B16 Forensic Analysis of Forensic Analysis of Spyware/Monitoring Software

Don L. Lewis, Lakewood Police Department, 445 South Allison Parkway, Lakewood, CO 80226*

After attending this presentation, attendees will be familiar with the challenges presented by the covert nature of spyware/monitoring software. An approach to identify and recover the application and its data files will be presented.

This presentation will impact the forensic community by exploring how the monitoring software, SpectorPro, is designed to be invisible to the computer user in order to avoid detection, but this results in a significant challenge for forensic examination.

Spyware/Monitoring software is marketed to consumers and businesses to monitor activities of children or employees. It is designed to be invisible to the computer user in order to avoid detection, but this results in a significant challenge for forensic examination. This presentation is the result of a case study and research in how to identify and examine spyware/monitoring software.

There are also monitoring emailer applications which monitor and email the user activity to the person monitoring an individual. Emailers have some advantages for the forensic examiner, because they send emails that are easily found in an examination. These emails appear in an unencrypted format and are easily viewed and documented. This presentation only deals with the spyware/monitoring application, which is more difficult to identify, process and examine.

Spyware, Covert Installation, Monitoring Software

Copyright 2009 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*