CENSUS
IT Security Works

DIGITAL FORENSICS

Digital evidence plays a crucial role in modern crime investigations, since people rely more and more on computer infrastructures for both business and personal affairs. Crimes involving the unauthorized access to systems, processes and data, corporate espionage, cyber-warfare but also identity theft, are all activities that are associated with some form of data manipulation, and as such, leave a **digital trail.** It is the job of a **Digital Forensics Investigator** to examine such trails and uncover concrete evidence that is non-repudiable and suitable for **supporting a case in court.**

The findings of a Digital Forensics investigation can also be of use outside of the courtroom. For example, a Digital Forensics investigation can reveal key information about an attack in an **Incident Response** scenario. There the investigator is called to determine the extend of compromised resources, the timeline of the attack, the technical details of the attack and the repercussions to the IT infrastructure as a whole. This scenario usually entails the examination of live (i.e. production) systems and processes that must be restored to a secure state within a minimum amount of time.

Digital Forensics may also be useful in cases where an organization requires more **insight into the actions of a particular user** of an information system, in order to prove or disprove a certain hypothesis.

THE CENSUS DIGITAL FORENSICS SERVICES

CENSUS offers Digital Forensics services to customers worldwide, through its state-of-the-art Forensic Analysis Laboratories. The labs' resident investigators are Computer Scientists with distinguished credentials and extensive prior experience in the field of Digital Investigations.

For the purposes of an investigation, evidence can be collected from:

- Desktops, Servers & Laptops
- Mobile Phones & Tablets
- Networking Equipment & Embedded Systems
- USB Flash Drives, SIM cards & other Storage Media

To identify and correlate evidence, the investigators use a multitude of techniques:

- Through **Disk Forensics** the timeline of user and application actions is reconstructed, based on filesystem data and metadata of both existent and deleted files.
- Through **System Forensics** events are correlated with those recorded on system log files and application data.
- Through **Memory Forensics** suspicious applications are identified, that were resident in memory at the time of an incident.
- Through **Network Forensics** suspicious communications are identified, that were made during the time of an incident.
- Through **Malware Analysis** the purpose and capabilities of suspicious software are analyzed in depth.

DATA ACQUISITION

CENSUS follows a Data Acquisition methodology that ensures that all acquired data have been collected in a non-intrusive manner and that the investigated system's original environment has been preserved. The acquired data are accompanied by a **Chain of Custody** document that describes the type of data collected and how these were handled.

DATA EXAMINATION

All data collected during the Data Acquisition step are examined in a **"clean room"** environment at the Forensic Analysis Laboratories. Through scientific analysis methods and correlation of data from different sources, CENSUS investigators identify digital evidence that is associated with high confidence values. Evidence that is deemed as trustworthy and non-repudiable will make it to the Timeline of Events, a reconstructed journal describing key events that occurred on the investigated environment during a period that is of interest to the case.

THE REPORT

CENSUS provides clients with a detailed report on the investigation findings, describing all evidence found along with the methodologies used, in a format suitable for submission in court.

INCIDENT RESPONSE

During Incident Response, CENSUS provides instructions for the safe recovery of affected systems and processes. Organizations interested in having their staff educated on "first responder" best practices may consider the CENSUS "Incident Response" training course.

EXPERT WITNESS TESTIMONY

CENSUS Digital Forensics experts are ready to deliver an **Expert Witness Testimony** in court when this is required. During this testimony the investigation findings are presented in simple terms, suitable for non-technical audiences. The Expert Witness Testimony (or other supportive material from the investigation process) can also be made available in video format.

WORKING WITH CENSUS

CENSUS works closely with clients and legal counsels so that the findings presented in its reports will support its customers in the best possible way. Our investigators provide **early feedback** on investigation results so that:

A. clients may experience shorter recovery times in Incident Response scenarios and,
B. legal counsels may have a head start at managing the newly discovered information.

As a final note we must stress the importance of an **early investigation.** Wasting time may result in the corruption of precious evidence and the disruption of business critical processes.

So if you have an indication that something is wrong within your IT environment, do not hesitate to call an investigator! CENSUS will be happy to investigate your case and support you with solid evidence, collected in a scientific manner and presented in the best possible way. This information may be the key factor for protecting your business and personal interests.

CENSUS
IT Security Works

Stadiou 33, 10559,
Athens, Greece
T. +30 2110 128 355
F. +30 2310 947 234

I. Gkoura 16, 54352,
Thessaloniki, Greece
T. +30 2310 947 233
F. +30 2310 947 234

E. info@census-labs.com
www.census-labs.com