1. Download the Lab4.zip folder from BlackBoard under Labs\Lab 4 and extract the contents to a folder on your Desktop.  Use Shellbags Explorer to open the UsrClass.dat hive from the Lab4.zip file.  Answer the following questions:

What is the name of the folder on the F:\ drive that was most recently interacted with?

**FTK Imager**

1. What is the name of the user profile identified in the UsrClass.dat hive? **Jcloudy**
2. When was the pic folder created on the D:\ drive?  (Note: this folder is not in the root of the D:\ drive) **2018-03-27 23:34:48**
3. Which of the following cloud storage services is NOT referenced in the shellbags of the UsrClass.dat hive? **One Drive**
4. What is the MFT entry (aka & “MFT record”) number of the “C:\Users” directory? **1417**
5. What type of file system is the F:\ volume? **exFAT**
6. Open the NTUSER.DAT registry hive from the Lab4.zip archive using Registry Explorer.  Click "No" to the prompt asking to replay transaction logs and "Yes" to the prompt asking to load the dirty hive.  Answer the following questions: Based on the RecentDocs key, when was "Planning.docx" last accessed? **2018-04-05 08:32:48**
7. Which cloud storage services were configured to start when the user logged in? **Both (b) and (c)**
8. What is most recently accessed URL referenced by the TypedURLs subkey? [**http://go.microsoft.com/fwlink/p/?LinkId=255141**](http://go.microsoft.com/fwlink/p/?LinkId=255141)
9. Analyze the RecentApps subkey in the NTUSER.DAT hive (Software\Microsoft\Windows\CurrentVersion\Search\RecentApps).  What is the name of the program executed on the F:\ drive?  Note: You can use the RecentApps bookmark and plugin in the Bookmarks tab of Registry Explorer**. FTK Imager.exe**