What Constitutes "Possession" of Child Pornography? Part II: Accidental Downloads

The accidental downloading or possession of child pornography occurs much more frequently than law enforcement would like to admit. The internet is saturated with these unlawful images and videos and they are encountered by innocent people every day. When an innocent person is charged with the possession of child pornography, how do we prove that the possession was accidental? To answer this question, we must first examine how accidental possession can occur.

Peer-to-Peer File Sharing Programs

The most common form of accidental downloading occurs with the use of peer-to-peer file sharing programs such as LimeWire, FrostWire and BearShare that provide access to the Gnutella network. The Gnutella network is the largest file sharing network on the internet and allows users to share music and video files for free. When the user downloads the program software, a Shared Folder is installed on the computer. Any files in this folder will be available for sharing with all other users and any files that are downloaded by the user are placed into this folder.

Many people use the Gnutella network to download pornography and the majority of it is legal adult pornography. To download pornography, the user conducts searches using terms for the types of videos he or she is looking for. The search results are typically voluminous and the file names are sometimes difficult to decipher so the user will usually drag the first 10-15 results into his Shared Folder. The files will often take over an hour to download. Once all of the files are downloaded, the user will be able to open them and watch them.

Every now and then, a file containing child pornography can be accidentally dragged into the Shared Folder and the user may not know this until it is viewed. Once the unwanted child pornography is viewed, the user will typically try to delete it (sometimes, these files contain defects that make them difficult or impossible to delete). As discussed in Part I, however, deleting the file does not remove it from the hard drive even though it may be out of sight to the user. Thus, a person who has now accidentally downloaded child pornography remains in possession of the file even well after it is deleted.

Temporary Internet Files

As discussed in Part I, when we visit a website, images and videos from the site are automatically downloaded to what are known as "cache files," or "temporary internet files." These files are downloaded without the user's knowledge and may remain on the computer for a long period of time. If a person regularly visits pornography sites, hundreds of files will be stored in the temporary internet folder as well as the unallocated space on the hard drive. Pornography sites are typically saturated with images and videos. Many times, just the home page can have close to a hundred files rotating in and out. Although the user cannot possibly see all of the images and videos rotating throughout the page, every single one of them is capable of being downloaded as a temporary internet file. If just one of these files contains child pornography, the user will be in possession of it.

Proving Possession was Accidental

With the assistance of a computer forensics expert, we can usually prove when a user has accidentally downloaded or possessed child pornography. Using software such as EnCase, the expert can retrieve data from the hard drive that enables us to retrace the steps that led to the unwanted file entering the computer.

With file sharing programs, we will search the hard drive for the search terms used by the person when downloading pornography. Very often, we can find a link between an innocent search term and the name of the child pornography file that would cause the file to end up in the search results. For instance, if the user used the search term "Female" and that word was in the name of the unwanted file. We can also survey the Shared Folder and show that all of the other files that have entered that folder were legal adult pornographic files.

Every file contains a set of properties that we can use to tell a story. The properties that we can typically recover will tell us when the file was "created" (or downloaded), when it was "last written" (or changed) and when it was "last accessed" (by anyone). These dates can be extremely important to our investigation. For example, if the properties indicate that the file was created and last accessed at the same date/time, it is quite possible that the user was unaware of the file because it was never accessed after the initial download. This is commonly seen with temporary internet files. If the last access date/time is within an hour or so of the created date/time, it may help support our argument that the user deleted the file shortly after it was viewed for the first time. Also, a file created or last accessed at a time when the user did not have access to the computer will establish an alibi.

We can typically retrieve several months of internet history which can help us show the user's general surfing habits as well as construct a timeline of the events surrounding an accidental download. Creating a timeline can also be very helpful if an alibi needs to be established. For instance, if the defense is that another user downloaded the child pornography file, we can sometimes show that this person checked his or her email, or logged into a bank account, shortly before or after the file was downloaded.

It must be stressed that very little of this data can be obtained from the hard drive without the use of a computer forensics expert. We are fortunate to be able to work with some of the best experts in the field and with their assistance we have successfully proven the innocence of many people in Georgia who have accidentally downloaded or possessed child pornography.