

BRISTOL COMMUNITY COLLEGE

CIT-155 Intro to Computer Forensics

Assignment a34 -- discarded drive (Klaus Koptstadt)

Preparation

As a general guideline, while working on this assignment, continue to follow the steps outlined in prior assignments to conduct your investigation. Use Module 1-3 exercise file (**mod1-3.dd**) as evidence file. Verify correct MD5 hash value:

C3A1DE297A374D9C47E5DA3685A2A006

Scenario and Instructions

You are a computer forensic examiner. A private investigator, comes to your laboratory and tells you that he has a wealthy client, Victoria von Koptstadt. She is afraid that her husband, Klaus von Koptstadt, is cheating on her and may be planning to divorce her and to hide financial assets. Klaus von Koptstadt is a wealthy surgeon who owns a pharmaceutical company and a chemical company, and has other financial interests in Europe. She has asked the private investigator to follow him and see what her husband is up to.

PI looked through the discarded trash behind Dr. von Koptstadt's office and found a removable drive in the trash yesterday. PI is presenting you with the image of the drive and asking you to look at it and recover any data that you can. If you find any data, he would like a copy of the data and would like to know when the data was created. PI would like to know anything else you can tell him about the disk.

1. Recover the deleted files on the diskette.
 - a. These files are in contiguous clusters. There are no fragmented files.
 - b. There is a sub-directory on the drive called PERSONAL; recover the deleted file in that directory.
2. Write a complete report and submit it to your instructor.

At the end of the report, write a conclusion and provide your own interpretation of the information that you've found, including, but not limited to:

- Did you find any files with evidence of financial information manipulation? If so, please provide the details.
- Was Mr. Koptstadt hiding any bank accounts, and if so -- which bank?
- Was Mr. Koptstadt dealing with any illegal activity? Which industry? Was it for financial gain? Please explain your answers.