D31 Internet Café

Jeffrey Barefoot, Department of Defense, Computer Forensic Laboratory, 911 Elkridge Landing, Suite 300, Linthicum, MD 21090*

After attending this presentation, attendees will understand how a suspect of a crime, without eyewitnesses, can be determined through the use of digital forensic tools and examination of computer data remnants.

This presentation will impact the forensic community by showing that digital forensics can provide valuable leads to a crime even when similar cases have failed or eyewitness testimony is not available. This presentation can also increase awareness that administrators of Internet cafés, that provide computers, should implement robust user management techniques to deter misuse of their resources.

Jeff Barefoot has been a computer forensic examiner at the Department of Defense Computer Forensics Laboratory (DCFL) for approximately four years. In August 2006, a follow-on examination to a Project KIDS (PK) case for additional analysis of media seized from an Internet café computer was initiated and assigned to Mr. Barefoot. Most case requests provide a subject and allegations of a crime. In the follow-on examination, the subject was unknown. Initial analysis revealed only one user profile that was identified as a generic Internet café account. Individual accounts are generally not created on Internet cafés because of the high volume of users. Mr. Barefoot's previous cases attempting to correlate a user associated with a computer crime on an Internet café had been unsuccessful. The forensic analysis was aimed at searching the media for chat or email messages during the timeframe of four images of suspected child pornography that had been recovered in the previous case.

Forensic analysis recovered creation times of the four images, where two of the images were found in a folder on the desktop and the other two images were found in a folder in the recycle bin. While no temporary Internet history records were recovered, there were four Yahoo!® Messenger chat messages that corresponded to the same creation times of the recovered picture files. In a review of the chat messages, one chat dialog revealed a Yahoo!® user account name and a connected Yahoo!® buddy icon picture to the username were revealed. This particular chat dialog displayed an individual chatting to a purported 15 year-old-girl. The entire timeframe of the chat session occurred during the creation times of three of the suspected child pornography images. During further examination of HTML files found in web cache, Jeff was able to connect the Yahoo!® user account to a nickname and the last name of an individual. While reviewing recovered emails, Mr. Barefoot was able to connect a "Classmates" email that addressed the subject's first name, thereby now correlating the individual's first and last name.

Based on the files of the suspected child pornography recovered from the analysis, it was determined that the images originated from a web-based photo storage site named "Photobucket." During analysis of five web page files from "Photobucket" photos, two filenames corresponded with the filenames of the recovered child pornography pictures. Additionally, a larger picture appearing to match the individual in the Yahoo!® buddy icon picture was identified.

After forensic analysis of the submitted media, the case agent was provided with the first and last name of the individual, the Yahoo!® buddy icon picture, and the larger picture retrieved from the Photobucket website. Subsequently, the case agent went to the personnel office and was able to successfully pull the individual's ID card, which revealed a perfect match to the information provided by DCFL. When confronted and interrogated, the subject confessed to viewing child pornography on the submitted Internet café computer and an additional café computer. An addition Internet café computer and the subject's personal computer was later sent to DCFL for forensic analysis, and additional images of suspected child pornography were recovered.

Yahoo!® Messager Chat, Buddy Icon Picture, Photobucket Website

* *Presenting Author*