INTERHACK

Interhack
5 E Long St Ste 1001
Columbus, OH 43215

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

There Goes The Neighborhood: A Forensic Computing Case Study

Summary

Crimes engaging technology require the legal system to follow. In our digital neighborhood, criminal activity is but a few clicks away. Now more than ever, defense attorneys must have technical expertise available to decipher the evidence and protect their clients from misguided prosecution.

When a high school senior was charged with a variety of felony and misdemeanor offenses, the honor student was faced with the prospect of going to prison rather than the prestigious university he expected to attend. Fundamental to the case was what was on his computer and how it got there.

Interhack's founder, Matt Curtin, served as the chief forensic computer scientist for the defense. He was tasked with making a critical examination of the data in question and reviewing the investigator's analysis and conclusions. As the case was handled as a juvenile proceeding, identifying details have been withheld but all other details are quite real.

Important lessons can be drawn from this case for anyone working with electronic evidence in the criminal justice system or civil litigation. Readers may also learn some important facts about the dangers of using Internet peer-to-peer (P2P) networks.

Background

In early 2005, a State police unit received a grant from the Department of Homeland Security to be allocated to the fight against Cybercrime. The State used its funding to purchase software and train investigators to pursue online criminal activity. Eager to put this investment to use, investigators began to crawl the Internet's P2P networks in search of contraband, specifically child pornography. P2P software enables users to search, download and share files with other network users.

The investigation led to the location of a computer within the jurisdiction that was allegedly distributing files containing child pornography. A warrant was obtained and in the predawn hours of a sleepy town, a home was raided. Two computers were confiscated as evidence.

Three suspect files were found on a computer belonging to an all-American teenage boy. The investigator's expert opined that the subjects in the image and video files were underage. A prosecutor brought charges against the high school senior alleging that he knowingly possessed and distributed child pornography. The charges included a second-degree felony, two third-degree felonies, a fourth-degree felony, and a first-degree misdemeanor.

While the prosecution believed in the strength of their case, the defendant proclaimed no knowledge of the files. State experts testified to various details of the case, including access logs indicating a timeline of when the defendant viewed the files. The teen's father, a respected surgeon in the community, supported his son and encouraged him to voluntarily submit to various psychological examinations. The results of these tests indicated that the defendant's statements were truthful. The prosecution proposed a plea bargain. Father and son discussed their options with their attorney. Ultimately, they chose to fight for exoneration rather than falsely admit guilt to lesser charges.

Objective

The defense needed a technology expert to examine the investigator's report and provide an understanding of how the defendant could unknowingly be in possession of the suspect files. After interviewing approximately thirty candidates, the defense retained Interhack's Matt Curtin as its expert. Matt is an author of multiple books on Internet security, a computer science Lecturer at Ohio State University, and the founder of Interhack Corporation. He began Interhack in 1997 and his forensic computing experience includes both civil and defense cases representing both the prosecution and defense.

Interhack's objective in this case was to perform a digital investigation to discover facts and examine the

evidence on behalf of the defense team.

Actions

For discovery purposes, Interhack secured a copy of the contents of the defendant's computer for its analysis. Using Interhack's software and forensic methodology, the investigation yielded several critical discoveries.

- The operating system file access times, which were the State's basis of knowledgeable possession, did not correspond to the access history of the three available software applications for viewing the suspect files indicating that the files were likely never viewed on this computer.
- The percentage of suspect files amongst the defendant's collection of P2P content was actually lower than what one would expect to find amongst a random sampling of files on this P2P network. While the files may have been present on his machine, this fact suggested that the user was not intent on possession and actually may have tried to avoid this type of content.
- In addition, the discovery of multiple viruses, including one specifically designed to automatically download files from this P2P network, allowed for the possibility that the suspect files were not even knowingly downloaded by the defendant.

Interhack reported its findings with the defense counsel who then, armed with a new understanding of the facts, proceeded to share the evidence with the prosecution. To support his expert opinion, Mr. Curtin prepared an affidavit for the court in preparation for the final hearing in front of the judge.

Resolution

After reviewing Interhack's discoveries and fully understanding the evidence, the State offered a new deal. All charges were dropped and the young man's record was expunged of all traces of the matter. In return, the defendant was asked to submit a paper to the judge describing how P2P networks operate and how users can protect themselves from being unwitting participants in criminal activity online.

Happily, the honor student is now continuing his education at a well respected college.

The Internet brings everyone, criminal and otherwise, into the same neighborhood. Qualified technical expertise can help an attorney distinguish their clients from online criminals and protect them from the dangers of overzealous prosecution.

About Interhack

The practice of law in both civil and criminal contexts is undergoing rapid change. Everything from routine discovery to the kinds of experts you need to support your practice have been affected by the ubiquitous nature of computer and telephone technology. Interhack helps prosecutors, defense attorneys, and plaintiffs' attorneys understand and manage the technology in their cases.

Electronic Discovery Whether you need us to acquire the data, to search it, or to present it, our technology and helpful staff ensure that you get what you need, how you need it—and when you need it.

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

Many firms will claim "computer forensics" capability; few have the case experience to back it up. When you have a case where technology matters, we'll be happy to talk with you about the issues at stake, how we can help, and strategies to answer critical technical questions without breaking the bank.