International Workshop on Cyber Crime
IWCC 2013

Workshop Introduction

Today's world's societies are becoming more and more dependent on open networks such as the Internet - where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and numerous information security issues which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals.

Moreover, the frequently occurring international frauds impose the necessity to conduct the investigation of facts spanning across multiple international borders. Such examination is often subject to different jurisdictions and legal systems. A good illustration of the above being the Internet, which has made it easier to perpetrate traditional crimes. It has acted as an alternate avenue for the criminals to conduct their activities, and launch attacks with relative anonymity. The increased complexity of the communications and the networking infrastructure is making investigation of the crimes difficult. Traces of illegal digital activities are often buried in large volumes of data, which are hard to inspect with the aim of detecting offences and collecting evidence. Nowadays, the digital crime scene functions like any other network, with dedicated administrators functioning as the first responders.

This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

The aim of this workshop is to bring together the research accomplishments provided by the researchers from academia and the industry. The other goal is to show the latest research results in the field of digital forensics and to present the development of tools and techniques which assist the investigation process of potentially illegal cyber activity. We encourage prospective authors to submit related distinguished research papers on the subject of both: theoretical approaches and practical case reviews.