Objectives:

- Use DumpIt.exe to capture memory from a live system
- Use FTK Imager to make a live forensic image of a USB drive
- Practice navigating and exporting files from a forensic image using FTK Imager.

1. Put the executable DumpIt in a directory that will serve as the storage location for the volatile memory evidence. *Note: This location would normally be an external device because you never want to write to your own evidence drive. However, for the purposes of this lab, feel free to store the volatile memory on the host system.
2. Double click DumpIt and respond to the program's question.
3. Install FTK Imager 3.01
4. Take a small USB drive (Preferably less than 1GB) and insert it into your computer.
5. Copy a folder containing some files of your choice onto the USB drive.
6. Open FTK imager.
7. Select *File > Create Disk Image*, choose *Physical Image* and click next.
8. Select the Physical Device that represents your USB device. (Likely *\\.\PHYSICALDRIVE1).* Click Finish.
9. Under the Image Destination(s) box, click the *Add…* button.
10. Choose *Raw (dd)* and click Next.
11. Add case information of your own choosing.
12. Choose a Destination folder to save your forensic image in and give the image a file name.
13. Click Finish.
14. Remove the checkmark from *Verify images after they are created*. This will run a second hash of your image file. In the real world, this is a good idea but it would increase the time it takes to do this lab in class, so we will not verify the image.
15. Once your forensic image is completed, click the *image summary* box. Record the following information:

    MD5 Hash:_____

    Source Data Size:_____

    Sector Count:_____

16. Select *File > Add Evidence Item*.
17. Check *Image File* and select *Next*.
18. Browse to your forensic image file. If it is multi-segmented, then only select the first one (.001)
19. Explore the folder structure of the image, note the files that you saved there previously.