Computer Forensics Consulting LLC
952-454-6951
consulting@computerforensicsconsultingllc.com
www.computerforensicsconsultingllc.com

Computer Forensics and Data Recovery FAQ (Frequently Asked Questions)

1. **What can be found in a computer forensics exam?**

    a. Many different things can be found, including information about files that currently reside or used to reside on the device being examined. In addition, information about files deleted recently or in some cases long ago. Fragments of files from long ago may also be uncovered. Deleted email messages, pictures, audio files, or any other type of file such as business documents and databases may be found. Details about certain user activity may also be able to be documented. See some of the following questions and answers for additional examples.

2. **Will formatting a disk erase the data?**

    a. In general, formatting a disk only removes the pointers to the data (the index – a bit like ripping out the table of contents from a book, you may not know what is there, but it is still there). The data itself will remain until overwritten by new data. If you were to inadvertently format a drive, by choosing the wrong drive from a list for example, if you stop using the device immediately, the vast majority of the data will be recoverable, most likely without significant damage.

3. **Is there a way to tell if someone copied data off of a computer just before they left the company?**

    a. It depends on a variety of factors, but most of the time you can at least strongly infer that data copying has occurred if it has. Some circumstantial evidence may include details such as the fact that a removable device was attached to the computer on the last day an employee was using the computer and a large number of files were accessed quickly shortly after that attachment. There may be information identifying specific files as residing on a removable device too.

4. **I think someone forged the date a computer document was created or last changed. Can you tell?**

    a. Some times yes, some times no. Again it depends on a variety of factors such as how long the change was in effect. If just for a few minutes it may be more difficult to tell. There are many logs that can be correlated to check for time anomalies. The time change itself may even be logged if the proper settings are in place. If the computer is part of a domain with time synchronization in place, there may be error messages as the system tries to correct for the incorrect time.

5. **I think a file was sent via email to a competitor and was later deleted. Is there a way to determine that?**

    a. It will depend on the email program used, the time since the deletion and several other factors. Another issue would be if this is a corporate or other large organization environment. If that is the case, backup copies may be available that can be restored to recover the data. Also in the case of another organization, cooperation from that organization may assist in determining if they in fact received the email and still have a copy available. In addition, logs may be available that can determine if an email was sent that matches the basic criteria even if the email itself is not available.

6. **Is it OK to have our IT staff look for things on a computer first prior to requesting a forensic examination?**

    a. NO
    b. "Looking for things" by personnel not trained in proper forensic protocol will likely change and potentially limit or eliminate some or all of the data from being admissible in court. Inappropriate activity can change dates and times, corrupt or completely overwrite critical data making it no longer accessible. Even simply booting or turning on a computer will change and/or corrupt data. Just leaving a computer turned on will cause data to change and get overwritten over time.

7. **Why do we need a forensic image of the computer disk? The local computer shop will copy the disk for us. Won't that be adequate?**

    a. NO
    b. Unless done in a forensically appropriate manner with the proper hardware and software, data will be missed, data will be changed, and for the most part, the data will likely not be admissible in court if needed. Generally when copying is done by untrained personnel, only the currently "active" data will be copied, and even then, date and time information will be changed. Any data previously deleted or other data from a prior version of a file system that remains on the disk will not be copied and therefore not available for analysis and review. Proper chain of custody would also be missing. This would limit the admissibility of the potential evidence.

8. **We're thinking about requesting a forensic examination of a computer. Are there any precautions we should take while we are deciding?**

    a. If you have any sort of device, computer, removable disk, flash drive, or other media, the most important thing you need to do is stop using the device and shut it off and/or unplug it and do not turn it back on until you decide what you are going to do. If the device is already off, don't turn it on or do anything with it until decisions are made. Even leaving a computer on with no obvious activity can destroy evidence. Most Operating Systems have ongoing processes running at all times in the background that will, over time, write information to the disk thereby overwriting previously available data. This is true even if no one is logged on to the computer or it is in a "locked" state. As long as it is powered up data is at risk.

9. **If we come up with some specific words to search for and you run a search and don't find them, what else can be done?**

    a. "Keywords" are not the end-all to trying to find something specific. There are many files that can not be adequately keyword searched. These include graphics such as fax image copies, many PDFs, some email files, compressed or "zipped" files, and encrypted files such as password protected Office documents. Those files will need to be handled in a different manner or in some cases manually viewed to check for any keywords.
    b. There are also many caveats related to keywords. Some data may not be stored as expected. For example names may be stored as "FirstName LastName", "FirstName MiddleInitial LastName", "LastName, FirstName" or "Initials, Lastname". Numbers can be stored in many ways, unless you know exactly what to look for they can be easily missed. They can also be stored as results of formulas, rather than the actual number so it may not exist as expected.

10. **We think someone has stored pornography on their computer or our server. What are some of the risks our company might face and what should we do about them?**

    a. If you are only dealing with adult pornography, you should probably check with your legal department before doing anything. You may risk exposing others to something they would rather not see and the problems related to that.
    b. If you suspect child pornography or even that possibility, you need to get legal advice before doing anything. Possessing child pornography is a crime, distributing it even more so. If the situation is not handled properly, there are many bad outcomes possible.

11. **The IT administrator just left the company and won't tell us the password to our servers. Can you help?**

    a. Most likely yes. Special precautions may need to be taken. Contact us prior to doing anything. If the computer is currently on, leave it on and don't attempt anything. If the computer is off, leave it off.

12. **We just had a flood and an important computer was under water when we found it, what should we do?**

    a. Do not attempt to dry it off yourself and do not turn it on. Contact us for additional situation specific advice.

13. **Our payroll department's computer just keeps rebooting and is unusable and the payroll needs to be processed. What can we do?**

    a. Turn the computer off and leave it off. The solution will depend on the specific condition causing the rebooting. If it is some type of logical corruption problem with the data on the disk, the data can likely be recovered and put on another disk for subsequent use. The original programs would need to be reinstalled on a new computer and then the data copied to that computer.
    b. If the problem is a hardware level failure of some sort on the disk itself, (bad sectors or some other electronics failure), the drive may need to be sent to a clean room facility for repair and data recovery services.

More questions will be answered as they become available. Feel free to email any questions for inclusion in this list. Send them to: consulting@computerforensicsconsultingllc.com