Objectives:

- Use FTK Imager to navigate a complete XP forensic image.
- Locate and extract suspect's INFO2 Files and deleted items from a forensic image.
- Use Mitec's Windows File Analyzer to Parse the INFO2 file
- Determine deleted file's original file name, path, and time of deletion.
- Understand the contents of the INFO2 file.

1. Open FTK imager
2. Add the suspect image (*Vader_Home_Computer.001)* in FTK imager.
    a. (File > Add Evidence Item > Image File & Next > Browse to path of image & Select *Vader_Home_Computer.001* & Open > Finish.)
3. Click the + buttons to navigate through the image.
4. Go to the root of Partition 1.
    a. What is the size, name, and file system of this partition?

---

5. Go to [root] and the RECYCLER folder, the subdirectory underneath the RECYCLER is a long number.
    a. What is this number?

---

6. Export the following files to your local system (INFO2, Dc3.rtf, Dc4.doc, Dc5.rtf, Dc6.doc, Dc7, & Dc8). Put them in a new folder and call the folder "Lab 6".
    a. Examine all of the deleted files. Do any of them indicate potential criminal plans? Which one was it? What were the plans?

---

7. Use Mitec's Windows File Analyzer to parse the INFO2 file.
    a. Open Mitec's WFA and select (File > Analyze Recycle Bin > Open > Navigate to the INFO2 File) and open it.
    b. What was the original file path, name, size, and deleted date of *suspect file*?

---

8. Right-click suspect file and select properties. What does it say the size is, in bytes?

---

9. What does the INFO2 file report the size as? Why is there a difference?

****Bonus: Use the techniques you just learned to examine Lex Luthor's Recycle Bin. It appears to be empty, what kind of information can you give me about the file that previously existed there?**
