

Rod Gregg

Rod Gregg has been in law enforcement for the past 22 years. He served with the Garland Police Department in positions as a patrol officer, hostage negotiator, rescue diver, detective, supervisor, SWAT team member and computer forensic examiner. He was assigned to the North Texas RCFL in 2000 where he served until his retirement in December of 2003. One day later, he joined the Federal Bureau of Investigation as an Information Technology Specialist – Forensic Examiner. He is the system administrator for the Evidence Control System, consults with forensic software vendors regularly and teaches various FBI-sponsored courses nationally. He has recently been selected to become a forensic video examiner. He is certified by the FBI to perform forensic examinations of Wintel systems, Unix/Linux systems and PDAs.

Abstract

Simply put, computer or digital forensics is the examination of digital evidence in a manner that protects the integrity of the evidence so that it may be used and testified about in a court of law or legal process. Too often, bad things happen to digital evidence at the hands of well-meaning private citizens, company employees and law enforcement officials. Sometimes, the damage renders the would-be evidence unusable. Before a forensic examination can occur, there must be the legal authority to do so. Improperly obtained evidence has the same value as no evidence at all.

Ideally, we could rewind the clock and go back in time to a point before the crime occurred and work with system administrators, legal advisors, corporation executives, and IT specialists to set up a system that would prevent any and all cracks, intrusions, counterfeiting, theft of trade secrets and acts of fraud to name a few. But since we can't do that, we will do our best to prepare everyone for the eventuality that their computers and systems might one day be used in a criminal enterprise or come to contain digital evidence. Cyber investigators will need logging turned on, gateway configurations, patch information, access lists and other items to prove up their case. System Administrators going out on their own should be very cautious about their efforts to help law enforcement. Generally, the key is integrity and validation. Once the crime has been discovered, the best practice is to notify the appropriate law enforcement agency right away and speak with the specialized investigators. They will guide you as to what they need to be done... or not done right away. Generally, they will ask you to isolate the affected systems and preserve all digital information until they come for it. In some cases, there is much hand-wringing at the executive level and legal office followed by gnashing of teeth by system administrators. The best practice would be to work out the likely scenarios with those likely to have input into the company's response and have those steps in place... before the crime occurs. This will improve law enforcement's response to your incident and reduce the anxiety that naturally comes with it.