KEY ASPECTS OF

Digital Forensic in Cybersecurity

DATA RECOVERY

Our digital forensics experts use specialized tools and techniques to recover data from various digital devices, such as computers, mobile phones, servers, and storage media. This data may include files, logs, databases, and more.

EVIDENCE PRESERVATION

We are strident about preserving the integrity of digital evidence to ensure it remains unaltered during the investigation. This involves creating forensic copies (bit-for-bit copies) of the original data, maintaining a detailed chain of custody, and ensuring that the evidence is stored securely.

ANALYSIS

Our E-Panzer team analyzes the collected data to discover relevant information. They may look for signs of malicious activity, unauthorized access, data theft, or any other activity related to the investigation.

IDENTIFICATION AND ATTRIBUTION

In some cases, our digital forensics will be able to help identify the source of an attack or a breach. This process involves tracing the digital trail back to its origin, which can aid in identifying the perpetrator.

DOCUMENTATION AND REPORTING

The findings from the digital forensics investigation are typically documented in detailed reports that can be used as evidence in legal proceedings. These reports should be comprehensive and clear, providing a timeline of events and the methods used during the investigation.

EXPERT TESTIMONY

Our digital forensics experts are often called upon to testify in court as expert witnesses to explain their findings and the relevance of the digital evidence to the case.

source: www.e-panzer.com