

Student Instructions:

Realistic Forensic Corpora for Undergraduate Education and Research

Image Author: LT Henry T Gilbert, USN

Image Creation Date: 10/22/09

Image Name: Gilbert.dmg

Objectives:

- Analyze the disk image for any abnormalities or indications of sensitive data being transferred.
- There are 3 folders on the disk image: Docs, Pics and Copy of Pics
- Carefully look at the files to determine if there is something suspicious
- Try to recover any deleted files and analyze them for clues
- You may need to look at the hex dump of the files, but there are easier methods and clues on the image

Tools:

- Sleuthkit
- You may need other programs, but part of the process is figuring out what you'll need. Any software required will be widely available and freeware, so the process should not be too painful

Resources/Websites:

<http://www.sleuthkit.org>