Computer forensics - digital fact-finding in trusted hands

Computer forensics is the process of acquiring, analyzing and documenting digital evidence. Xandstorm conducts high grade forensic IT examinations utilizing equipment and software, generally considered 'industry standard' within both Intelligence & Security, and Law-enforcement communities.

The objective of computer data examination and analysis is to disclose facts as recorded on computer systems and electronic media, in a forensically sound and non-biased manner. It entails following the chain of evidence as it unfolds.

Forensic examinations can be divided into the following categories:

**Disk forensics**

Disk forensics encompass the acquisition and analysis of data stored on physical storage media like computer hard drives, volatile memory, and removable media. It includes the recovery of hidden, encrypted and deleted data, as well as file identification and the extraction of meta-data, the proverbial 'data about the data'.

**Network forensics**

Network forensics is the process of examining network traffic, including transaction logs and real-time monitoring. It concerns the capture, recording, and analysis of network events. The objective of network forensics is to disclose the source of IT related security breaches and includes both physical and virtual network environments.

**Internet forensics**

Internet forensics is the process of uncovering where and when a person or organization has utilized the internet or company intranet with malicious intent. For example with regard to digital financial fraud, corporate espionage and identity theft. It seeks to identify, extract and report evidence related to such uses.

**E-mail forensics**

Electronic mail is still one of the most common ways persons and organizations exchange information, and which is not seldom of a confidential nature. E-mail forensics encompass the analysis of source and content of electronic mail as evidence. Among others it includes activities like identifying the actual sender, recipient, date, time, and location an email originated from or was sent to.