C13 Child Pornography in Computer Forensics: What Are the Most Relevant Pieces of Digital Evidence?

Pedro M.S. Eleuterio, MSc, Brazilian Federal Police, Campo Grande 79040010, BRAZIL*

Learning Overview: After attending this presentation, attendees will understand the essential evidence needed in a computer forensic analysis involving child pornography, including shreds of digital evidence of illegal file possession, sharing, and production. Furthermore, in these cases, the intention of the user to reach these files is one of the most important items for the computer forensics expert to prove.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by reviewing the most important pieces of digital evidence in cases of child pornography, which computer forensics experts must look for to make the forensic analysis. This presentation includes computer forensics knowledge regarding peer-to-peer tools, image and video metadata, and computer forensic analysis.

Computer forensics involving child pornography is increasing year by year. This type of digital evidence is crucial for computer forensics experts to be able to unravel related crimes, considering their country's laws. The possession of child pornographic files and their sharing are crimes in many countries. Therefore, in a computer forensic analysis, there are many pieces of digital evidence that experts must find. This study reveals some of the most relevant digital evidence in cases of child pornography in computer forensics.

First, the forensic expert must look for images and videos of child pornography stored in the digital devices. Thus, it is possible to use techniques such as comparing hash values, searching for common pedophilia keywords, using nudity detection in images, and even motion detection in videos. The EXchangeable Image File (EXIF) metadata information in images can be useful in determining if the user device has produced some pictures.

After locating the possession evidence, the computer forensics expert must look for file sharing evidence, analyzing logs of: (1) peer-to-peer programs (such as Kazaa™, Shareaza™, Ares™, Limewire, uTorrent®, eMule™, BitComet®); (2) instant messaging programs (such as WhatsApp Web, Skype®, ICQ, Google Talk®, Facebook® Messenger™); (3) web browsers' histories (such s Chrome®, Internet Explorer®, Firefox®); (4) e-mail programs and webmail caches (such Google® Mail™, Outlook®, Thunderbird™, Hotmail®, Yahoo!®); and (5) programs to access the Dark Net and Deep Web (such as Tor™ Browser, Onion Browser™). In fact, there are many programs to download and upload files, which can be used to share illegal content. Therefore, the study of the newly available tools is always crucial to the forensic expert.

However, one of the most relevant forms of evidence in these cases is to prove the intention of the user to obtain this kind of illegal content. Therefore, the forensic expert must search for the keywords used to reach these illegal files, like Web browser keyword/form list, keywords of sharing programs and visited sites, among others. In some cases, the forensic expert may find texting, sexting, and child grooming evidence, which are imperative in cases of child exploitation and child sexual abuse.

The evidence found in digital devices related to child pornography is very relevant to the solution of these cases. There are many ways to find child pornography evidence in digital devices and the computer forensics experts must be aware. After all, in some cases, the computer forensic analysis can be the only method to discover the sexual abuse of children, allowing the aggressors punishment.

Computer Forensics, Child Pornography, Pedophilia