Objectives:

- Use FTK Imager to navigate a complete XP forensic image.
- Locate and extract suspect's Link Files.
- Use Mitec's Windows File Analyzer to Parse the Link files
- Understand the contents of the Link File.

1. Install / open FTK imager
2. Open 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. On Partition1, go to *C:\Documents and Settings\Owner\Recent*
    a. Look at the file *Fake Light Saber Authenticity Papers.lnk* in the hex view window in FTK Imager? What information can you decipher?

---

5. Export all of the files in Owner's Recent folder to a new directory on your local computer, call the folder *Recent*.
6. Use Mitec's Windows File Analyzer to parse the Link Files.
    a. File > Analyze Shortcuts… > Browse to recent folder that you just created.
    b. When prompted about the Analyzed Operating System, select *Windows XP.*
    c. Based on file names, could any of these files indicate illegal activity? What are their names and when were they last opened?

---

d. Note the different types of information recorded in the link files. Do you see an anomaly in the reported "linked path" for the link files? (This is explained by Windows seeing the link files incorporating them into the local system).

e. If your suspect states that he had "no idea *the* incriminating file was on his system and he never opened it." How might you respond, based on the Link File Evidence?

f. *One of the incriminating files is a zip file. Use FTK Imager to go to the path where that zip file exists on the suspect image. What files are contained within the zip file?*

g. Assume one of the incriminating files turned out to be encrypted and you needed a password to open it. Do the link files indicate any files that may contain the password? Where was it located and how might you find that file?