



Susquehanna Digital Forensics

# Digital Forensic Newsbytes

June 17, 2005

Volume 1, Number 2

## In This Issue

- Wrongful Termination Suit Prevention
- Presence of Encryption Software Found Relevant to Child Abuse Conviction
- Company Data Found on EBay

## Mentioned Links

Peter McLelan

PGP

O&O Software

EBay

## Legal Links

State of Minnesota Appeals Court case (A04-381)

## Contact Us

<http://SusquehannaDigitalForensics.Com>

Examiner@

[SusquehannaDigitalForensics.Com](mailto:Examiner@SusquehannaDigitalForensics.Com)

1-717-704-0067

## Wrongful Termination Suit Prevention

Issues such as wrongful terminations suits, theft of trade secrets and harassment typically do not surface until months after an employee has left his or her position. Critical computer evidence has probably been over-written by this time and is un-recoverable. Making a forensic image of an employee's hard drive upon termination, resignation or internal transfer and then archiving the image to DVD or CD as part of your standard operating procedure can prove extremely valuable.

Peter McLelan, a former RCMP officer and consultant with Deloitte says that 'If you're going to terminate an employee, consider employing computer forensics professionals early. The employee's information on the computer system will provide a classic amount of evidence to support the dismissal. If you wait a couple of months after the employee has been fired, tracing his or her tracks will be difficult "

In the event that the archived image is needed to defend a lawsuit, make sure that it is a qualified forensic duplicate of the original drive. If not, any potential evidence may be inadmissible in court or civil action. Simply copying files, turning a computer on, or using backup software will change many things on the disk and reduces the value of its data. Are you depending on your IT staff to make a "GHOST" copy, or a Windows Backup to preserve your evidence? Will they be able to testify that the image they made is a "bit-for-bit" exact duplicate?

---

## Presence of Encryption Software Found Relevant to Child Abuse Conviction

In a recent (May 3, 2005) State of Minnesota Appeals Court case (A04-381), State of Minnesota, Respondent, vs. Ari David Levie, Appellant, one of the issues that was raised asked the question "Did the district court err in admitting evidence concerning appellant's internet usage and encryption capability for his computer?"

The software in question was PGP (Pretty Good Privacy), industry standard software that allows digital signing and encrypting of email, files and documents and is in wide use. No evidence was provided that the defendant actually used the software to hide evidence of abuse, but rather the mere presence showed criminal intent.

The courts decision in regards to the presence of PGP was that

## Editor

Robert L. Maley, CIFI, EnCE,  
CISSP, MCSE

the "Evidence of appellant's computer usage and the presence of an encryption program on his computer was relevant to the state's case. We affirm the district court's evidentiary rulings."

Although this case did not go before a jury, it may, at least in Minnesota, establish a precedent that the use of encryption software

---

## Company Data Found On EBay

German data recovery firm O&O Software recently conducted a study in which they purchased 200 hard drives on EBay. In their report, Data Data Everywhere 2005, They found and recovered 3.3 million files from the 200 hard drives, which included more than 40,000 Word Documents, about 15,000 Excel Spreadsheets, and around 50 Outlook containing approximately 2000 messages.

Some of the data recovered was rather amazing. They found documents from a German government institution internal memos and legal correspondence. They also recovered documents from a German bank with competitor intelligence. Other drives contained personal documents, financial information and photographs from a variety of people.

A quick check on Ebay US found over 7400 entries in the category of Internal Hard Drives. Many these are used, re-formatted or refurbished drives. It begs the question "How many secrets for sale today?"

If you do not have a tested procedure in place for the disposal of hard disk drives in your Enterprise, you could possibly be sharing your confidential data like the companies described above.

Formatting alone does not remove your data. Many purportedly "DoD" compliant wiping programs miss some areas on a system. The only sure way you can clean a disk is to wipe the entire drive with known software, then test your process to make sure that it gets everything.

## Susquehanna Digital Forensics

- ▶ The company principal has a 29 year background in law enforcement, court testimony, computer systems, information systems security and forensic investigations.
  - ▶ EnCE - Encase® Certified Examiner
  - ▶ CIFI - Certified Information Forensics Investigator
  - ▶ CISSP - Certified Information Systems Security Professional
    - ▶ SSCP - Security Systems Certified Practitioner
    - ▶ MCSE - Microsoft Certified Systems Engineer
    - ▶ MCSA - Microsoft Certified Systems Administrator
  - ▶ IISFA - Member International Information Systems Forensic Association
- ▶ ISSA - Member of the Information Systems Security Association, Vice President of the Central PA Chapter
  - ▶ InfraGard - Member Central Pennsylvania Chapter
  - ▶ Decorated former Law Enforcement Officer