for determining whether or not an item is in fact infringing copyright or not. These can be considered the key objectives when trying to determine whether or not a forensic image does in fact breach copyright laws.

Another key point, which Bainbridge (2005) discusses, is the part-copying of work, and whether or not this can be considered copyright infringement. He outlines, that for copyright to be infringed, a whole copy of the work does not have to be taken which is a view supported by Millard (2000). In *Cantor Fitzgerald International vs. Tradition (UK) Ltd* (2000), 2952 lines of programming code were taken out of a total in excess of 30000, and it was deemed that enough of the copyrighted work was taken for it to be considered a breach of copyright law. This has implications in the context of this discussion because it can be related directly to the process of “*qualified bit stream*” copying, where only partial elements of a source system are copied. Therefore implying, that if a partial forensic image was taken and specific parts of a piece of software were copied, copyright infringement has occurred.

Millard (2000) also discusses the implications that European legislation on copyright may have on British implementations. He outlined that although Britain has quite clear copyright guidelines, the European Union (EU) implemented a directive (EC 2001/29/EC) to harmonize member states copyright implementations. The changes made through the EU directive do not really have much effect on the discussions of this paper and context of copying images, but changes through the directive primarily tidied up vague areas in the original Copyright, Designs and Patents Act 1988.

The Business Software Alliance (2006) is primarily responsible in the United Kingdom for the pursuance and prosecution of companies and individuals involved in copyright infringement involving software. Together with Customs and Excise (2006), they have had a number of successful prosecutions where individuals have essentially made “*bit stream*” copies of CD’s and DVD’s, which have been either sold or passed on at no cost. This draws parallels to what a forensic investigator

carries out when extracting evidence from a suspect's machine. This is supported when Bainbridge (2005) states that "*An unauthorised copy of a computer program may be ... where a disk to disk copy is made*" and this statement is important because it supports the assumption that the creation of a forensic image can be considered illegal.

A recent legal case made in the United States also provides bearing onto the discussion. The BBC (2004) reported that the company 321 Studios, that produce DVD copying software, were ordered by the US Court to cease distributing their software because it indirectly allowed people to breach copyright. DVD copying software is considered to be no different to that of forensic imaging software, because both have exactly the same function, i.e. to produce bit for bit "*bit stream*" copies of an original source.

The possibility for the usage of forensic imaging applications for purposes other than those defined by their title, is entirely possible. The extraction of software and applications from a forensic image is entirely feasible. The procedures when considering forensic imaging software, rely on the professionalism of the users of such applications, ensuring that they will be used appropriately and for the purpose for which they were designed.

#### **EXEMPTION OF EVIDENCE FROM COPYRIGHT**

The previous discussion on the copyright legislation in the United Kingdom outlined the clear objectives of the law and how different aspects of copyright can be infringed. The discussion of whether or not forensic imaging can be a breach of copyright is very much dependent on the context in which it is used. As discussed earlier, the general perception that anyone working for the Crown or the Police, has limited protection against prosecution for copyright theft, is accurate. An analysis of the Copyright, Designs and Patents Act 1988 identifies that under Section 45 entitled the public administration clause part 1 and 2, states that;

45. (1) "*Copyright is not infringed by anything done for the purpose of parliamentary or judicial proceedings.*"

45. (2) "*Copyright is not infringed by anything done for the purpose of reporting such proceeding; but this shall not be construed as authorising the copying of work which is itself a published report of proceedings.*"

What this section of the Act is identifying is that although certain works may be copyrighted, they can be used in the context of parliamentary and judicial proceedings. The important phrase to discuss here is "*judicial*", which the Oxford dictionary of Law (2003) outlines to mean "*of, by or appropriate to a law court*". This essentially implies that proceedings which involve the use of law courts provide exemption from copyright protection. What this states is that evidence which is obtained as a forensic image, for use with trial and prosecution as part of the public or criminal legal system, has protection from infringing on copyright when being used. This therefore provides a definitive answer to the question of the legality in terms of copyrighted work for criminal proceedings. However, it does not provide a clear answer for civil and private investigations.

As discussed earlier, there are two approaches to the legal system in the United Kingdom, Civil and Criminal. The civil process involves the use of privately

hired digital forensic investigators and on many occasions, the work carried out by such investigators will never reach a court room or tribunal. This leaves a question mark hanging over the legality of forensic images which they have taken. The question of whether or not forensic images they have made are infringements of copyright is quite sound. If they produce images of copyrighted software, and these forensic images are then taken off the site of the company who purchase the licence for set software, then technically, this does break the copyright rules as outlined earlier. Because there appears to be no protection for the private investigator that does not appear in court and therefore does not have the legal protection of the Crown, the possibility is that they leave themselves open to prosecution.

The second area which is quite important to this discussion is, if a copyright law was breached would a company which owns the right to the software actually pursue a copyright infringement action against the forensic investigator? This question can be looked at from two possible angles; the first being large companies such as Oracle, Sun, and Microsoft. These companies are less likely to complain too much about their software being imaged in the legal arena, be it for court action or not. The reality being that it is more than likely that the forensic investigator will image the disk, analyse the contents, and then lock it away for a period of time before destroying it. On the other side of the argument, there would be companies which produce software to subvert forensic investigations. For example, companies which produce Internet History Erasure Utilities and companies who produce specialised security applications. If a breach of copyright were to occur on their work it is quite conceivable that such companies would consider legal action, as their primary business target is the people who are likely to be investigated. The technique used for the imaging is also important. If the investigator took a full "bit stream" copy of the source then it is extremely likely that the copyrighted work was infringed upon. However, if the investigator took a qualified "bit stream" copy, it would be hard to determine which parts of the source the investigator took. This clouds the issue in terms of trying to identify when and if copyright was infringed and also if enough of an application, which was copied, was in fact taken to prove copyright infringement.

An interesting legal argument comes into play here because although the companies have no way of knowing that their software has been imaged, it is a fair assumption that anybody purchasing forensic imaging software (such as EnCase (2006) or AccessData's (2006) Forensic Tool Kit) is likely to be using it to produce forensic images. Referring back to the discussion on 321 Studio's application software, if their application is being stopped because it provides the ability to make copies of DVD's, couldn't the same precedent be applied for forensic imaging software? If an investigator knowingly purchases either of the above mentioned forensic applications, they must have an idea as to how they are going to use it and that not all of their work will be for public prosecutions. This raises the issue that if a court can ban one type of application, yet allow another with the same type of functionality to be sold, how can an applications developer determine whether their software will be classed as legal or illegal?

## **CONCLUSIONS AND RECOMMENDATIONS**

This paper has provided a detailed background into the different elements which may affect the process of forensic imaging. It has provided an overview to the processes involved in forensically imaging a disk. It has also discussed the copyright legislation which currently exists in the United Kingdom and whether or not it applies

to applications which carry out forensic imaging. Following the discussion carried out in this paper, it is possible to clearly identify that evidence which is forensically imaged for use in judicial proceedings is perfectly valid from the view of copyright. What is not clear is whether imaging carried out by a private digital forensic investigator for an organisation with no connection to legal proceedings is legal. This paper identifies a question which still remains unanswered, although not a serious threat to copyright of a product, forensic imaging never-the-less sets a precedent similar to those in the cases discussed. How can the legal system block certain types of applications but not others that perform the same types of function? The paper draws conclusions that the current legislation which is in place, via the Copyright, Designs and Patents Act 1988, is reasonably old in nature and can be paralleled to that of the Computer Misuse Act (1988). As technology is ever changing and the legal world has to try to keep up, surely it is time for a revised set of legislation on copyright, one which is appropriate for technology and the adaptive future of the 21<sup>st</sup> century.

## REFERENCES

AccessData Software, 2006, *The Forensic Tool Kit* [online]. Available from: <http://www.accessdata.com> [Accessed 7<sup>th</sup> April 2006].

Bainbridge, D., *Introduction to Computer Law*. 5th Edition. London: Pearson.

British Broadcasting Corporation News, 2004, *Court stops DVD-copying program* [online]. Available from: <http://newswww.bbc.net.uk/1/hi/technology/3512825.stm> [Accessed 6<sup>th</sup> April 2006].

British Broadcasting Corporation News, 2005, *Legal action for 784 file sharers* [online]. Available from: <http://news.bbc.co.uk/2/hi/entertainment/4640415.stm> [Accessed 6<sup>th</sup> April 2006].

Business Software Alliance, 2006, *BSA Online* [online]. Available from: <http://www.bsa.org> [Accessed 5<sup>th</sup> April 2006].

Carrier, B., 2005, *File System Forensic Analysis*, New York: Addison Wesley.

Davis, C., Philipp, A., Cowen, D., 2005, *Hacking Exposed: Computer Forensics Secrets and Solutions*. California: McGraw Hill.

Dictionary.com, 2006, *Definition of term "Image"* [online]. Available from: <http://dictionary.reference.com/search?q=image> [Accessed 5<sup>th</sup> April 2006].

Ferraro, M., Casey, C., 2005, *Investigating Child Exploitation and Pornography: The Internet, The Law and Forensic Science*. London: Elsevier.

Guidance Software, 2006, *Encase Forensic Tools* [online]. Available from: <http://www.guidancesoftware.com> [Accessed 7<sup>th</sup> April 2006].

HM Customs and Excise, 2006, *HM Customs and Excise Home Page* [online]. Available from: <http://www.hmrc.gov.uk/home.htm> [Accessed 7th April 2006].

Inman, K., 2000, *Principles and Practice of Criminalistics: The Profession of Forensic Science*. New York: CRC Press.

Keenan, D., Smith, K., 2004, *English Law*, 14<sup>th</sup> Edition, London: Pearson.

Martin, J., 2005, *The English Legal System*, Oxon: Hodder Arnold.

Microsoft, 1999, *FAT32 File System Specification* [online]. Available from: <http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx> [Accessed 7<sup>th</sup> April 2006].

Millard, C., 2000, Copyright. In: C. Reed, J. Angel. *Computer Law*, 4<sup>th</sup> Edition. London: Blackstone Press, pp 177-226.

National Institute for Standard and Testing, 2001, *Disk Imaging Tool Specification* [online]. Available from: <http://www.cftt.nist.gov/DI-spec-3-1-3.doc> [Accessed 5<sup>th</sup> April 2006].

National Office of Statistics, 2002, *Household Internet Access 1998-2001* [online]. Available from: <http://www.statistics.gov.uk/STATBASE/ssdataset.asp?vlnk=6016> [Accessed 5<sup>th</sup> April 2006].

Record Industry Association of America, 2006, *RIAA Website* [online]. Available from: <http://www.riaa.com> [Accessed 7<sup>th</sup> April 2006].

Rowland, D., Macdonald, E., 1997, *Information Technology Law*, 2<sup>nd</sup> Edition, London: Cavendish Publishing

Sharman Networks Limited, 2005, *Kazaa* [online]. Available from: <http://www.kazaa.com> [Accessed 7<sup>th</sup> April 2006].

The British Phonographic Industry Limited, 2006, *The BPI* [online]. Available from: <http://www.bpi.co.uk> [Accessed 7<sup>th</sup> April 2006].

The Register, 2003, *Trojan defence clears man on child pornography charges* [online]. Available from: [http://www.theregister.co.uk/2003/04/24/trojan\\_defence\\_clears\\_man/](http://www.theregister.co.uk/2003/04/24/trojan_defence_clears_man/) [Accessed 4<sup>th</sup> April 2006].

.