

EMPLOYMENT TRIBUNALS and the use of Digital Forensics

WHITE PAPER

Compiled by Vassilis Manoussos, Msc, PG Cert, BSc, AAS
Digital Forensics Consultant.

Digital Forensic Services

Most people are familiar with the term "computer forensics" which is understood as the investigation of a computer in order to discover evidence of an event or a crime. The evidence may be available and apparent or it may be deleted and one may need to retrieve it from a magnetic media.

Today, electronic data is stored in a wide variety of media and evidence can be sought and retrieved from many devices that are not a computer in the classic meaning of the word.

Businesses and their employees use (apart from computers) mobile phones (like Blackberry, iPhones and Nokia smart phones that provide access to internet, instant messaging, Office suites etc.), satellite navigation devices (SatNav), iPads, USB storage devices, wireless printers, digital cameras etc.

It is often the case that the line between personal and business use of these devices is not drawn clearly, and as a result disputes may lead to long and costly litigation, law suits and dismissals. People use their business phones for personal calls and business laptops to send personal emails. But where does the "acceptable use" end and the abuse starts?

What pieces of evidence can be used to dismiss an employee? What is not acceptable?

This White Paper aims to provide you with the basics of the use of digital forensic evidence in Employment Tribunals

Case Studies

Here are some case studies to demonstrate some of the most occurring issues in the workplace, related to the use of digital technology:

Case 1. Excessive use of the internet

An office worker is accused for using the internet constantly for personal use. Based on their team leader observations of their workstation they are dismissed.



In the presence of digital evidence, an observation may be not enough to dismiss an employee without the fear of being taken to an Employment Tribunal.

The employee may have a browser open all day but never use it, or use it only during a break. This can be easily proven by examining the history of that browser's activity, and if the computer is on a network by logs and records of internet filters.

Another issue is the company's IT Policy. Does the business have one? Was the employee

aware of it? Was he/she notified of any changes? Did they actually deviate from the IT Policy?

A thorough forensic investigation can provide the evidence, no matter which side your law firm represents.

The internet has become an irreplaceable tool for businesses. It is your image, your corporate identity exposed to the world, and the easiest way for potential customers to find you.

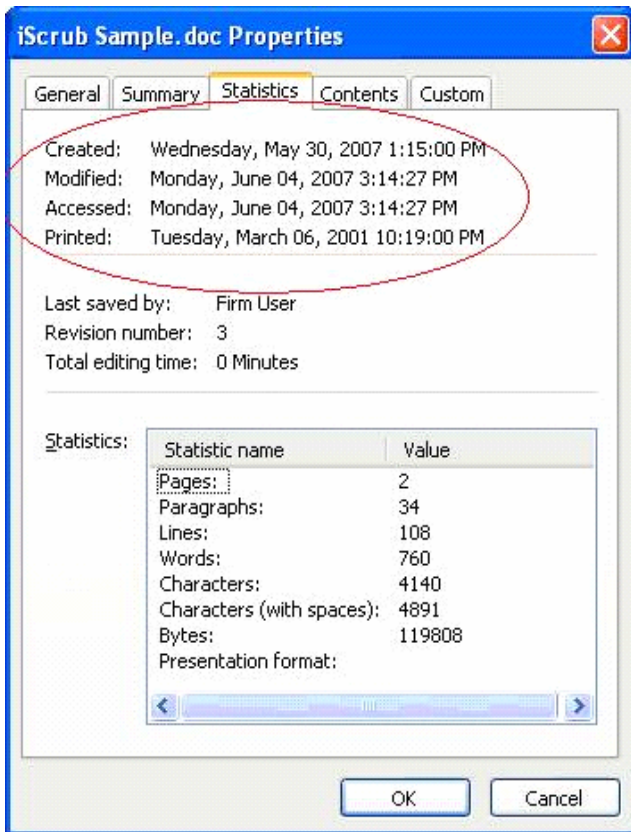
The use of internet by employees though is an open door for trade secrets to find their way to third parties, outside your company. It is important to find the right balance between the need of your employees to use it and your need to protect your business.

Case 2. Validity of electronic documents

An employee is fired because of her absences. Her employer claimed she violated the terms of her employment. At the Employment Tribunal an electronic document was produced with the company policy on absences. Who was right?

The employee in question claimed that this document (which was a newer version of her original terms of employment and business policy) was never shown to her. There was no signed record of her getting a copy.

The employer claimed that the document was given to her and the original electronic document was provided as evidence.



Upon examination, it was proven that the document was created more than a month after the day the employee was dismissed. This placed the employer at a predicament.

The date a document was actually created is not what the Windows file system will show you. This sample shows how sometimes meta-data can be confusing. It is important to make sure when you send (or receive an electronic document) to understand the significance of its date and time stamps and any other metadata, the hidden information inside the file.

This applies to all documents (Microsoft Word, ODF, PDF, Excel spreadsheets, Powerpoint presentations) as well as media files (photos, MP3s and other audio and video files).

Case 3. Hidden information inside electronic documents

An employee was investigated because he wrote a document with inside information and made it public. The employee denied this, so the document needed to undergo forensic investigation.

The document was created using Microsoft Word and then exported in a PDF (Portable Document Format) file. The file was distributed through a disposable webmail account.

The examination of the PDF provided with information about how it was created. It was obvious it was created with MS Word, saved as DOCX (which although existed in Microsoft Office 2003, it was the default format of Office 2007). It also provided information about when it was converted to PDF (although the Microsoft Word date stamps were removed at the conversion stage).



The meta-data (hidden information **inside** the document and **about** the document) also revealed the software that was used to convert it to PDF.

The most important part was the User ID of the user which identified the said employee. Meta-data stay with a document.

Case 4. Computer abuse at work

An employee was investigated because they were suspected they used their manager's desktop to access confidential letters, and send applications to other jobs from the said computer.

The suspect computer was investigated. The "recently opened documents" in Microsoft Word showed that there was a file opened with the employee's name in the filename. The file did not exist in the hard disk and so I tried to recover it. However because the computer was used heavily since, the file was not recoverable.

The employer believed the file was brought in through a USB stick. However further investigation revealed that the file was downloaded from a disposable web-mail account. The file was downloaded as a ZIP (compressed file), opened, emailed and printed, and then deleted. There was also evidence that recent temporary files were deleted leaving a gap in the overall activity image of the computer.



The evidence recovered and the spotting of "missing evidence" was all put in a time-line that put the pieces together and explained what happened.

The employer showed the report to the employee during a disciplinary hearing, and the employee admitted the truth.

Case 5. Harassment at work

An employee complained that she received sexually explicit emails from a Hotmail account but she suspected one of her colleagues.

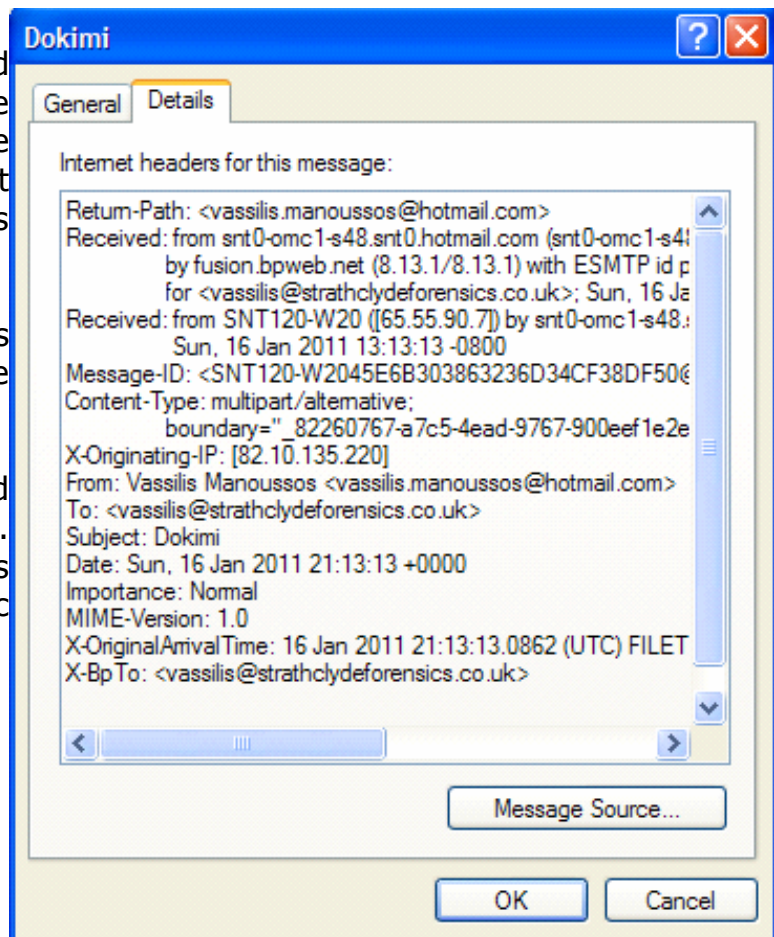
The email messages sent through Hotmail were investigated.

The headers of the email were examined in order to determine where the user was when they logged in to Hotmail.

The information retrieved proved that the user's IP Address was the same as the IP address of the business, so there was no doubt that whoever sent that email was working in that office.

However further evidence was needed in order to identify the person.

Further investigation provided evidence of who the user was. Internet logs and the time stamps of the email matched it to a specific PC and person.



Other potential scenarios.

Here are some other possible cases that you may come across. The investigation may apply for both sides (employer and employee).

- ✓ An employee returns a smart phone before leaving the company. Do you know what kind of "inappropriate" photos or videos is stored in it?
- ✓ Did an employee install a keylogger in a laptop they returned? A software keylogger can send information on the activity of the next user, including log in credentials (usernames and passwords), financial data, documents etc.
- ✓ Is an employer's IT Policy solid? Is it comprehensive and up to date?
- ✓ A malicious message or spam is sent through an employee's business email account. Did the employee send the email or was it sent by a virus or some other form of malware?
- ✓ Can you find from the company SATNAV if a sales person was where they said they were , at a specific day and time?
- ✓ Is an employee using the business infrastructure to set up their own online business and run it through your computer network?
- ✓ Is an employee watching porn or downloading child pornography in the business computer? How does that affect the employer?
- ✓ Is an employee sending out business trade secrets through email or FPT ?

Other advice.

The case studies and list of possible cases provided in this White Paper, are only indicative of how digital forensics can provide litigation support. There are hundreds of other possibilities and each scenario is unique.

Strathclyde Forensics provides you with comprehensive support and an open mind to any investigation of digital evidence. Feel free to contact us for a non-obligation conversation about e-crime and your needs. Take litigation support and digital evidence to the next level.

We provide our services on a case-to-case or on a contract basis.

You can distribute this documents without limitations, as long as you do not alter it in any way.

For more information about digital forensics services and how you can integrate them into your litigation processes, please visit the [Strathclyde Forensics website](http://www.StrathclydeForensics.co.uk).

www.StrathclydeForensics.co.uk

Find out what other forensic services you can incorporate to your litigation processes. Read about our previous cases and discover new opportunities for your future cases.

For more information about forensic investigation of Blackberry and Nokia mobile phones, please visit our two sister sites:

www.BlackberryForensics.co.uk or www.NokiaForensics.co.uk



Copyright 2010-2011 Strathclyde Forensics