Digital Forensics: Data Recovery and Steps You Can Take to Assist in the Recovery Effort

Picture this: You've been working on that all-important document for hours, and you finally save the file in its proper location with the rest of your important files. Then you decide it's time to do a little bit of file clean-up on your device. Instead of selecting one file you click on the folder with all the documents, and…BAM…delete key pressed.

Panic sets in -what are you going to do? All those needed documents are gone forever. Wait – not so fast.

In most cases those files you deleted are probably recoverable. However, there are several actions that users often take that make data recovery even more difficult. This post is aimed to prevent users from making those mistakes after deleting a file or folder.

Deleted data recovery is often called the "bread and butter" of digital forensics, and in truth, a lot of digital forensic cases involve deleted data recovery. A digital forensic professional should be familiar with the various ways computers and other electronic devices store data, and below are some questions that a reputable professional will likely ask you.

- **What type of computer/device do you have?** – This question aims to get a few crucial pieces of information that will help the digital forensic professional be able to determine what the likelihood of data recovery will be. Data recovery depends on several factors including the make and model of the device.
- **How was the data deleted?** – This is an important question because there are many ways that data can be "deleted" from a device. What is being asked is, was it simply just pressing the delete key, or was a file cleaning program being used? Did a mobile device get factory reset?
- **How long ago was the data deleted from the device and has the device been in constant use since?** – This question helps an examiner figure out some additional information about the deletion as well as helps them gauge the device's use since the deletion (more about device usage in just a bit).
- **What type of data/files were deleted?** – This question helps to narrow the scope of the data recovery efforts. When asking this question, an examiner is trying to determine what type of files you are hoping to recover (Word docs, PDFs, spreadsheets, pictures, videos, etc.)

What can you do to assist in the recovery efforts besides knowing at least some of the answers to the questions above?

DIY Data Recovery

If you have deleted data from a device, one thing that you should absolutely not do is try to recover that data yourself. When you download a program that claims it will recover those deleted files, you are installing a brand-new program on your device. Which, if you didn't know, writes new data to your device's storage media.

The new data being written to the storage media has the potential to overwrite the deleted data. When data is deleted from a device, it's often recoverable because the data either partially or completely resides in a storage media's unallocated space (this is space that is currently not in use by a device and is available for new data to be stored in). If that partially deleted data in unallocated space is

OVERWRITTEN (meaning that new data has been placed over top of the old data completely replacing it) then that data is no longer recoverable and is gone.

In a state of panic, you want to do everything that you can to try and recover the data that was deleted. However, a DIY approach to data recovery often leads to recoverable data being overwritten and is not recommended.

Device Usage After Deletion

Much like the tips in the prior section, device usage after data deletion can hinder the recovery efforts. On most devices, when data is deleted, the space that file is occupying is marked as available for new data to be written to. If new data overwrites that old data, the old data is no longer recoverable. What does this have to do with using a device after data is deleted?

If you continue to use your device after data is deleted, you are going to continue to create new data on that device. Even if you think, this is only one text message on my phone, it's fine. Maybe you decide to browse the internet for some service offerings that provide data recovery. These actions that you as a user are taking create new data on the device.

Now, these actions are not always going overwrite deleted data, but continued usage of the device may lower the success of data recovery efforts. What should you do?

You should try your best not to use that device. If it's a computer, power it down so that data cannot be created on the system. If it's a mobile device such as a phone or tablet, disconnect it from Wi-Fi and the cellular network (Airplane Mode) or simply power it off.

You should also contact a digital forensic service provider that offers data recovery services as quickly as possible. In many cases involving data recovery, time is of the essence to prevent data from being overwritten.

The Windows Recycle Bin

For a computer running Microsoft Windows, there may be a relatively simple way for you to recover some of those deleted files depending on file size and deletion method. Usually, when a user clicks on a file and presses the delete key or uses the delete option, that file gets sent to the user's Recycle Bin (the trash can icon with the three arrows making a circle).

If the deleted data lines up with the parameters of fitting in the user's Recycle Bin, that data should be there. Opening the Recycle Bin may show you some of the files that were accidentally deleted, and you should be able to recover some of them by selecting the file(s) and clicking the "Restore the selected items" or "Restore all items" options.

In conclusion, when it comes to recovering data, it is better to have someone who has knowledge of how an electronic device stores data and understands the recovery process than an unfamiliar computer program. In the long-term, hiring a digital forensic professional to recover your data will likely save you time and result in some or most of the deleted data being recovered if you follow the recommended steps.