

TRACK: IT Security
SESSION #: IT13
DATE: Wednesday February 6, 2008
TIME: 10:00-11:00AM
SESSION TITLE: Panel Discussion
SPEAKER(S): Robert Andrews, Eoghan Casey
ORGANIZATION: P3 Strategic, Stroz Friedberg, LLC

ABSTRACT: Please join two experienced practitioners as they discuss how to deal with developing challenges in modern digital investigations, including full disk encryption, handheld devices, and sophisticated computer intrusions. Case studies are used to provide practical approaches to handling fully encrypted systems, preserving and examining information on cell phones, and insight into advanced hacker tools and techniques.

SPEAKER BIO(S): Robert Andrews is co-founder of P3 Strategic, a forensics investigation and training firm. He currently is CTO and lead investigator. Robert A. Andrews II is a security consultant and trainer as well. He previously was the lead instructor and program coordinator of the IT Security and Forensics Associate Degree program at Pittsburgh Technical Institute. His service experience includes working with several Fortune 500 companies and governmental agencies at the local, state and federal levels. His experience also includes teaching high level security certification programs, CISSP and Cisco boot camp classes around the nation. Rob has been a technical editor for and has collaborated on several IT certification manuals for Course Technology and McGraw-Hill. He has also been the Key Note Speaker at many National Information Technology seminars including several ISSA/ISACA organizations nationwide. He is also a member of the International High Technology Crime Investigation Association.

Eoghan Casey is one of the leaders in the field of digital forensics and high-technology crime investigations. He co-manages the firm's technical operations in the areas of computer forensics, cyber-crime response, incident handling, and electronic discovery. He maintains an active docket of cases himself and has extensive experience managing complex investigations and preserving, harvesting, and analyzing relevant digital evidence. He has performed hundreds of forensic acquisitions and examinations, including e-mail and file servers, handheld devices, backup tapes, database systems, and network logs. He has regularly applied digital forensics in response to security breaches to determine the origin, nature and extent of computer intrusions and has utilized forensic and security techniques to secure the affected networks.