

The Top Ten Most Unusual Computer Forensics Cases

Adrian Palmer

Managing Director, Computer Forensics

Computer forensics experts can help lawyers, investigators and executives obtain electronic data from individual hard drives and systems for use in an investigation or a court of law. From restoring hard drives burned to a crisp to detecting cyber scams, computer forensic engineers are increasingly working on some of the most high-profile computer investigations throughout the world. The following Top Ten case examples offer an insight into how computer forensic experts can uncover the who, what, when, where and why of some of the most puzzling technology mysteries:

1. Hot Hard Drives: In an arson and murder investigation, computer forensic investigators were asked to analyse hard drives recovered from a burned house which were charred and covered with ash and soot. When experienced engineers opened the drives in a sterile cleanroom – designed for repairing damaged computer media – they discovered the data contained on the individual data platters was not subjected to a high enough heat to cause permanent data loss. Relying on years of experience with fire-damaged computer media, engineers recovered and produced all of the data to the prosecutor's office for analysis. The evidence contained on the hard drives helped the prosecutors build their case against the charged individual.

2. Keystroke Calamity: Attempting to access passwords, account information and other confidential data, an individual planted small "keystroke loggers" on the back of several computers at a large company. While investigating the situation, forensic engineers discovered these loggers, enabling the time and date of when the logger was installed to be detected. This allowed the company to retrieve its security videos and catch the corporate thief in the act.

3. Scamming Stopped: In an attempt to swindle an elderly couple, a man handed them a hard copy of a sales "contract," alleged the couple created it on their computer, and then demanded they sell him a piece of property well below the fair market price. Computer forensic engineers uncovered the fraudulent activity, finding the couple did not even have Microsoft Word installed on their computer at all, making it impossible for them to have created the document on their computer.

4. Cracking Encrypted CDs: Working with one of the largest district attorney's offices in the United States, computer forensics experts recovered more than 30,000 confidential files, stored on two CDs and written in a foreign language. After one computer forensic company unsuccessfully attempted to open the files, different experts were called in and were able to surmise that the files were encrypted or compressed with some unknown piece of software or, alternatively, so corrupt they were unreadable. After completing an extensive analysis, the engineers determined these were in fact GIF (Graphics Interchange Format) files containing non-standard headers that prevented them from opening. The forensic experts then repaired the non-standard headers, enabling the district attorney's office to open and read all 30,000-plus files for their review of evidence specific to the matter at issue.

5. Pivotal Palm Pilot Passwords: A small financial services company sought to access calendar and email items contained on two former employees' Palm Pilots. The company suspected the ex-employees had made several appointments, emails and phone calls with financial planning customers in attempt to steal the accounts shortly before leaving the company. The company's IT resource could not access the Palm Pilot data due to password protection. The forensic experts could, however, decipher the system and file passwords on the PDAs, allowing a client to access calendar items, emails and phone logs not available in any other computer location.

6. Sinking Ships: After part of a large cargo ship sunk in international waters, a client called computer forensics experts to recover and analyse the computer log files associated with the ship's loading processes. The client asked the focus to be the metadata – specifically the "create" and "modified" dates – associated with the log files. Information resulting from the computer forensic investigation revealed the log files were altered after the ship sunk and one month before the computers were to be turned over for inspection.

7. Usurping USB Drives: On behalf of a bank, a computer forensic investigation was undertaken focussing on several computers owned by a bank customer suspected in a money laundering scheme. The initial review of the computers revealed that a large capacity USB drive was installed on the machine one day prior to turning over the computers pursuant to the court order. Upon further review of the USB drive, the engineers proved the individual had engaged in corporate financial fraud, stolen business funds and moved the money in foreign bank accounts.

8. Email Evidence Exposed: A company suspected its Chief Financial Officer of passing trade secrets and confidential information to one of the company's biggest competitors. Computer forensic engineers recovered emails confirming the CFO's illicit acts, even though the CFO's email PST was deleted and the hard drive was defragmented shortly before the engineers were permitted to mirror image the machine.

9. Preservation Protocol: A company asked computer forensics experts to help it comply with a document preservation order in a large government investigation. The company, at risk for damaging potentially relevant information, sought assistance creating mirror images of several thousand hard drives scheduled to be erased and re-deployed within the company's IT system. To date, experts have imaged more than 2,100 hard drives for the company, totalling more than 84,000 gigabytes of data.

10. Diary Discrimination Debacle: In a discrimination case, a former employee used electronic notes about the discrimination – created in an email system diary – to support his claims. The employee then claimed his computer crashed, making it impossible to examine an electronic copy of the notes. A computer forensic investigation determined the diary feature was not available on the email system during the time the employee claimed to have created the notes, making the employee's claim void.

Disclaimer

This document is neither designed nor intended to provide legal or other professional advice but is intended merely to be a starting point for research and information on the subject of legal technology. While every attempt has been made to ensure accuracy of this information, no responsibility can be accepted for errors or omissions. Recipients of information or services provided by Kroll Ontrack shall maintain full, professional, and direct responsibility to their clients for any information or services rendered by Kroll Ontrack.