Computer and Cell Phone Forensics

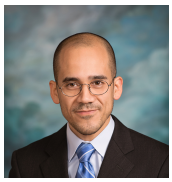
Certified in Computer Security and Information Assurance, GWU

Certified in Digital Forensics; CCE, X-PERT, EnCE, ACE, CCME

MS in Computer Science, GWU

Discreet Evidence Collection Without Alerting Staff or the Media

Documented Chain of Custody



Contact

Michael Yasumoto
Senior Forensic Examiner
Deadbolt Forensics, LLC
1915 NW AmberGlen Pkwy
Suite 400
Beaverton, OR 97006
(P) 503-683-7138
(F) 503-296-5504
michael@deadboltforensics.com

Forensic Services

Law Firms

Whether it's recovering documentation of hidden assets in a divorce case, authenticating multiple revisions of a will and last testament, or using Internet history to establish that a parent is unfit in a custody battle, digital forensics has a place in any case involving electronic evidence.

In a society where everyone carries a computer in their pocket that monitors their location and personal communications, criminal cases can hinge upon proper analysis and reporting of the digital evidence involved. With large case backlogs, budget cuts, and limited training, it is often sound advice to verify law enforcement's analysis of the electronic evidence with your own independent examination.

Businesses

All too often, confidential information is removed from a company by departing employees. This problem is compounded by the prevalence of USB drives and disc media, which are now ubiquitous and constantly increasing in size. Your highly guarded intellectual property can literally be in someone's pocket as they walk out the door to start up a new business or join a competing firm. Something as trivial as personal email access from a corporate machine can allow transfer of documents directly to competitors or employee homes.

A similar risk is encountered when former employees file suit alleging wrongful termination, harassment, discrimination, or compensation irregularities. In such cases, evidence can be fabricated in support of the claims before an employee leaves the company.

The risks and associated costs of these scenarios can be greatly mitigated by preserving forensic copies of hard drives and phones for all departing staff. As time passes, the difficulty and expense of examining deleted evidence increases greatly, which is why preemptive preservation yields significant savings in the long term. In situations where litigation is inevitable, an initial examination of the digital evidence can provide crucial information for making informed decisions regarding an effective defense and avoiding costly drawn out litigation. In many cases, a preliminary exam will reveal evidence of fraud, theft of digital assets, and misuse of corporate property resulting in the filing of counter claims.

Examinations Include

- Identifying recently attached storage devices
- Restoring deleted files and formatted drives
- Checking for signs of data destruction and spoliation
- Determining internet activity, including sites visited and search history
- Defeating password protected and encrypted files
- Recovering e-mails, chats, and text messages
- Constructing a timeline of user activity