

## **From The Editors:**

The thirteenth issue of IJDE contains four articles we believe will be of immediate interest to our readership.

Our first paper in this issue is "Exploiting the Rootkit Paradox with Windows Memory Analysis," by Kornblum. While a number of rootkit detection kits exist, they run in memory with the rootkit, allowing it to actively evade detection. This paper explores how an examiner can create a memory image and thoroughly search it for rootkits. It is possible to infer the presence of a rootkit even without directly detecting it.

"Hidden Disk Areas: HPA and DCO" by Gupta, Hoeschele, and Rogers focuses on certain manufacturer hidden areas of a hard disk, specifically Host Protected Areas (HPA) and Device Configuration Overlays (DCO). These areas can be problematic for computer forensic investigators, since many of the common industry tools cannot detect the presence of the HPA and DCO.

Our third article, "Forensics and SIM cards: an Overview," by Casadei, Savoldi, and Gubian presents an open source tool for data objects extraction from SIM and USIM cards which is capable of extracting all observable memory and all the non-standard files that are found in every SIM card.

The final article in this issue, "Google Desktop as a Source of Digital Evidence," by Turnbull, Blundell, and Slay, while focusing on the free Google Desktop application, discusses the emerging trend of Personal Desktop Searching utilities on desktop computers, and how the information cached and stored with these systems can be retrieved and analyzed.

We are currently reviewing several articles for the next issue which should be online in January 2007. We are actively soliciting articles for future issues. Please submit as soon as possible to provide time for the peer review process.

Gary R. Gordon, Editor  
Utica College

John J. Leeson, Editor  
University of Central Florida (retired)