

Saturday, 30th August 2003

**Report on the Case of Detective Constable Brian Stevens
Snaresbrook Crown Court,
August 20th 2003.**

NB: clarification commentary is provided in italicised red.

This case attracted a great deal of public and press attention because of D.C. Stevens' association with the investigation into the murders of the two little girls, Holly Wells and Jessica Chapman at Soham in Cambridgeshire. What is presented here is solely concerned with the forensic investigation into the contents of a laptop hard drive. A full report is not provided because Cambridgeshire Police are considering disciplinary proceedings and I have no wish to compromise these. However, in the public interest I present below some extracts from both expert reports to illustrate the particular technical areas which persuaded the Crown Prosecution Service to abort the case. Legitimate forensic practitioners are well aware of the difficulties of conducting an investigation when the opposing expert is clearly lacking in the relevant technical knowledge and appears to have no idea of the precise duties and responsibilities which are expected of him. Direct quotations from Mr Underhill's statements are noted and italicised below, the English is his - not mine.

Note also that I have never knowingly met or spoken to Mr Underhill. The observations here are all based upon his written statements in this case and these constitute a technical 'expert' report in which precision of language and reasoning should be paramount.

The Charges

Detective Constable Brian Stevens was charged with six counts of possessing indecent images of children, contrary to section 160(1) of the Criminal Justice Act 1988 and two counts of distributing indecent images of children, contrary to section 1(1) (a) of the Protection of Children Act 1978. All of these offences were alleged to have been committed by the defendant between 1st January and 13th September 2002.

At least two of these charges were insupportable and there was some dispute about the remainder.

Introduction

This case came about as a result of D.C. Stevens' credit card number appearing on a list of alleged subscribers to child porn sites provided by U.S. Authorities - resulting in the much publicised **Operation ORE**.

On 12th September 2002, D.C. Stevens's home was visited by the Police and a laptop computer was seized. This was initially examined by a Police technician at West Midlands Police Hi-tech Crime Unit. He found a number of what he considered to be indecent images of children and the laptop was then passed by West Midlands Police to Brian Underhill for expert investigation.

The Investigation

Mr Underhill investigated the hard drive and produced a number of statements presenting his findings. Included in these were three statements dated 14th November 2002. Each of these contained several pages which were identical and various identical phrases and paragraphs appeared elsewhere. In his introductions to these statement Mr Underhill claimed to have, *"over 20 years experience working with computers"* and he was *"conversant with the various Microsoft® Windows' Operating systems, and DOS, along with other common systems"*. He also claimed, *"experience in a vast number of Software Applications on numerous Operating Platforms"* and in particular was *"fully conversant"* with the operation of the AOL software. In addition he claimed *"over 25 years experience as a Police Officer and as such I am familiar with the rules of evidence and its provisions."* He went on to say that *"For the last 40 months, I have been working in the field of Computer Related and Hi-Tech Crime. During that period I have assisted in/conducted approximately 600 Police Investigations in the field of 'Computer Evidence' and presented evidence in Criminal Court on this matter."*

These figures produce an average of 15 cases per month - or slightly under 3.5 cases per week.

Within the various statements, a total of 48 exhibits were generated and duly

numbered. The origin and content of some of these is still a little obscure but all except two of them were picture exhibits - either printed or electronic copies.

Analysis indicates that Mr Underhill produced a total of 219 exhibits depicting 85 different pictures. A significant proportion of these did not depict sexual subjects.

The email system was the standard one provided with AOL 7.0 (with which Mr Underhill was "fully conversant") and he reported upon a total of 16 live emails recovered from the drive. Some of these contained attached or embedded pictures.

There were actually a total of 67 live emails, which provided additional information concerning the chronology of email traffic, the dates and times of a number of relevant downloads (including WINZIP80) and other periods of activity.

Mr Underhill commented upon the presence of a directory named **C:\Program Files\AOL 7.0\misc\temp** which contained a number of zip files, and suggested that this was not a standard directory and had therefore been created by the user as a storage area for pornographic images. He also stated that all of the zip files in this directory contained pictures of a sexual nature.

This was demonstrably not true. Tests showed that this directory was created and maintained by AOL 7.0 as a storage area for zip files created during email attachment procedures. If a user attempted to attach two or more files to a prepared email, this version of AOL created a zip file within the 'C:\Program Files\AOL 7.0\misc\temp\' directory, containing the attached files. The zip name was the same as the first attached file (but with an extension of 'ZIP'). This occurred whether or not the email was subsequently sent. If the directory did not exist, it was created by AOL. There was no indication that a user would ever be aware of this directory or the circumstances under which it was created or used.

Mr Underhill went into some detail concerning the use and history of WinZip on this drive in an apparent attempt to recover evidence concerning the manipulation of relevant zip files. He recovered details of four files processed by WinZip, none of which could be found on the drive.

Vital information that Mr Underhill missed included the facts that a) one of the four files was an included part of the WinZip80 package, b) All four files had been processed on 2nd & 3rd June (WinZip was installed on 10th February) and c) Recovered backup records dated as late as 19th August indicated that these were the only four files processed by WinZip. He did not attempt to explain how a user could have created or accessed the zip files within the 'C:\Program Files\AOL 7.0\misc\temp\' directory without using WinZip.

The general presentation of evidence by Mr Underhill was so poor and riddled with errors that I took the unusual step of providing a specific appendix in my own report which discussed his statements. This is only the second time that I have done this - the first was in the David Mould case involving Nick Webber.

Within this appendix a total of 20 sub-paragraphs itemised the more serious errors and omissions. Some of these are listed here (each was preceded by various multiple page references and filenames have been concealed) :-

- "He states that: "If a file is 'renamed' or 'copied', the date and time will remain unchanged as the actual 'file content' has not been 'created, altered or modified'. This is not true."
- "Mr **UNDERHILL**'s description of pictures in emails is incomplete and misleading."
- "It is stated that "when an email is sent, the date/time is allocated from the computers internal clock". This is incorrect, only the date is allocated in sent emails in the AOL system."
- "It is stated that one of the sent emails had a ZIP file attached which contained a picture of "a child apparently under the age of 16 years". This is not true. In fact none of the sent emails listed in this section of the statement contained ZIP files."
- "Contrary to the displayed entry, the file ??????????.zip was not sent to ???????"
- "It is suggested that some of the AOL usernames implied that the user "is a young female". This is an unsupported inference which appears to be based upon the forced numeric suffix to the usernames."

- "The suggestion that the files **?????.zip** and **??????.zip** were 'made' on this computer is misleading. Examination and analysis show that these files were downloaded, probably as attachments to incoming emails. The automatic AOL unzipping procedure then created the relevant subdirectory and unpacked the constituent files of the ZIPs into the subdirectory."
- "Mr **UNDERHILL** appears to claim that 32 of the pictures found within the **?????????** directory "*depicted children who appear to me to apparently be under the age of 16 years*". In fact only 16 pictures were recovered from this directory. The listing of 32 pictures includes 13 duplicates and it appears that the description deliberately avoids using the word "indecent" with the subsequent misleading effect.
- "The explanation that "*ZIP files accessed from an Internet site will (normally) be copied to the cache*" is not true. If a ZIP file is referenced within a web page, it will normally appear as an icon or link text. If the user clicks on this link then the browser will prompt for a location for the ZIP file and then download it to that location. The cache is solely for transient display elements within a web page command file (usually HTM or one of its derivatives)."
Subsequent research has shown that under certain highly unusual circumstances it is possible to force a zip file into the internet cache. This does not alter the sense of the above criticism, ZIP files are rarely if ever, found in the internet cache.
- "The suggestion that **Window Washer** was configured by this user to delete traces of internet activity is not true (see **Appendix H** above)."
- "The conclusion that a user "*viewed 'zip' files from internet sites . . .*" is not supported by the evidence."

In a field where precision and clarity of thought is vital, the above demonstrates conclusively that Mr Underhill had neither the computer expertise to collect and analyse the evidence, nor the communications skills to present his findings in a clear and non-partisan manner.

The Truth

The tangled web of false inferences, incorrect deductions and misleading conclusions which Mr Underhill created from incomplete and inaccurate information appeared to be aimed at proving the guilt of the defendant. Quite apart from breaking the first rule of forensic investigation, his statements suggested that D.C. Stevens had a case to answer and the C.P.S. had little choice but to act on his advice. After a more accurate investigation, the following facts were confirmed :-

- The computer was a laptop machine belonging to D.C. Stevens.
- It was not in his possession the whole of the time.
- The configuration of the machine was such that anyone with a minimum amount of computer knowledge could have used the machine to connect to the internet. No passwords or telephone numbers would have been needed, they were all stored on the machine for automatic access.
- The pattern of activity on the machine suggested occasional rather than regular access to the internet, with the distinct possibility that this had been opportunistic.
- There was no evidence of subscription or connection to any of the Landslide websites.

In the light of the above facts, the expert advice to the C.P.S. should have been that additional information was needed before any charges could be brought. Further investigation should have concentrated upon the whereabouts of the laptop and the whereabouts of D.C. Stevens and anyone else who had access during any of the relevant periods of activity recovered from the computer. I gave similar advice to the defence team, along with a detailed listing of the dates and times involved, and it was this which resulted in an alibi being provided by D.C. Stevens for one of the most important of the periods of activity (when 3 of the indictment pictures were received). This meant that of the original 8 counts in the indictment, 5 were simply not supported by the evidence and there was serious doubt about the remaining three. I believe that the C.P.S. had no option but to act as they did.

The Fallout - West Midlands Police

When I was engaged by the defence and I attempted to obtain access to the computer for the purposes of making my own forensic copy of the hard drive, this was refused on the grounds that "new guidelines" prevented the Police from allowing such access. They

said that they did not want to be party to any proliferation of child pornography. It was necessary to obtain a Court Order before I was allowed to do my job. Given my background and the fact that I had been legitimately instructed by the defence solicitors, this constituted a completely unnecessary waste of court time and money.

I now understand that at that time (6th May 2003), no new official guidelines had been issued. This raises a question about what the real reason was for denying the defence appropriate access. In addition, it appears that such access and non-proliferation 'guidelines' did not seem to apply to the Police expert, especially since the 6 different pictures mentioned in the indictment were exhibited a total of 33 times.

I am told that a senior spokesman for West Midlands Police is reported as saying that it was unfair that a "well respected expert" should be so vehemently criticised for a single mistake. I am happy to go on record with this report where it can be seen that this was not "a single mistake", it was a whole catalogue of errors (not all of which are reported here) which clearly demonstrated that Mr Underhill's various pronouncements were worthless as any sort of expert evaluation of the available evidence. I am also aware of at least one other case where Mr Underhill demonstrates yet more evidence of incompetence. Some of his errors there are even more serious than those reported above but since this case is sub-judice, no further details can be published at the moment.

It follows therefore that the suggestion that Mr Underhill was "well respected" is itself a serious example of misjudgement on the part of West Midlands Police and further reinforces calls for an examination of their own competence in this field. The reasoning is quite simple, if they are unable to accurately evaluate the forensic expertise of someone like Brian Underhill, how reliable is their own expertise in the same area?

This is not a global criticism of all who work at West Midlands Hi-tech Crime Unit, just those responsible for advising that Brian Underhill was a suitable candidate for employment as a forensic expert.

The Fallout - Operation ORE

Some sections of the press have suggested that the collapse of the Stevens case may cause the collapse of Operation ORE itself. I disagree.

There are many good and competent police officers working hard to evaluate and investigate the information provided under this operation and I have no doubt that dangerous offenders will continue to be correctly identified and successfully prosecuted for their activities in supporting the appalling abuse of children around the world. It is apparent to me that Operation ORE and any subsequent similar operations **must** continue and **must** be helped to succeed. If the appropriate authorities look at and learn from the mistakes in the Stevens case then I am sure that with some slight re-evaluation of both the relevant legislation and current police procedures, this initiative could proceed much more effectively and with far less risk of similar mistakes in the future.

Opinion

Many of the media reports castigated the Crown Prosecution Service for this fiasco and I do not believe that this is fair. In prosecutions where there is a significant technical element to the evidence, the C.P.S. are in the hands of their expert and must assume that he knows what he is talking about. It was not the C.P.S. who employed Mr Underhill, and there is no reason to suspect that they knew he was a charlatan. Amongst honest members of the forensic computing community, Mr Underhill is known as an associate of the infamous Nick Webber (see [the Case Report 3](#)) and their operations (through their company, CELT Limited) are known to be thoroughly unreliable.

Responsibility for this mess rests squarely between Brian Underhill and elements of the West Midlands Hi-tech Crime Unit who employed him in the first place. The damage can only be undone by a thorough review of any cases where convictions were obtained solely on the evidence of Underhill or Webber.

T. J. Bates.
August 31st 2003

5th September 2003

The article in Private Eye was interesting. It seems that they are somewhat scandalised that I am, "hardly a disinterested observer in all this." I thought about replying and telling them that of course I'm not disinterested and giving them many reasons why (competition with the likes of Webber and Underhill not being one of them) but if they can only count

the words and not the commas, full stops, dashes and all the other paraphernalia of me matchless prose then why should I bother?. The facts are that I am semi-retired, have more work than I can handle and I am happy to support any members of the honest forensic community in any way that I can - "competitors" or not. Additionally, since Webber and Underhill only work for the Police and something over half my cases are for the defence, there's no question of competition.

The interesting bit was that they seem to be under the impression that it is an expert witness's job to "nail child abusers". Does that mean that all honest forensic practitioners in this field are secretly apologists for internet paedophiles?

11th September 2003

News has just been released that Brian Stevens has been re-arrested by West Midlands Police. This time apparently for attempting to pervert the course of justice. It appears that there are questions concerning the alibi which was provided.

This development does not alter the facts presented above. Whether the alibi was real or concocted Brian Underhill is still shown to be incompetent. It may even be thought that he should face charges of obtaining money by deception.

© 2003 Jim Bates

[Return to previous page](#)