**Lab 15 – Examining DropBox Cloud Storage**

**Background**

Filecache.dbx is an important file associated with Dropbox. It stores information shared directories, user accounts and file transfers. Dropbox files can be sources of forensic evidence.

**Tasks**

1. Copy the Dropbox folder from the Chapter 13 data files folder into your evidence folder and start Autopsy. Create and New Case.
2. The new case name and number will be C13Proj1. Put your initials in the examiners text box and finish.
3. The add data source box, choose logical and select your source file. Your source file will be the location of the Dropbox folder you just copied across earlier as part of step 1.
4. “users” will be the search criteria that will be entered in the keyword search. Search for the username associated with the Dropbox account.
5. Click the DROPBOXINSTALLER.EXE-802BABAC.pf (dropbox prefetch file). You can see the name LAURIE in lower pane.
6. Do another keyword search this time using “LAURIE” do see what information can be associated with this user.
7. Expand LogicalFileSet1 and DropBox and click the DropBox folder, under AppData to see the files that were synced with cloud storage.
8. Click the Thumbnail tab in the right pane to see images transferred with Dropbox.
9. Expand views and file types and then click Documents. Click the table tab in the right pane to see the docs stored in the cloud.
10. Click gthe keyword search and look for filecache.dbx and search.
11. Exit Autopsy.

**Lab 16 – Examining OneDrive Cloud Storage**

OneDrive cloud service come with Windows installations. The files in this lab have come from the same machine as was used in Lab 15. Users can use many different cloud accounts so all options and applications should be investigated. One drive stores their information in a SyncDiagnostics.log file. Look after sync the cloud and users machine. Also, ONEDRIVESETUP.EXE-nnnnnnn.pf is a prefetch file that can be useful in finding client linked folders for storing documents and paths that tie the computer and cloud account together.

**Activity**

1. Copy the OneDrive folder from the Chapter 13 data files folder into your evidence folder and start Autopsy. Create and New Case.
2. The new case name and number will be C13Proj2. Put your initials in the examiners text box and finish.
3. In the add data source box, choose logical files and select your source file. Your source file will be the location of the Dropbox folder you just copied across earlier as part of step 1.
4. “users” will be the search criteria that will be entered in the keyword search. Search for the username associated with the OneDrive account.
5. Click the 42-f7a03bfblc86c703.ini file in the right pane to view the username for the OneDrive account. Click the ONEDRIVESETUP.EXE-1224F619.pf (prefetch file).
6. Click the keyword search again and look for SyncDiagnostics.log. Click the Table tab. Click the SyncDiagnostics.log file and then click the Strings tab in the lower pane to see the metadata about the folder transactions associated with this OneDrive account.
7. Exit Autopsy.