CYBER SLEUTH SCIENCE LAB

Sample Forensics Report

Overview / Case Summary

Following a dispute between Mrs. Star and Healios Pharmaceutical Company (HPC).
Mrs. Star claims that the work for a human vaccince for monkeypox (A 270 page PDF document) belonged to her after working for six months on the project.
HPC claims otherwise, and had not backed-up the files before Mrs. Star left the company, and seeks to reclaim the files, valued roughly at $3 million dollars.

Objectives

This report is a summary of Cyber Sleuths attempts to recover the lost and missing PDF files within Mrs. Stars home computer system.

Evidence Analyzed

Pursuant to the Court Order, Mrs Star gave up the following devices for analysis.

A Compaq Presario SR5413WM desktop computer with a 250 gigabyte hard drive.
A Toshiba Satellite L305-55968 laptop computer with a 320 gigabyte hard drive.

A 500 gigabyte Western Digital internal hard drive.

Using widely-accepted digital forensic techniques and procedures, digital forensic personnel from Cyber Sleuth Science Labs made bit-for-bit, verified forensic copies or images of: the hard drive within the Compaq Presario desktop computer; the hard drive within the the Toshiba Satellite laptop; the Western Digital Hard Drive.

The digital forensic copying process captured the entire contents of each piece of media, including the active user-accessible files, the deleted files, and the unallocated space, which may contain deleted content.

Investigation Steps

With the hard drives secured and copied securely and bit-by-bit, Cyber Sleuth Science Labs began to seek and identify the missing document. Within the file manager for Windows, a search was conducted for any file with the extension of .pdf. While Windows began it's search, a toolkit named Apache Tika was employed to find the metadata for any and all files within specific folders. This is used to find files that may have had their extensions changed to hide them.

Cyber Sleuth Science Labs also issued a basic scan through the hard drive using the EaseUS Data Recovery Wizard. No files related to the case were found in the first 'Quick Scan'. Therefore, Cyber Sleuth Science Labs swapped to using the 'deep' scan method to find deleted files.

After a few passes of scanning, the software was able to find and identify a PDF file within the 500 gigabyte Western Digital internal hard drive. Selecting the PDF file named 'Labratory Documents.PDF', we allowed the program to attempt to recover and piece together the PDF file.

Findings and Conclusion

After identifying and successfully recovering the missing .pdf file, Cyber Sleuth Science Lab uploaded and scanned the .pdf file for any virus or other harmful software that may be hidden within. The file came back clean and unmodified. Opening the file afterwards, Cyber Sleuth Science Lab was able to claim that it was the missing file. Therefore, the file had been tampered with in an attempt to delete and hide the evidence.