Activity 3

Deleted Data

**Learning Objective**: To demonstrate the ability to recover deleted data using data recovery tools and manually carving for files based on header and footer information from unallocated space.

**Narrative**: Recovering deleted data is one of the tasks we are most often asked to perform as digital forensic analysts. It is also a great party trick. In this exercise we will be using tools and manual processes to recover deleted data.

USB1.E01

**Narrative**: *A suspect has been accused of traveling to Dubai for arms deals. The subject denies any involvement in arms, or any travel/interest in Dubai. A thumb drive was seized from the subject, which appears to be blank. A forensic image of the thumb drive has been created (USB1.E01), and you are asked to recover any deleted data from the image.*

1. What type of file system is on this drive?
2. Using the program FTK Imager, examine this image for previously deleted images.
3. List any deleted files of value found on this device – include file name and parent directory.

USB2.E01

**Narrative**: *A suspect has been accused of trying to obtain microbrewery equipment to manufacture Anthrax. The subject was found to be in possession of a thumb drive, which appears to be blank. A forensic image of the thumb drive has been created (USB2.E01), and you are asked to recover any deleted data from the image.*

1. What do you see using FTK Imager?
2. Using the program Recuva, examine this image for previously deleted files.
3. Zip any recovered files and submit along with this document as *USB2.zip*.

USB3.E01

**Narrative**: *A suspect has been accused of smuggling several shipments of cocaine using small human powered boats. The subject was found to be in possession of a thumb drive, which appears to be blank. A forensic image of the thumb drive has been created (USB3.E01), and you are asked to recover any deleted data from the image.*

1. What do you see using FTK Imager?
2. Using the program PhotoRec, examine this image for previously deleted files.
3. Zip any recovered files and submit along with this document as *USB3.zip*.

USB4.E01

**Narrative**: *This usb was found in a secure facility. It is believed that a document existed on this device at some point that is of value. It is believed that the file type is a PDF file.*

*Research the file type and discover the file header on the image using a hex editor (like HxD).*

1. Do not use the automated tools, recover this file using nothing more than HxD.
2. Give a brief description of the contents of this file.
3. Submit this file along with this document as *USB4.PDF*