INTERHACK

Interhack
5 E. Long Street, Suite 1001
Columbus, OH 43215

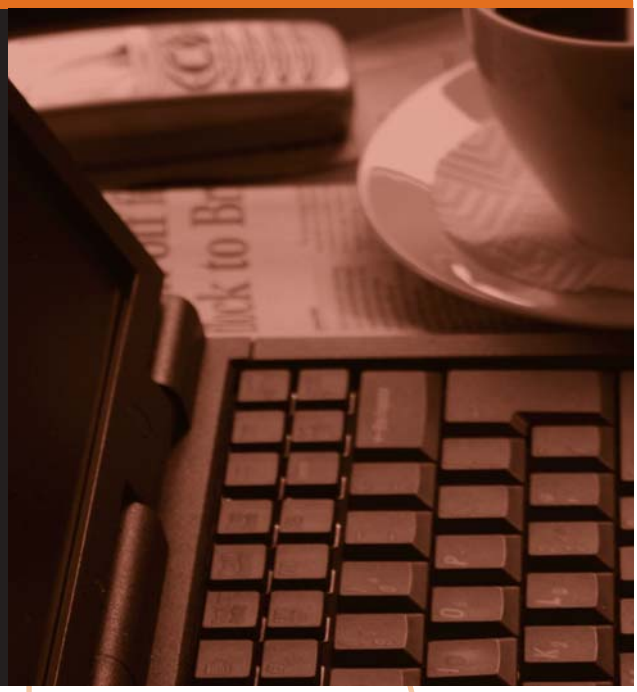
VOX+1 614 545 HACK
FAX+1 614 545 0076
WEB http://web.interhack.com/

Posthumous Message Authentication:
A FORENSIC COMPUTING CASE STUDY

SUMMARY

In the world of computer technology, deletion does not always mean destruction. When litigating where electronic information is material, valuable evidence can exist in deleted or hidden files.

- **Through digital forensic analysis, Interhack authenticated suicide messages sent by email in litigation over payment of a decedent's life insurance policy.**
- **With a $5 million dollar insurance policy claim at stake, Interhack reconstructed digital evidence to reveal the facts in the civil case, leading to a quick settlement.**



Background

Civil litigation was initiated after an insurance company refused to pay the entire sum of a $5 million life insurance policy to the beneficiary. The policy included an anti-suicide clause, and the decedent was believed to have taken his own life. The beneficiary of the policy argued he was entitled to the full $5 million, claiming the policy holder, the decedent, had not committed suicide.

While the coroner held that the policy holder had accidentally shot himself while cleaning his gun, the assistant coroner disagreed, holding that the shot was intentional. There was a chance, however, that additional electronic evidence existed, for the decedent had sent suicide messages via email to several of his associates. None of the recipients was thought to be able to provide credible testimony needed to authenticate the messages, though.

The challenge for the insurance company was to prove the authenticity of the suicide emails; if these messages were genuinely written by the decedent, then the full $5 million dollar payout would not be warranted.

Objective

The Defense contacted Interhack to investigate the decedent's computer. Interhack's objective was to determine whether the messages could be authenticated as genuinely from the decedent. A forensic computer scientist was assigned to the case and developed a method for authenticating the email messages in question. With neither the sender nor the recipient available to testify to the authenticity of the messages, counsel hoped that examination of the computer systems would provide the evidence needed to introduce the messages into evidence.

Actions

Under court order, discovery began with Interhack taking forensic images, which are exact copies, of the decedent's desktop and server. Interhack performed an analysis on the machines, combing through raw data, in search of text from the suicide messages. The search found the complete messages as well as fragments created automatically by the system during the course of composing the messages. The file fragments, generally considered deleted, contained vital "metadata" (data about the data). Analysis of the metadata allowed Interhack's expert to show not only that the messages originated on the decedent's machine, but the time when the messages were composed and sent.

In addition to discovery and analysis of the data, Interhack's scientist served as a strategic advisor; he put his technical findings in context, explaining to counsel how they were relevant to the case.

Resolution

Interhack effectively confirmed the facts needed to resolve the case: 1) suicide messages were in fact composed on the deceased policyholder's machine, 2) each one of them was authentic, and 3) the text composed on this machine was verified to be composed before the policyholder's death.

Ultimately, Interhack produced a report firmly authenticating the suicide messages as being sent by the policy holder himself. Immediately after releasing the report, a settlement was reached – very quickly and very quietly. Settlement terms were kept confidential.

Interhack: Demystifying Computing Technology

As computing technology becomes increasingly important in the practice of law, so does the need for understanding the technology, finding electronic facts and interpreting them in the context of a specific case.

Founded in 2000 by computer and information science researchers in Columbus, Ohio, Interhack is a professional services firm with practices in both Information Assurance and Forensic Computing.

Interhack Forensic Computing serves the legal system by finding facts through collection and analysis of electronic information. Services we provide support adjudication in civil litigation as well as criminal proceedings. Demystifying technology for attorneys, judges, and juries, we use computer science to establish the facts, and provide informed, impartial opinions, allowing the legal process to follow its course.

Aside from acting as undisclosed technology consultants in numerous cases, we have served as testifying experts in cases such as Sony BMG "Rootkit" Litigation, RIAA v. MP3Board.com, Avenue A Privacy Litigation, and the Pharmatrak Privacy Litigation, which led the First Circuit to establish standards for application of Federal wiretap statutes to Web technology.

Interhack Forensic Computing Services

- **Expert Testimony** – Testimony for the court on technical matters.
- **Forensic Consultation & Analysis** – Technical analysis of data or programs for legal argumentation. Explanation of computer or networking technology to attorneys, including assistance in definition of discovery, deposition, and the cross-examination of experts.
- **Data Recovery** – Recovery and reconstruction of data, apparently deleted, damaged or lost.
- **Electronic Discovery** – The routine collection and reporting of electronic documentation in evidence.

When you have a case where technology matters, we'll be happy to talk to you about the issues at stake, how we can help, and offer strategies to answer critical technical questions without breaking the bank.

We have supported even the most high-risk and complex adjudication.

We can do the same for you.

INTERHACK