



census[®]

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 search for concrete evidence that is non-repudiable and suitable for presentation 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 information about the timeline of an attack in an **Incident Response** scenario, where the investigator is called to assist in securing an infrastructure that has received the attack. 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.

By scanning the contents of computer **storage devices**, the Digital Forensics investigator is able to retrieve older versions of (sometimes deleted) documents and thus is capable of recreating a timeline of events describing a document's history. In much the same way, the investigator can get information on events that have occurred throughout the lifetime of a file system and thus trace the actions of a saboteur in a corporate espionage scenario. Ancillary information such as **network traffic traces** and **log files** are also very important, since they provide a means for event correlation and ultimately, evidence evaluation.

A Digital Forensics analysis can also be applied to computer **memory resources**, allowing for the detection of stealthy malware applications (e.g. trojans). Unfortunately, due to the volatile nature of computer memory, this technique is limited only to the discovery of information that has been resident in memory since the computer's last power cycle.

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. Their ongoing research efforts allow Census to provide high quality services to its clients and spearhead the competition. Census investigators use a mixture of internationally acclaimed, cutting edge and in-house developed technologies to perform data examination, but also apply advanced techniques, sometimes borrowed from other disciplines (e.g. reverse engineering), to further analyse the investigation findings.

The Investigation Process

The Census Digital Forensics Investigation process consists of four phases: the Data Acquisition phase, the Data Examination phase, the Report Preparation phase and the Expert Witness Testimony phase.

Data Acquisition

During the Data Acquisition phase the investigator collects information about the case and data from the under examination systems. Data collection happens in a non-intrusive manner, making sure that the original system's environment has been preserved.

Data Examination

The data collected in the previous phase are examined in a "clean room" environment at Census Labs. Through scientific analysis methods and correlation of data from different sources, Census investigators seek digital evidence that is associated with high confidence values. Evidence that is deemed as **trustworthy** and **non-repudiable** is then further analysed in order to build a **timeline** of the events that occurred on the investigated environment.

census[®]

census[®]

Digital Forensics

Report Preparation

Census provides its 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.

Expert Witness Testimony

Census Digital Forensics experts can deliver an Expert Witness Testimony in court, if so required. During this testimony the investigation findings are presented in simple terms, suitable for non-technical audiences.

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.

Census Digital Forensics services are designed in a cost-effective manner, allowing Census clients to achieve the highest possible returns from their investment in Digital Forensics. Census provides the following service options, giving clients the opportunity to select the type of service that best suits their needs:

- On-site Data Acquisition service
- Delegated Data Acquisition
- Standalone Data Examination service
- Standalone Data Recovery service
- Reverse Engineering service
- Malware Analysis service
- On-site Incident Response service
- Remote Incident Response service
- Personal Testimony in Court
- Expert Witness Testimony in video format

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[®]

