

[Click to view this email in a browser](#)

IT Acceleration

Forensic Front

Volume 1 | Issue 1 | June 2008

In This Issue

- [Director's Message](#)
- [IT Brain Dump](#)
- [CSI](#)
- [How We Did It](#)
- [Ask the Expert](#)
- [Meltdown](#)
- [Did You Know](#)

Technologies Discussed

- Microsoft Vista
- eDiscovery
- Computer Forensics
- Data Wiping Software
- MD5 Hashing

Directors Message

by David Yarnall

Welcome to ITA's inaugural issue of Forensic Front. As IT Acceleration enters its sixth year providing outsourced IT services, and Computer Forensic & Electronic Discovery expertise, we wanted to offer the reader insight into our capabilities and experiences in both industries.

For those of you new to IT Acceleration, we incorporated in 2002, providing IT support. Shortly thereafter, due to an increased need from our corporate clients, we began conducting computer investigations. Individually, IT Acceleration's partners, managers and senior technical staff each have 25 or more years of experience supporting and managing technology. In fact, our fulltime forensic staff alone has over 125 years of combined experience working in Information Technology. Our forensic capabilities continue to expand, learning by deploying and supporting new products.

This model has proven to be invaluable when consulting with counsel, negotiating with opposing experts, addressing issues during onsite collections and communicating "how to" to client's IT staff during their ongoing preservation obligations.

On the IT side, our Helpdesk provides first rate, 24/7/365 immediate technical support to clients – no waiting for a callback or being transferred overseas - you are on the phone with our technical staff when you place the call! The advanced technology that our Helpdesk uses enables us to provide secure and authorized remote desktop assistance at the time of the call. Not only does this negate the need for traveling onsite, but the problem is fixed significantly faster!

Forensically, we provide a complete and comprehensive set of skills to help with discovery and production. We developed the ForenSys™ Methodology which defines our process from preservation to review. Critical components include overall process management commencing with evidence collection while maintaining data authenticity throughout the eDiscovery life-cycle. It is increasingly important to ensure collection and processing tasks are legally defensible as litigation involving electronic discovery evolves. ForenSys™ eliminates the ability for the opposing side to successfully challenge chain-of-custody issues and potentially introduce spoliation as a trump card later.

In conclusion, welcome and we hope you find this newsletter interesting and informative. As always, your feedback is invaluable.

Our vision is to provide the best possible service & value, and be a reliable technical resource to our clients.

[Click here](#) to learn more about David

[back to top ^](#)

IT Brain Dump: New in Technology, Vista or XP?

By Pete Gilmartin

The big question we hear at IT Acceleration is, "Should I purchase Vista for my office or stick with XP?" After personally test driving Vista here at ITA and working with other early adopters, our answer is: stick with XP.

While Vista offers an attractive user interface and simplifies some processes, it fails to offer any productivity gains to businesses and lacks compatibility with many existing applications and hardware.



ITA started with three Vista PCs, but we are now down to one with limited applications. Users trying out Vista as their everyday OS experienced too many issues such as: unexplained errors, random reboots and slow performance that drove them back to XP. Vista will require at least 2 GB of RAM to run well.

Given all of this, it seems like a simple choice to stay with XP. But things are never that simple. Microsoft has announced that they will stop selling XP on June 30, 2008. You will not be able to purchase XP in stores or on new PCs after this date.

FYI: Dell and Lenovo have announced that they will continue selling XP on select PCs and laptops. Vista Business and Vista Ultimate have downgradeable licenses. Dell and Lenovo will allow you to purchase either of these Vista versions and then downgrade to XP, at least until Microsoft closes this loophole.

So, will you be forced to upgrade to Vista, kicking and screaming? Well, the web chatter says Microsoft is now looking to replace Vista with Windows 7 in the third quarter of 2009. If you have been listening to the rumors, then you know that "Microsoft sees that Vista is a failure like Windows ME and will be quickly replaced by a much better OS, Windows 7." Unfortunately, ITA cannot confirm either the rumor or that Windows 7 will be an improvement over Vista. But at this point, it looks like Microsoft may be betting its future on exactly that. They need a home run with Windows 7 and they know it!

One last note: unless you are the type who loves the challenge of learning something new or will play with new technology until you "get it", you may want to plan for training when the time to upgrade does arrive. I know the ITA Help Desk will be ready when you are!

IT Acceleration Helpdesk can be reached at:

610-995-9160 Option 1

[Click here](#) to learn more about IT Acceleration

[back to top ^](#)

CSI: Computer Systems Investigations eData Collection vs. Computer Forensics

By Joe Baxter

It is not unusual to see the terms eDiscovery and computer forensics used interchangeably, but they are vastly different processes. In reality, eDiscovery is the process of collecting active files relevant to a matter. Computer forensics is the process of making a bit-for-bit exact duplicate image of source data (I.E. hard drives, network folders, USB drives, etc) in an effort to collect evidence from the entire media.

An analogy in non-computer terms can be made with an office. eDiscovery would be equivalent to making a photocopy of specific documents in a filing cabinet. Any documents not in the filing cabinet at the time the copy is made, will not be collected.



A forensic collection would be the equivalent of photocopying every document in all filing cabinets, drawers, on the desk and in the trash can; in addition, any documents that had fallen to the bottom of the file cabinet, the contents of the shredder and anywhere else in the office.

Obviously, forensic imaging can produce far more items to support or defend an allegation, including the "smoking gun". By using new high speed imaging tools, forensic imaging can be completed faster than an eDiscovery collection yet yield much more evidence. Forensic imaging also preserves the metadata (data about the files) and avoids spoliation issues.

Due to the ability to preserve data and authenticate the forensic collection over the course of the eDiscovery engagement, IT Acceleration recommends forensic imaging, except when specifically excluded by prior agreement with opposing counsel.

[Click here](#) to learn more about Forensics

[back to top ^](#)

How we did it...

by David Yarnall

Case Study: Defendant was accused of using data wiping software to knowingly destroy evidence. Therefore, plaintiff alleged spoliation.

Facts: the defendant did indeed have data wiping software installed on the computer and stated this was downloaded from the Internet in efforts to clean up the computer of spyware, adware and other potentially malicious programs as a result of web surfing.

Technical Insight: data wiping software is used to overwrite (wipe) files or entire hard drives. The goal is to eliminate any possibility to recover data from the media.

There are some products available for free on the web but be warned, "you get what you pay for".

The utility will overwrite the media with zeros or random patterns during one or more passes. The Department of Defense (DOD) standard is seven



passes of overwriting. Our ForenSys™ Methodology requires all new media to be wiped to DOD specs when used as part of an eDiscovery engagement, thereby eliminating any possibility for data cross-contamination.



How We Did It: IT Acceleration's forensic analyst researched and downloaded the same version of the wiping utility found on the computer. A USB thumb drive with files saved to it was wiped by the utility using the default settings and then forensically examined. We were able to recover the files from the "wiped" thumb drive confirming that the utility was unreliable as a wiping utility. In addition, there was no consistent and unique wiping pattern to indicate the software was actively used on the computer.

Therefore, its use on the computer would be inconclusive but if it was used, the media potentially "wiped" would be available for the possibility of file recovery.

[Submit a request](#) for "How we did it..."

[back to top ^](#)

Contact IT Acceleration:
www.ITAcceleration.com

610-995-9160

Option 1: Helpdesk

Option 2: Forensics

Tip to Remember:



*When turning in your cell phone to upgrade or donate, ALWAYS perform a "**hard reset**" to wipe your personal information.*

Otherwise, all your contact information can potentially be retrieved by others.

[back to top ^](#)

Ask the Expert

Q: What is an "MD5 Hash" or "hashing"?

David: MD5 stands for Message Digest 5. It was developed by RSA Security to provide one-way authentication of data. In essence, it is a mathematical algorithm applied to data to verify authenticity and is analogous to data fingerprinting. The value created by hashing is a unique 128 bit hexadecimal value such as:
05163F96DAA633369E4FBE3095A04322.

We use MD5 hash values when forensically imaging hard drives by hashing both the physical hard drive (source) and the newly created image (destination) to ensure the values match. Since forensically imaging physical media is a bit-for-bit exact duplicate of the source, successful imaging will provide for a match. This is an industry standard practice.

In addition, individual files can be MD5 hashed. Only by changing the content of the file will the MD5 Hash value change. A change to the file name or metadata of the file (I.E. the last access date of a file) will not change the MD5 Hash value of the file. Data can be re-hashed at any time to ensure the data is authentic and not corrupt.

Our ForenSys™ Methodology routinely utilizes MD5 hashing throughout the process to authenticate and re-authenticate images and files.

[Submit a question](#) to the Expert

[back to top ^](#)

Meltdown

Did You Know?



"You sure this is the proper way to drag files to the recycle bin?!"

Recycling Bin:

When you move a file to the Window's Recycle Bin, that file is not deleted from your PC. Even after you empty the Recycle Bin, the file may still exist and could be recovered forensically.



[back to top ^](#)

FORENSIC COMPUTING | eRISK PROTECTION | IT INFRASTRUCTURE

The Woods
995 Old Eagle School Road Suite # 307
Wayne, PA 19087 USA
www.ITAcceleration.com

Sales & Marketing
Phone: 610-995-9160 x813
Fax: 610-995-0130
E-mail: sabine.mehnert@itacceleration.com

[Forward this message to a friend](#)

If you no longer wish to receive these emails, please reply to this message with "Unsubscribe" in the subject line or simply click on the following link: [Unsubscribe](#)

IT Acceleration
995 Old Eagle School Rd., Ste. 307
Wayne, Pennsylvania 19087

[Read](#) the VerticalResponse marketing policy.

