

# eForensic Focus

www.ExpertDataForensics.com

MARCH 2010

## COMPUTER FORENSICS AND WHITE COLLAR CRIME



Data & Computer  
Forensic  
Investigator  
(NV PI Lic#1498)  
Adrian Leon Mare



In the wake of fraudulent charity scams, stealing money intended for disaster victims, and investment banker, Bernard Madoff being sentenced to a prison term of 150 years, it seems white-collar crime is something that cannot be escaped these days. White-collar crime overlaps with corporate crime because the opportunity and ready availability for fraud, bribery, insider trading, embezzlement, computer crime, identity theft and forgery to white-collar employees.

It's important to look at the circumstances and evidence from all angles. Today's corporate markets are competitive, it is thought that some will try to frame others or set them up for failure in order to benefit themselves. This thought process can lead to false accusations. Computer and cell phone forensics examinations can help to prove either way. Was an individual framed? Or it likely that they committed the crime? (Con't)

We examine their wireless service, remote access to their computer. An IP address record that does not match. Whatever is on the device (s) in question.

### State-Corporate Crime

The negotiation of agreements between a state and a corporation will be at a relatively senior level on both sides; this is almost exclusively a white-collar "situation" which offers the opportunity for crime. White-collar crime has become a priority of law enforcement. In 2002, U.S senate passed the Sarbanes–Oxley Act of 2002, also known as the 'Public Company Accounting Reform and Investor Protection Act', is a United States federal law enacted on July 30, 2002.



### What to Do If You Are Suspected or a Victim in a White-Collar Crime?

Most people involve a Computer Forensic expert when they suspect accounting fraud, money laundering, or conspiracy. If you think white collar crime is happening in your company, confiscate all things belonging to the company from the suspicious employee (s), including: company laptops, assigned desk computers, thumb drives, camera memory cards, and smart phones. Additionally, step your security and protect your valued technological information. Change your passwords, get new firewalls and take action against the suspected employees.

In most white-collar criminal cases, the case can quickly boil down to a "he said, she said" fiasco. It's important to get help that does not have an interest in either party.



Follow me on

TWITTER:

DataForensics

You may consider getting a moderator and definitely a licensed Computer Investigator.

If **you** are accused of committing a white collar crime, get an attorney and hire a licensed Computer Investigator. The Investigator can make forensic images of all media used and determine whether or not there is evidence supporting your accuser's claim.

A Computer Forensic Expert can properly seize evidence: company computers, assigned laptops, Blackberrys, CDs. Retrieve emails, chat records, user histories, etc. Authenticate the evidence, analyze the findings, and create reports that are helpful and admissible in a court of law.



It's important to preserve data as it is when the suspicious activity is first discovered or hypothesized. A Computer Forensic Investigator will make a forensic image of the accused's data. Do not try to do this yourself! By doing so, you risk making the evidence inadmissible to court, use a professional.

There is a lot that a Computer Investigator can gather from a person's belongings, files and emails, especially, can be crucial to a case. As stated in February's newsletter, deleted files are rarely, truly gone. The Master File Table (MFT) in most computer systems; such as Windows XP or Windows Vista, simply change their index when a file is deleted to mark that file space as available for overwrite. Because a user cannot indicate to save a new file directly over the deleted file's indicated space, the deleted file may remain there for a lengthy period of time, making it accessible for retrieval by a licensed Computer Investigator.

Concerning email; due to many email applications, (such as Microsoft Outlook) are essentially a database, email continues to be stored after deletion until an application level elimination is performed, or until the database grows to be too large and automatic maintenance is performed by the operating system.

The database itself is similar in some ways to an MFT, in that the deleted data (email) is no longer in the database index when deleted, but remains within the database. Computer Forensics tools and techniques provide the recovery of deleted email, bypassing the index. Familiar web based email systems such as yahoo.com, does not use



an application such as Microsoft Outlook to send, receive and store mail. Instead, the user simply navigates to particular web page and logs on the email system. Rather, the user navigates to a particular web page and logs on the email system.

The folders that are created by the



user are stored on servers hosted by the email providers, not the user's local computer.

If you are involved in a white collar crime, take action.

To receive this newsletter electronically via email subscribe at;

[ExpertDataForensics.com](http://ExpertDataForensics.com)

and click on

"**Contact Us**" to go to the subscription page.

Call **888-355-3888**

**ext (802 )**

**702-435-8885**

**We Can Help**

**ExpertDataForensics.com**

Follow me on...



***What's in our lab.....***

*Domestic Dispute: 2x*

*Data Recovery: 3x*

*Child Exploitation: 2x*

*Corporate Dispute: 5x*