Computer Forensics & Data Recovery

A Computer Forensics investigation can be initiated for a variety of reasons. The most high profile are usually with respect to criminal investigation, or civil litigation, but digital forensic techniques can be of value in a wide variety of situations, including perhaps, simply re-tracking steps taken when data has been lost. In Nevada as in most states, you need to be a licensed Private Investigator to conduct theses Computer Forensics exams. We are licensed to do so, which allows us to do compete consulting work while protecting your interests.

Like DNA, Computer Forensics has the potential of developing both inculpatory and exculpatory evidence that without its use, will remain hidden. One definition is analogous to "Electronic Evidentiary Recovery," known also as e-discovery, requires the proper tools and knowledge to meet the Court's criteria, whereas Computer Forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.

The forensic examiner renders an opinion, based upon the examination of the material that has been recovered. After rendering an opinion and report, to determine whether they are or have been used for criminal, civil or unauthorized activities. Mostly, computer forensics experts investigate data storage devices, these include but are not limited to hard drives, portable data devices (USB Drives, External drives, Micro Drives and many more). The objective being to provide digital evidence of a specific or general activity. Computer Forensics is only a tool, it is not a substitute for investigation. But, with some estimates that 85% of the time, some evidence of illicit activity can be found on computers, it is a tactic we always consider. Examples include:

- Incident response to theft, divorce, criminal activity.
- Employee internet abuse (common, but decreasing), employee communications.
- Unauthorized disclosure of corporate information and data (accidental and intentional).
- Industrial espionage.
- Damage assessment (following an incident).
- Criminal fraud and deception cases.
- Employee downloading of Adult pornography.

DATA RECOVERY

STORY: I'm notified by the client that a formerly trusted partner has taken $500,000 from the joint business accounts. On his haste to leave town and change his identity, he forgets his office computer. After seizing the computer, and 13 hours of data recovery, I was able to recover a deleted file called "to do list." This document literally was his "to do" list on everything from bank withdrawals, to device destruction and his top choices on new places to live. He was captured several months later and this document proved intent, and sealed his guilty plea.

As an Air Force Electronic Warfare Officer, Mr. Jones has been government trained and is a Certified Specialist in Ethical Hacking, Data Recovery and Computer Forensics Examiner by the Information Assurance Certification Review Board.