Departing Employees: Beyond IT Email Search

OCTOBER 2011

Computer forensics can quickly provide useful insight into your employee's activities

COMPUTER FORENSIC INVESTIGATIONS CAN HELP IDENTIFY, RECOVER AND ORGANIZE EVIDENCE THAT IS DIFFICULT TO LOCATE AND DECIPHER

- Preservation of Evidence
- Webmail (Yahoo!, Gmail, etc.)
- Instant Messaging / SMS Chats
- Copied Files / Company Information
- Violations of Employee Policies
- Deleted Evidence
- Hidden Backups
- Proof of the "Cover Up"
- Suspicious Activity Timelines
- Chain of Custody & Authenticity

One of your key employees just left or is about to leave to join a competitor. You've asked IT to search his email and have a look at his computer, but they don't see anything of concern. What more may result from a forensic investigation?

Evidence of disloyalty, theft and malfeasance

- Preservation of Evidence: It's best not to turn on or examine suspect computer(s) until you have created a write-protected forensic image. If the computer(s) were left on you may want to capture memory. IT personnel may lack the specialized equipment and experience to do this. As a result, their examination may result in the loss of valuable evidence and earn time in court explaining why we haven't tampered with or altered evidence.
- Webmail: Most employees know that their employer can monitor their work email account, so it is common to use Yahoo!, Gmail or Hotmail email accounts for activity an employee does not want his employer to see. Forensic investigations may recover relevant webmail emails or fragments of webmail emails accessed on a computer.
- Instant Messaging / SMS Chats: People tend to be fairly casual and open when chatting through IM on computers or smartphones. Forensic investigations may recover backups of these chats even if the computer examined was not used to type them in.
- Copied Files / Company Information: There are many ways to take company files – e.g., you can email them to yourself, copy them to a thumb drive or upload them to cloud-based storage like Dropbox. Forensic investigations may uncover what files were copied, when they were copied and where they went to.
- Violations of Employee Policies: Forensics can provide insight into what an employee was doing before leaving, such as improper moonlighting, web surfing or working for a competitor before leaving.
- Deleted Evidence & Hidden Backups - the "Cover Up": Employees engaged in wrongdoing may make an effort to cover their tracks by deleting files or evidence. A forensic investigation may recover the deleted evidence, and potentially establish both the wrongdoing and the attempt to cover it up.
- Suspicious Activity Timeline: A good forensic investigator should have a sense for what data matters, and be able to find much of it quickly. A timeline detailing suspicious activity during key time periods can provide the facts you need to quickly make informed decisions.

RESURGANT
COMPUTER FORENSICS, INC.

650.799.7051 mobile
650.832.1530 office
www.resurgant.com

CA Private Investigator license #27408

Resurgant Computer Forensics, Inc. offers expert technical analysis, advice and support services when dealing with computers or electronically stored information. Resurgant is based in California's San Francisco Bay Area. Resurgant's director and lead examiner, Wayne Hale, practiced as a licensed California attorney and investigator with a multinational law firm for seven years before starting Resurgant. Resurgant has substantial experience conducting computer forensic investigations in civil matters, such as those involving trade secret/IP theft, corporate espionage, spoliation and employee malfeasance.