Frequently Asked Questions – Digital Forensics

If I suspect something about a company computer, that it may have been misused how do I examine it for evidence?

Firstly if the device is turned off – not just hibernating or in sleep mode, then pull the power cord out, then any other connection. Bag it up if it is a laptop or wrap it up if it is a desktop and place a seal over any securing tape with your date, name and signature on it. Lock it away in a secure place until you can consult someone with the necessary skills to advise you on how to proceed.

If the device is switched on then seek professional advice, switching it off will remove any suspect evidence that may be in memory or cache memory – dealing with a computer that is still on and connected to a network requires specialist help. However, you need to take a view, if company secrets are being uploaded to a third party as a fraud, you may need to disconnect the network – but you need to seek advice, or risk an uncertain outcome. If you need to switch the computer off, do not go through the normal shut down procedure but unplug it from the back – pull the lead out. Do not touch the keyboard or mouse or remove any devices connected to the computer.

If the suspect computer is already off – do not turn it on.

Can I take a quick look to see if I can find any damming evidence?

No, do not touch it. Do not allow any internal IT staff to conduct a preliminary investigation. By accessing it you change what is happening on the PC and will damage any chances of a successful outcome if recourse to legal action is necessary.

To you need all of the equipment associated with a suspect user?

Provided the computer is switched off and disconnected, if possible seize any peripherals assets such as external hard drives, USB sticks, CD's and secure any backup server data. If the suspect has a company laptop, smart phone or tablet, seize that as well. You need management clearance to do this preferably at senior manager/director level.

How do I secure the (crime) scene?

Make sure you secure the crime scene and take full notes on what actions you take, inform your management chain. If you have a forensic readiness plan in force then invoke it. If a suspect has been caught-in-the act of doing something to the company computers then you should ensure he returns any company equipment such as his laptop and mobile phone. Start an incident log to contain all actions giving name, date and time. These must be contemporaneous and if you make any mistake strike them through, do not attempt to rub any notes out or use any correcting fluid.

If we call you in, what will you do?

We will collect all the evidence and transfer it to our laboratory, examine and log the material carefully. One of the things we will do is to safely remove the hard drive and make a forensic image of the drive using write blocking techniques to ensure that the original data is not altered or changed in any way. We will use a forensic copy to analyse the information contained on the original hard drive.

These are generic answers to the most common questions that we get, they should not under any circumstances be considered advice.

Camtek CSI operate mainly in London and the South East but also take enquiries and assignments from the UK nationwide and Europe.

Camtek CSI assist firms with business resilience issues relating to cyber-security, business continuity/disaster recovery and digital forensics. We carry out risk assessments on companies to identify any potential threats that they may have which may impact on them to successfully operate during a period of crisis, and develop a business continuity plan for them.

For more information please visit our website at www.camtekcsi.com
or email us at: enquiries@camtekcsi.com

V2 – Sept 2014