

Lab-1: Evidence Recovery & Processing

Digital Forensics
Spring 2004

Posted: March 8th
Due: March 22nd

This is a two-week long assignment to sharpen your skills on evidence recovery and processing. A forensic analyst often comes across files and file systems that are subverted to hide evidence. In this lab, you will play that role and recover evidence from a crime scene.

In an on-going investigation your services as a forensic analyst is required to analyze some evidence seized at a crime scene. You're given a file that the CSI officials collected (evidence was gzipped by the collection official) from the crime scene and are asked to recover as much evidence as you can from the file. You may download the file from <http://isis.poly.edu/courses/cs996-forensics/misc/lab-1-evidence.gz> (MD5 = 1b825a21a758880b83b632252dced328). Following questions are posed just to guide you through the process and you're by no means limited to answering these questions:

- What type of file or files are contained in the evidence, `lab-1-evidence.gz`?
- How would you unravel the contents in the evidence (after gunzipping it, of course)? Describe the process.
- List all the items you can find in the evidence you're given in detail.
- Using the items found, what kind of investigation do you think is this? Can you name some characters that are part of this investigation?

Kulesh will be your point of contact at the law enforcement. As and when you need more information about the evidence (details on the circumstance of evidence collection, victims, suspected crime, possible MO etc.) or questions regarding what the law enforcement expects from you, you may email him at kulesh@isis or reach him at extension 4073. Your grades will depend on how much information you furnish to the law enforcement and based on the rigor of the forensic process you carry out to analyze the evidence. Please handle the evidence you download as the only copy available. If we determine that you have tainted the evidence you will lose points. With your findings, you should produce details (especially a *typescript*, if possible) of what operations and tools used on the evidence to obtain the results.