Why Deleted Files Can be Recovered

Many of us believe that in order to permanently remove data from a device, we merely need to click 'delete' then empty our recycle bins. Whilst this certainly frees up storage space and makes it appear as though the relevant data no longer exists, however, this is simply not the case.

When you complete the actions outlined above, you inform your machine that you no longer require access to the relevant data. The machine therefore marks the space that contains this data as writeable. In other words, it does not delete it, but merely earmarks it as data that can be overwritten with new data should this become necessary. So, if you take no further steps, then the data in question will remain on the drive until it is overwritten. If you're using a Windows operating system then this data could be overwritten at any time as this system will indiscriminately write files to any viable location. Other operating systems such as OSX and Linux will automatically save new data to sections of the drive that have not held data previously.

To put it another way, deleting data via the standard removal process is like moving an important physical document from one file to another and then forgetting where you placed it. The file still exists, but you're unable to find it. Locating the document may prove to be a time-consuming and laborious process, but it can still be located with sufficient effort. Similarly, finding deleted files can also be an arduous and intensive task but, provided the data has not been overwritten, a skilled digital forensicist will be able to locate and restore it.

In order to restore a deleted file, a forensicist will simply find space that has been flagged by the drive as an area that contains data that can be overwritten. Following this having been done, the data located within this space can be identified and any that is pertinent restored.

Data that is deleted via the standardised route and many other common means of deletion is so recoverable, in fact, that many companies employ the services of third parties in order to securely dispose of their data by physically destroying the drives in question or, should they consider the data to be highly sensitive, magnetically degaussing the drive thus ensuring that the magnetic portion of the drives becomes unstable and that the data previously held on it becomes completely unreadable.