B18 Should We Fear Peer-to-Peer? Some Basics in Peer-to-Peer Investigation

Walter T. Hart, MBA, 149 Hamerton Avenue, San Francisco, CA 94131*

After attending this presentation attendees will gain a better understanding of peer-to-peer file-sharing application installation options and artifacts, possible uses of the applications, artifacts created during use, and approaches to investigating cases involving the use of peer-to-peer file-sharing applications.

This presentation will impact the forensic science community by providing a basic understanding of peer-to-peer file-sharing in investigations involving digital evidence including risks, vulnerabilities, and opportunities.

Peer-to-peer networking and other file sharing programs have become increasingly popular with users of the internet for sharing both large and small files. Many small organizations will use the capabilities of peer-to-peer file-sharing to effectively share information about their organization without having to maintain a centralized server. These could include families, bowling leagues, social organizations, and virtually any other groups of individuals sharing the same interests or a need to access the same data. Larger organizations utilize peer-to-peer file-sharing to economically and rapidly deploy very large datasets. There are a number of legitimate business uses for peer-to-peer networking and distributed file sharing including rapid dissemination of patches for software and new distributions of games and their data.

Peer-to-peer file sharing has also become popular with distributors and others sharing illegal files or illegally sharing legal files such as intellectual property rights protected software and media including movies, television shows, music, and almost any other copyrighted material that can be stored in a digital format. With rapid and widespread distribution of files, it is also possible to distribute viruses and other malware unchecked quickly. Without proper controls, this could provide entry into otherwise secure networks by unwitting users. These illegal uses of peer-to-peer networking have created a challenge in the digital forensic community due to the volume and perceived anonymity of the process. The number of available peer-to-peer applications and incredible volume of data being shared could easily overwhelm digital forensic examiners.

As is the case with many software applications, there are similarities between the many peer-to-peer applications but the differences and the forensic artifacts created are significant. This presentation will discuss many of these applications and some differences in the artifacts created. Examples will be given of the installation, configuration, and use of some common peer-to-peer file-sharing applications. This will include some of the standard, default installation options that both hamper and help investigators in these cases. Some general approaches to peer to peer investigative cases will be examined as well as the use of available tools to assist these cases. While generally accepted investigative techniques will uncover the presence of peer-to-peer installations, there are some specific tools directed specifically at investigating these products.

The presentation will also discuss smaller subset of file sharing applications appropriately called friend to friend as opposed to peer-to-peer as they are a group of applications that employs the ability to have some level of access control before users can share or download files. This subset of file sharing applications, while using some similar processes and technology, presents even greater challenges to the investigator as users frequently must “buy” their way into the group.

Peer-to-Peer, File Sharing, Friend-to-Friend

Copyright 2012 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS. ** Presenting Author*