

Lab 1 Forensic Investigation on Your Own Personal Computer

Note:

Please redact all the sensitive information that you are uncomfortable to share in this assignment.

Objectives:

- Become familiar with a forensics tool.
- Become familiar with the basic forensics process.

Instructions: Do a forensics investigation on your own personal computer using any case management tools (or some other forensics tools) you choose. OSForensics is recommended for this assignment. It is already installed on the lab computers in RVR 2009. You may also install the trial copy on your own machine. Other tools such as FTK, Sleuthkit/Autopsy_Browser, Encase, ProDiscover Basic, etc. will also work.

1. Provide screenshots showing the following information:

- Number and type of documents (Word, Power Point, Excel, etc)
- Number of images
- Number and types of encrypted files
- Number of executable files
- Number of deleted files
- Number of files in slack space
- Size of unallocated space
- Top 20 web sites visited
- Types of external devices (eg. USB, printer, etc.) connected to the computer

2. Do a search to determine the number of times your name appears, and typical places your name appeared.

3. Do a search to determine the number of times CSUS or Sac State appeared and typical places where it appeared.

4. Any surprising information you least expected to find.

Deliverable:

1. You need to submit a lab report to Canvas. In all cases show the commands used to obtain your results and any screen shots as appropriate. Please include necessary narrative and analysis to make your report clear. The report will be evaluated based on the correctness, completeness, clarity and quality of English writing.