

FEBRUARY 2010



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



The use of a Computer Forensics Expert can be extremely effective in building and collating evidence in family law matters such as: divorce cases with larger estates, complicated businesses, real estate holdings or cases with multi-jurisdictional assets, proving/disproving parental competence or harassment. Most cases of custody and visitation have been solved or modified because of computer evidence recovered by a Computer Forensics Expert. Experts assist attorneys in the recovery of financial information, decryption of passwords, recovery of instant messages and archived data.

In family law matters, the analysis of the spousal or family computer should always be seriously considered. Deleted files are rarely, truly gone. In most computer systems running Windows XP or Windows Vista, there is an index called a Master File Table of (MFT).

When a file is “deleted” on MFT all that really happens is that changes are made to the MFT’s index entry to indicate that space occupied by the “deleted” file is no longer needed and is available for use. The “deleted” file still resides at the same physical location, but the operating system no longer knows about it. The file will stay there until a new file is placed into the same physical sector location by the MFT. Since standard hard drives now have capacities usually over 100GB, the chances of the same physical sector location being assigned by the MFT to store a new file are greatly reduced, making recovery of deleted files more likely by using forensically sound tools and techniques.

Perhaps the most obvious searches when it comes to family law matters are web history and email searches. Names of visited

websites can provide valuable information on a person’s action or character; others can provide credible evidence to the possibility of secret assets and bank accounts.

Microsoft Windows operating system has a feature that makes a local copy of the WebPages you visit. This feature was designed to provide faster service but can create important information for a family law attorney. A licensed Computer Forensic Expert can recover the local web pages that are stored in a hidden system area and recover web pages that were created in this



manner previously, that have since been deleted by the operating system as part of its routine maintenance.

A licensed Computer Expert can find search terms used in an online



Follow me on
TWITTER:
DataForensics

search engine in the very same manner. This information has provided very important information of intent or interests. Fore example, intent to acquire information on offshore banking, illicit images or locating a safe haven to store hidden assets, or intent to meet new people.

EMAIL

Recoverable deleted email can make or break a case. 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 OS.

The database itself is similar in some ways to an MFT, in that the deleted data (email) , *Cont’d*



Remember:

~Just because you hit “delete” doesn’t mean the file is truly gone.

~Online email accounts may require a subpoena to get the email records.

~Never try to do a forensic search yourself, you risk making evidence inadmissible to court.

~ Always use a licensed Computer Expert.

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 www. 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 provider, not the user’s local computer. Recovering these pages is not much different from recovering internet history. Tracking the source of web based email can be tricky and may ultimately result in a subpoena for the records pertaining to customer IP addresses.

Selecting a licensed Computer Expert is crucial to your case. You want an expert that knows how to properly investigate and document for the courts so that the recovered evidence is credible and admissible.

Additionally, consider all



electronic evidence when proceeding with a Computer Forensic investigation, such as thumb drives, camera memory cards, and smart phones.



The Methodology

- Seize eEvidence
- Authenticate
- Analyze
- Report

To receive this newsletter electronically via email subscribe at;

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...



Case Logs for

February

What’s in Our Lab?

- *6x Child Exploitation Cases*
- *3 x Infidelity Cases*
- *5x Corporate Dispute Cases*

And counting...