



## COMPUTER FORENSICS

## Cyber Investigations, Incident Response and Computer Forensics

The volatility of electronic evidence requires that strict procedures are followed during all acquisition, handling and analysis activities. Investigations are always performed by computer forensics experts that have an extensive expertise and training in the field and that employ specialized tools in order to ensure the admissibility of the evidence.



For over 30 years, OKIOK proved themselves as market leaders thanks to the strength of its specialists in the field of information security.

The involvement of OKIOK in computer forensics is a natural progression of the specialized services it provides to its customers.

Committed to providing a personalized service, OKIOK offers a pragmatic and tailored approach for each engagement, taking the utmost care in respecting the confidentiality and reputation of the client and the deadlines specific for each litigation.

Ever since computers and the Internet have become integral parts of our lives, legal disputes and litigations involving information technology systems are becoming more and more common. Because of this, computer forensics has become a specialized field of information security in growing demand in recent years.

Our team of cyber investigators and forensics analysts is experienced in rapidly handling a variety of investigations related to situations such as:

- Disloyal employees
- Information theft
- Possession of pornography
- Breach of contract
- Industrial espionage
- E-mail fraud
- Disputed dismissals
- Web page defacements
- Defamation
- Criminal evidence
- Computer hacking



## Training and specialized tools

In the case of computer forensics investigations, the suspect computers and other electronic devices must be thoroughly analyzed in order to determine if they were used to commit a crime or other illegal acts. The complexity of these investigations demands that this analysis is performed by computer forensics experts that have the required experience, training and tools to handle electronic evidence.

In order to ensure that the analysis and evidence are admissible in court and are robust against any attempts at their invalidation, OKIOK employs a series of specialized tools such as:

- Media duplicators
- Forensics analysis specialized tools
- Cryptanalysis tools
- Tools specific to the target field (e.g. video, audio, etc.)
- Live forensics tools

Moreover, OKIOK customers can rely on a team of specialists that have advanced training and certifications such as:

- Computer Hacking Forensic Investigator (CHFI)
- Encase Certified Examiner (EnCE)
- GIAC Certified Forensics Analyst (GFCFA)
- Certified Information Systems Security Professional (CISSP)
- Information Security Master of Science
- Bachelor of Laws
- Bachelor of Engineering

## Forensics services offered:

1. Forensically sound acquisitions
  - Hard drives (workstations, servers, etc.)
  - Individual files
  - Portable media
2. Smartphones
3. Tablets
4. File integrity analysis
  - Documents
  - Vidéo
  - Audio
  - Image
  - Other
5. Cryptanalysis and encryption cracking
6. Analysis of submitted evidence and support for an action or defense
  - Reliability
  - Correctness
  - Flaws / Limits

7. Anti-forensic
  - Identification of falsified electronic evidence
8. Analysis of contentious emails
  - Identification of originator
  - Content alteration
    - i. Metadata
    - ii. Body
9. Malware identification and analysis
  - Spyware
  - Trojan horse
10. Technical support during seizures
11. Identification and correlation of traces
  - Following a breach
  - Following an information leak
  - Following the tampering of systems

## Protection of evidence and rigorous analysis

The handling of the evidence obtained by our specialists is given the utmost care in order to ensure its integrity throughout the process: acquisition, duplication, analysis, processing and presentation.

Any evidence obtained by OKIOK is handled according to an explicit engagement protocol that ensures the confidentiality, integrity, chain of custody and reliability of the evidence in court. In addition to the strict procedures followed by the OKIOK specialists, they make use of a secure forensics laboratory, physically secured areas, safes and secure transport containers.

The OKIOK expert witness present the results of their analysis and their opinions, in the form of reports, presentations and where required verbal testimonies supported by written expert witness reports, for example, in the case of civil, penal or criminal courts.



Trademarks are the property of their respective owners

OKIOK is a leader in the field of computer security. Since 1973, the company has distinguished itself through the excellence of its products and the high quality of its services. OKIOK offers a wide range of integrated solutions designed to meet the needs of organizations of all sizes.

