



# WELCOME



In the arena of law enforcement digital forensics is primarily considered a post-mortem activity: actions performed after a crime has been committed to help punish those responsible. In a Corporate environment, however, digital forensics can also help a business to prevent a crime from occurring and this pre-emptive action can save money that in most cases would otherwise be unrecoverable. In many cases Employers aren't even aware a crime is being committed.

Employees, as part of a business enterprise, have access to many kinds of physical and intangible assets not limited to their desktop PC:

- Mobile Devices like Cell phones, Laptops, and PDAs
- Networked resources like storage devices and printers
- Phone systems
- Usernames and Passwords
- Software and Software licenses
- Confidential business records and intellectual properties

Disgruntled employees are more than a cliché – when an Employee chooses to abuse company resources they can become a serious and costly liability. Employees have been prosecuted for violating contractual obligations, abandoning fiduciary duties, stealing proprietary business information, participating in unfair business competition, forging business records and receipts, fraud, destruction of records, and impersonation.

In recent national news a corporate Vice President, aware he was about to be laid off, stole business contacts and process information with which he started a competing company. In another recent headline a woman abused her access to corporate records to impersonate a business and forge more than \$500,000 dollars in checks. Although these are both examples of Employees exceeding the scope of authorization that their Employers entrusted them with they are also both examples of crimes that are completely detectable and preventable.

Employees may commit more than high crimes, as well, that may provoke censure and reprimand. Installing unauthorized applications allowing them to download copyrighted materials from P2P services, downloading and viewing pornography, and engaging in harassment are common behaviors. These relatively benign violations can still cost a business in terms of lost productivity and time.

There are important ways that businesses can protect themselves, though. First and foremost every business should have a documented policy explaining what kinds of behaviors are permitted using company resources and outlining those that aren't. This **acceptable use policy** should also explain to employees that, while using those company resources, they have no expectation of privacy and may be monitored. Employers can then request specialists to verify whether a crime is occurring and provide corporate officers with information they need to take action. Many businesses believe, admirably, that employees should be treated like family and are reluctant to search employee PCs when they feel it unlikely that employee has done something wrong. From a financial perspective, however, it is in the best interest of every business to include an investigation, however brief, as part of an exit interview.

## FORENSIC DIGITAL DETECTIVES, L.L.C.

45 EXCHANGE BLVD, SUITE 1017  
ROCHESTER, NY 14614

TELEPHONE: (585)232-3916

TOLL FREE: (866)651-2336

FAX: (866)448-5655

EMAIL: [INFORMATION\\_REQUEST@FDDUSA.COM](mailto:INFORMATION_REQUEST@FDDUSA.COM)

WEBSITE: [WWW.FDDUSA.COM](http://WWW.FDDUSA.COM)

### CUTTING EDGE TECHNOLOGY FOR THE DIGITAL AGE