C20 Steganography Analysis: Efficacy and Response Time of Current Steganalysis Software

Jordan B. Green, BS, Marshall University, 317 Gallaher Street, Huntington, WV 25705; Ian Levstein, MS, Marshall University, 1401 Forensic Science Drive, Huntington, WV 25701; Robert J. Boggs, West Virginia State Police Digital Forensics Unit, 1401 Forensic Science Drive, Huntington, WV 25701; and Terry Fenger, PhD, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will understand the basics of steganography including methods of hiding information, applications, practical use, and the current software used to analyze hidden data.

This presentation will impact the forensic science community by educating digital forensic investigators about a form of data obfuscation that is difficult to detect in a practical setting. Awareness of its presence, especially in the realm of organized crime and terrorism, is a first step in addressing the proliferation of potentially illicit data.

Steganography, Latin for "covered writing," is a method of hiding information within digital media. In steganography, a message is embedded into a carrier or host file through means such as least-significant bit encoding, appending, or watermarking. Many file types, including audio, video, image, and text, can be embedded into carrier files of equally diverse formats. Today, steganography grows more complex with an increase in open-source applications, which hide data. As applications become more sophisticated, the need to detect, analyze, and stop the flow of dangerous information becomes more crucial.

Due to the increasing need for steganalysis software, companies like Backbone Security have developed programs that detect and decode steganography. StegAlyzer™ is a software program that detects and analyzes suspect files in order to aid law enforcement in the discovery of evidence that may condemn criminals. While there are four programs within the StegAlyzer™ suite, this investigation dealt with its Signature Search (StegAlyzerSS™) and Artifact Scanner (StegAlyzerAS™) due to their abilities to detect steganography applications and the steganography created from these applications.

Several questions were asked in this study: (1) does analysis time change with different carrier and message sizes and formats; (2) how well does StegAlyzerAS™ detect multiple steganography applications; and, (3) can StegAlyzerSS™ detect steganography from these applications? For the first question, a free application named GhostHost was selected to create steganography of differing sizes and formats. The open-source steganography applications chosen for the latter two questions were GhostHost, ImageSpyer G2, OpenStego, Steg, Steganography Studio, Open Puff, Silent Eye, Steghide, and Secret Layer.

StegAlyzerAS was able to identify signatures from five out of nine applications investigated in this study and StegAlyzerSS had a success rate of 33% in identifying steganography created by the applications. StegAlyzerSS was also used to analyze the duration of detection for image steganography created by GhostHost, a steganography appending, open-source application. Analysis time fell within the range of 0.15 and 0.25 seconds regardless of carrier or message file size. A one-way analysis of variance showed that different carrier and message sizes and formats had no statistical effect on analysis time.

Further studies should investigate StegAlyzer's™ abilities compared to other steganalysis software, such as WetStone's StegoHunt™ or open-source steganalysis software such as Steganography Studio. StegAlyzer™ is an invaluable tool for investigations of digital crimes, and requires competent analysts to be effective.

Steganography, Steganalysis, Investigation