|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2020/21) Semester 4/6 | Week 4 |
| Practical 6 |
| **Windows Artifacts** | |

**OBJECTIVES**

1. To be familiarized with Windows directory structure.
2. To be able to navigate and locate important Windows folders and files.
3. To be able to export Event Logs from EnCase.

**Part A: Windows Artifacts**

**1. User files and folders**

The folder structure of a Windows operating system (XP, Vista and 7) can provide evidence by itself. Within the Windows operating system, there is a unique artifact that appears when a user logs onto a computer for the first time.

A series of folders and files is created on that machine in a manner that is transparent to the user. This folder structure is created whether the person logs on locally or authenticates through the network.

The root folder of that structure (the user’s root folder) is named after the person’s username. Windows XP, Vista and 7 all store these folders in different places.

Windows XP store the folders under the C:\Documents and Settings folder.

Windows Vista stores these folders under C:\Users\.

**Open up evidence file from Laura’s hard disk and find out where Windows 7 stores these folders**

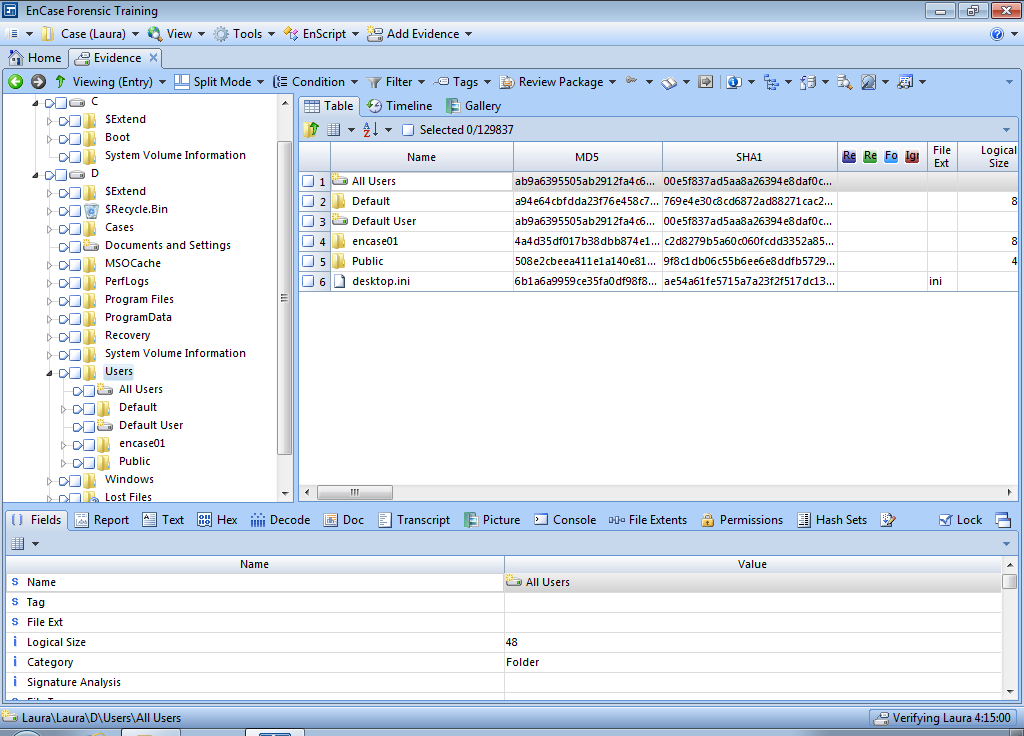
**Answer:**

D:\Users\.

Default accounts are created during the install process as Windows will not allow the system to be accessed without a valid login. The account for All Users is one that should be included in all examinations as this account is accessible by all others and will hold information that is global in nature and not user specific.

As an example, if an application is installed and the selection is chosen to make this application available to all users, then the Desktop icon and other information regarding this application will be populated within All Users account rather than the account of the user installing the software.

Under the user folder is a series of folders and files that are specific to the user. For instance in our screen shot below:

Figure 1: Folder structure of Windows

We shall start exploring some of the important folders and files under the user folder where examiners can gather important evidence for their investigations.

**2. Root folder**

The root folder is the folder that is named after the user’s login name. There are a few files that are created and stored in the root folder. The most important is the NTUSER.DAT file, which contains settings specific to the user. The NTUSER.DAT file is updated by the operating system when the user logs out, therefore, its last written time can be used to possibly determine when the user last logged out.

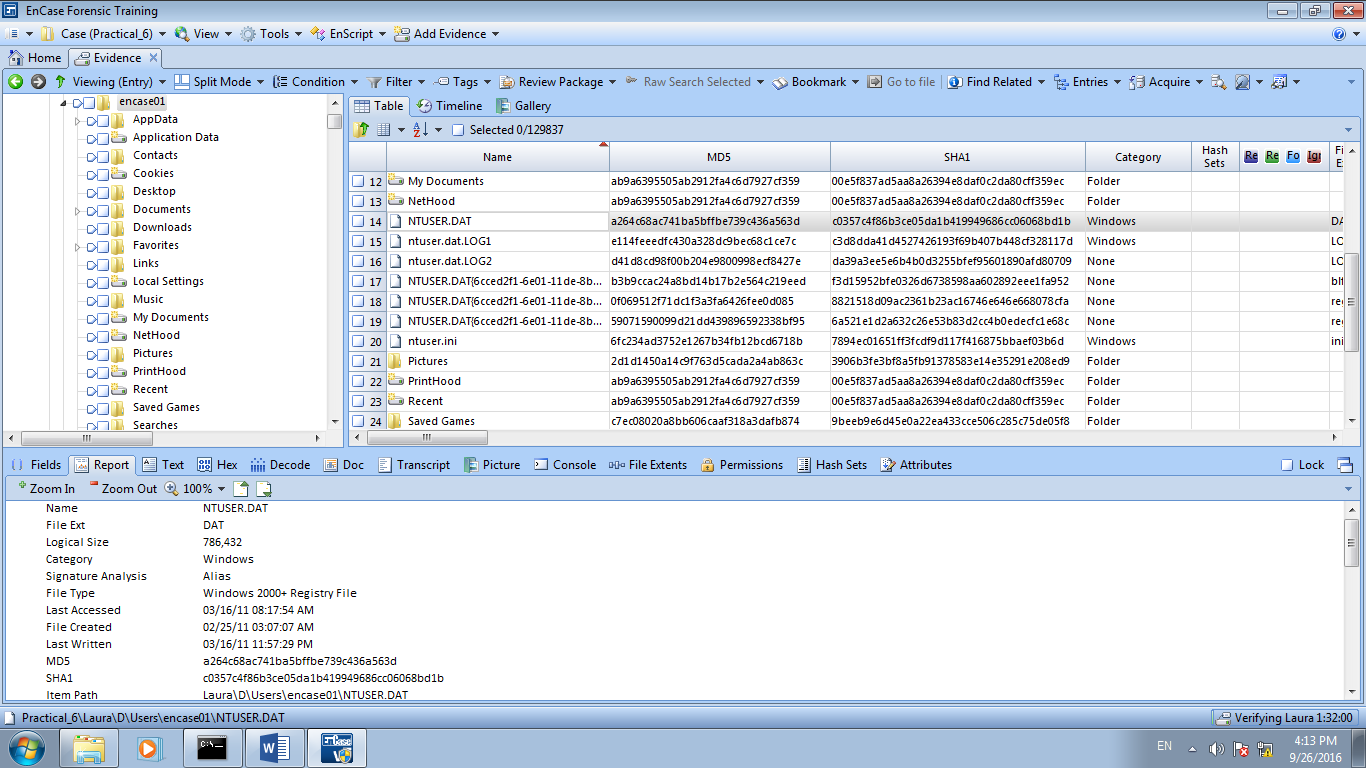


Figure 2: NTUSER.DAT file

**3. Recycle Bin**

By default when a user deletes a file in Windows, the file is placed in the Recycle Bin. When a file is in the Recycle Bin, the user has the option of restoring the file to its original location. A user can also select an individual file or files and delete them from the Recycle Bin. The final option is to empty it, which deletes all the files in the Recycle Bin.

As an examiner, we need to understand the fine details of the Recycle Bin process so we can completely examine and later explain the evidence found therein.

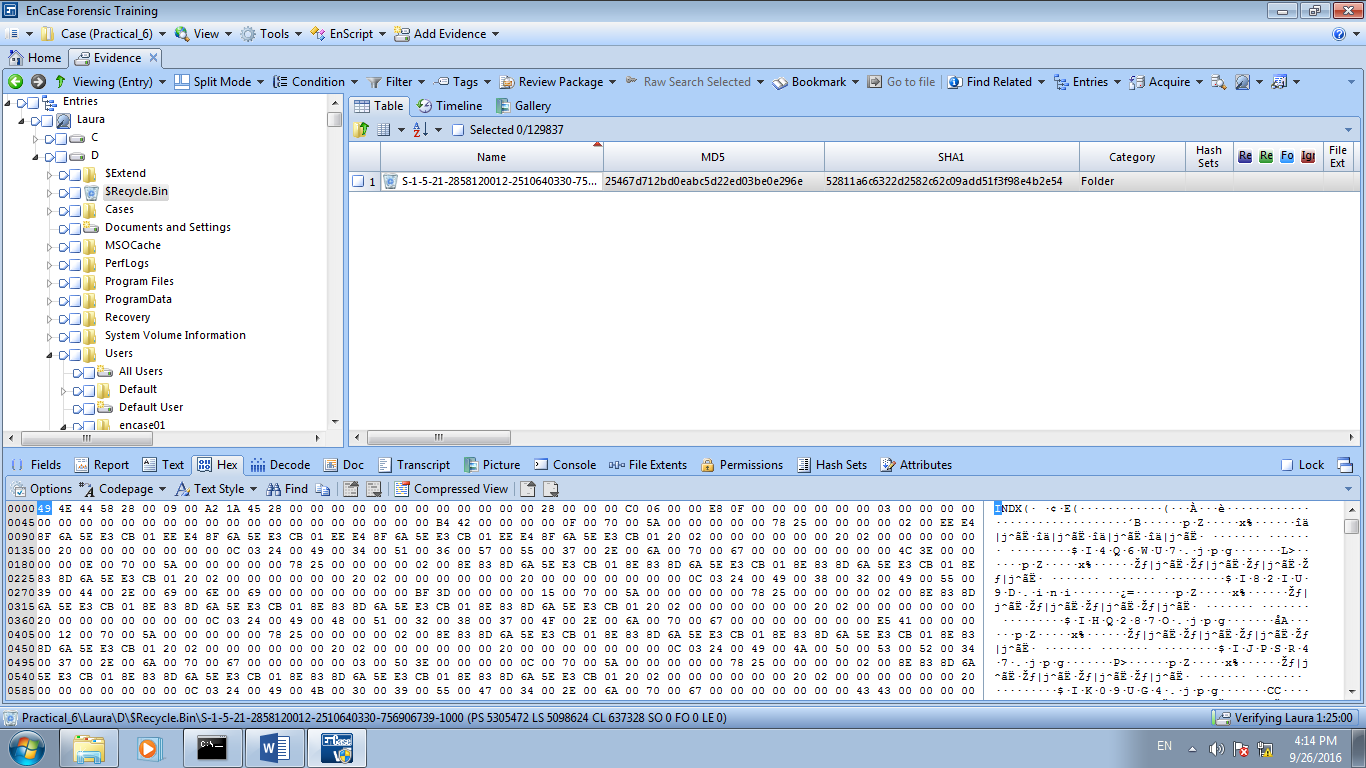


Figure 3A: Recycle Bin

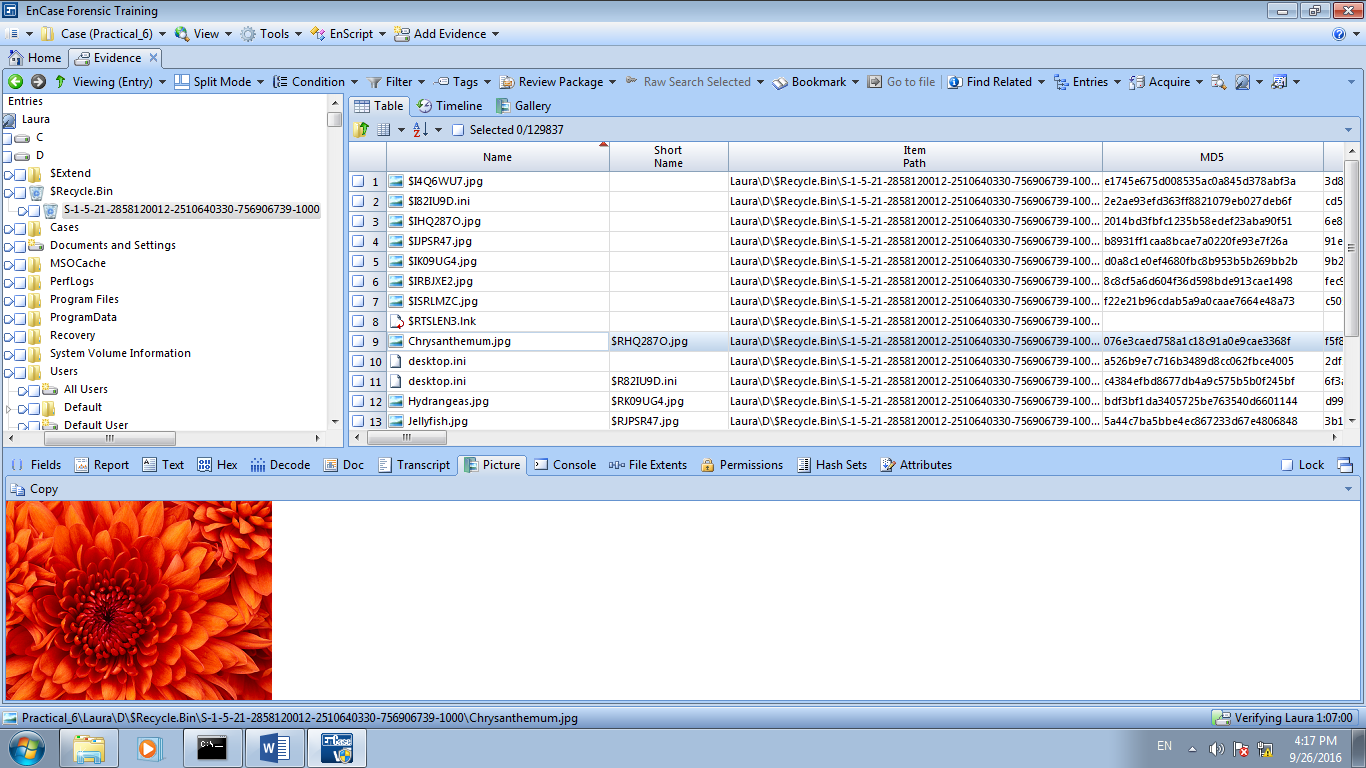


Figure 3B: Deleted file, chrysanthemum.jpg

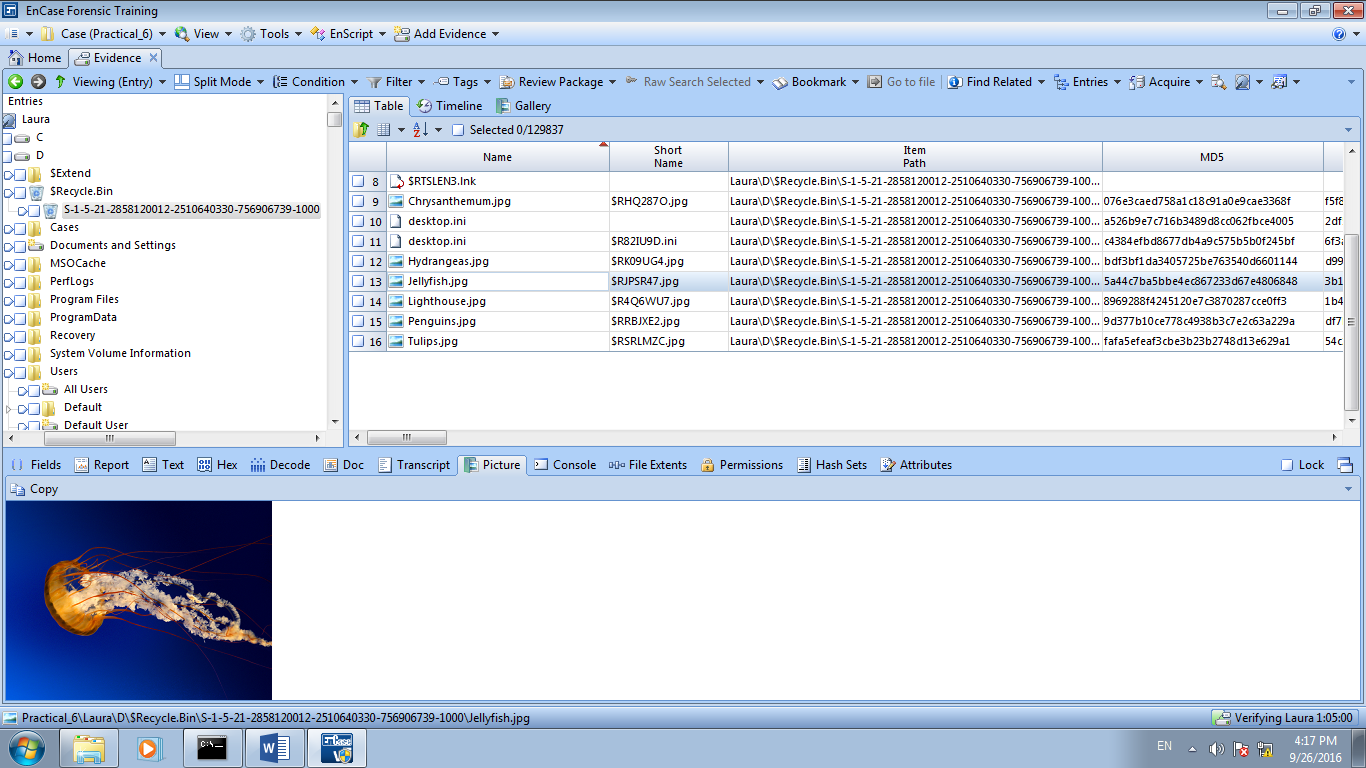


Figure 3C: Deleted file, jellyfish.jpg

**Bookmark 2 deleted items chrysanthemum.jpg and jellyfish.jpg**

**What are the $I and $R file names for each of these 2 deleted files?**

**Answer:**

**chrysanthemum.jpg**

**$R = $RHQ2870.jpg**

**$I = $IHQ2870.jpg**

**jellyfish.jpg**

**$R = $RJPSR47.jpg**

**$I = $IJPSR47.jpg**

**Windows XP**

When files were placed into the Recycle Bin they were placed within a hidden directory named \Recycler\%SID% where %SID% is the SID of the user that performed the deletion.

A file named INFO2 was placed in the user’s Recycler directory and it container entries, identified by index number, which described the original files size, full path/name, and size.

**Windows Vista and Windows 7**

Recycle Bin is located in a hidden directory named \$Recycle.Bin\%SID%, where %SID% is the SID of the user that performed the deletion.

When files are moved into the Recycle Bin, the original file is renamed to $R followed by a set of random characters, but maintaining the original file extension.  At the same time a new file beginning with $I followed by the same set of random characters given to the $R file and the same extension, is created; this file contains the original filename/path, original file size, and the date and time that the file was moved to the Recycle Bin.  You’ll also notice that all of the $I files are exactly 544 bytes long.

**4. Cookies Folder**

Cookies are pieces of code created by websites and placed on the user’s local computer to allow identification of the user on subsequent visits. Cookies documents exhibited preferences. Examiners can gain insight to the sites accessed by the user. The dates and times maintained by these text files, as well as the visit count provide additional information about the user’s activity.

In Windows Vista and Windows 7, cookies folder is found at

\users\%username%\AppData\Roaming\Microsoft\Windows\Cookies

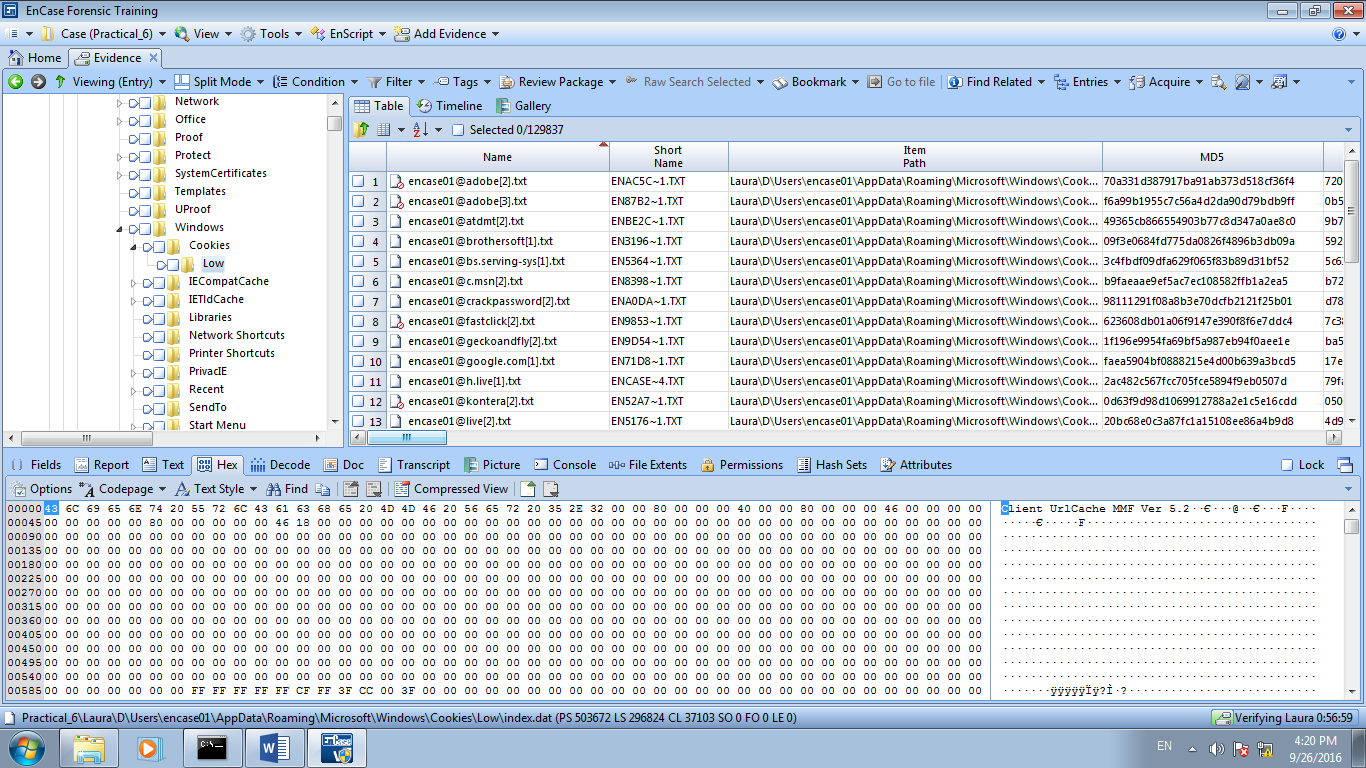


Figure 4: Cookies folder

**5. Temporary Internet Files (TIF)**

This folder contained in the TIF folder stores the files downloaded and cached from the Internet. By storing or caching these files, when a user returns to a site they often visit, the browser checks to see whether the files in cache are current. If so, there is no need to download from the Internet.

C:\Users\%UserName%\AppData\Local\Microsoft\Windows\Temporary Internet Files\

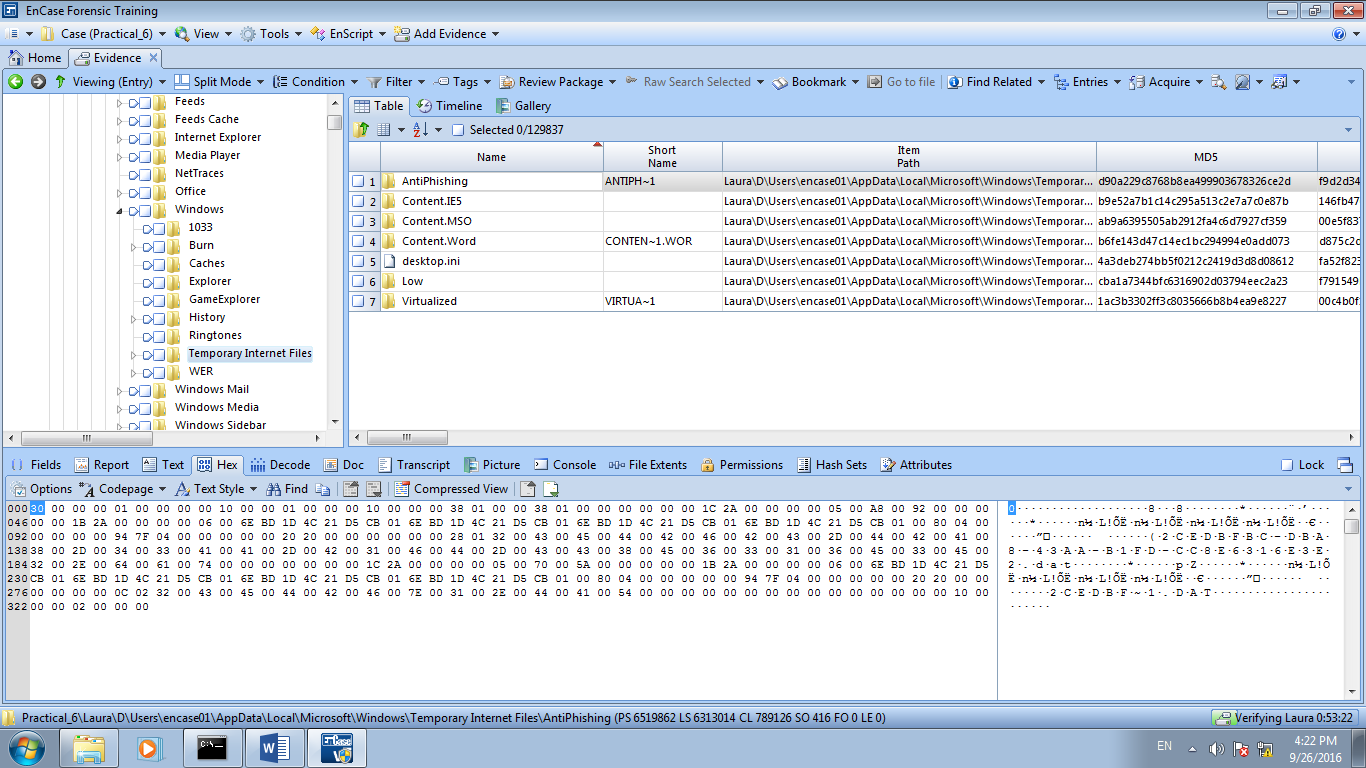


Figure 5A: Temporary Internet Files

**6. Recent Folder**

This folder contains link files (short cuts)

C:\Users\%UserName%\AppData\Roaming\Microsoft\Windows\Recent

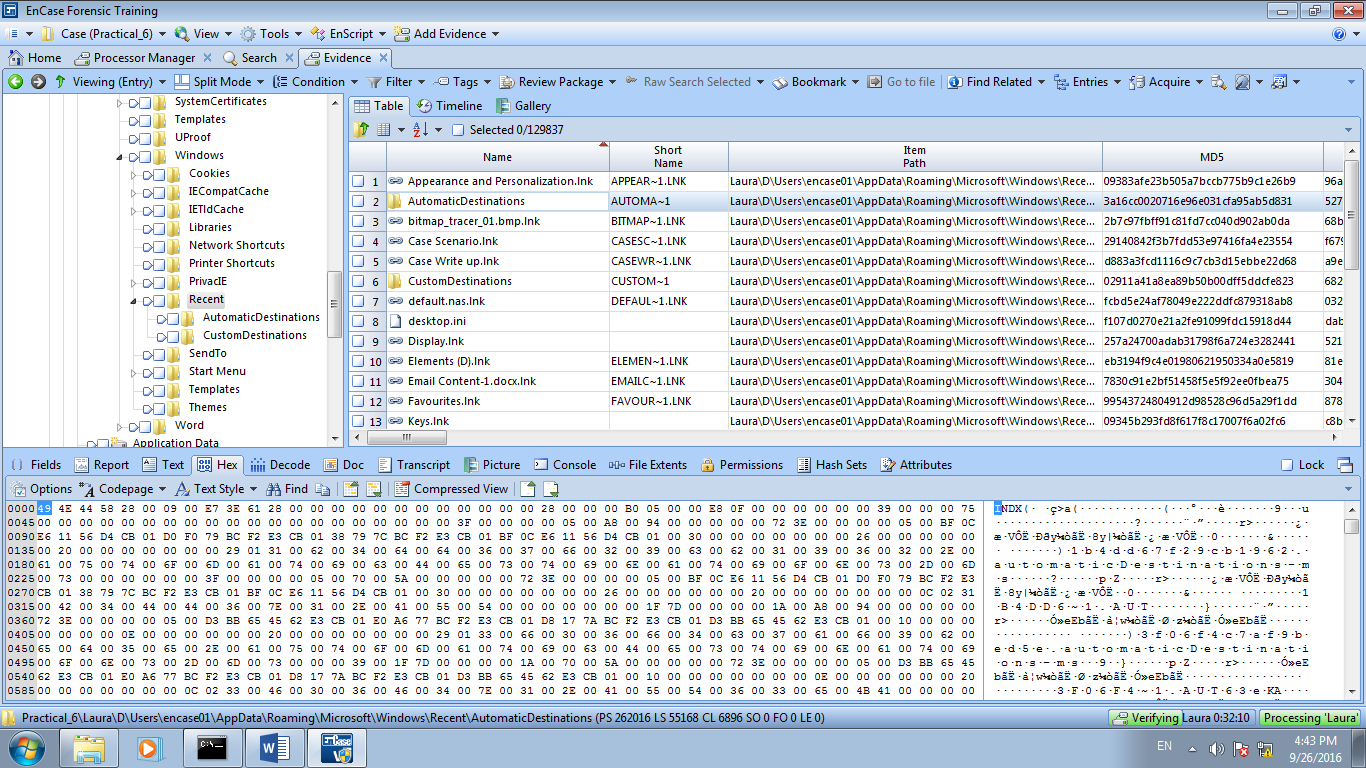


Figure 6: Recent folder

**7. History Folder**

C:\Users\%UserName%\AppData\Local\Microsoft\Windows\History

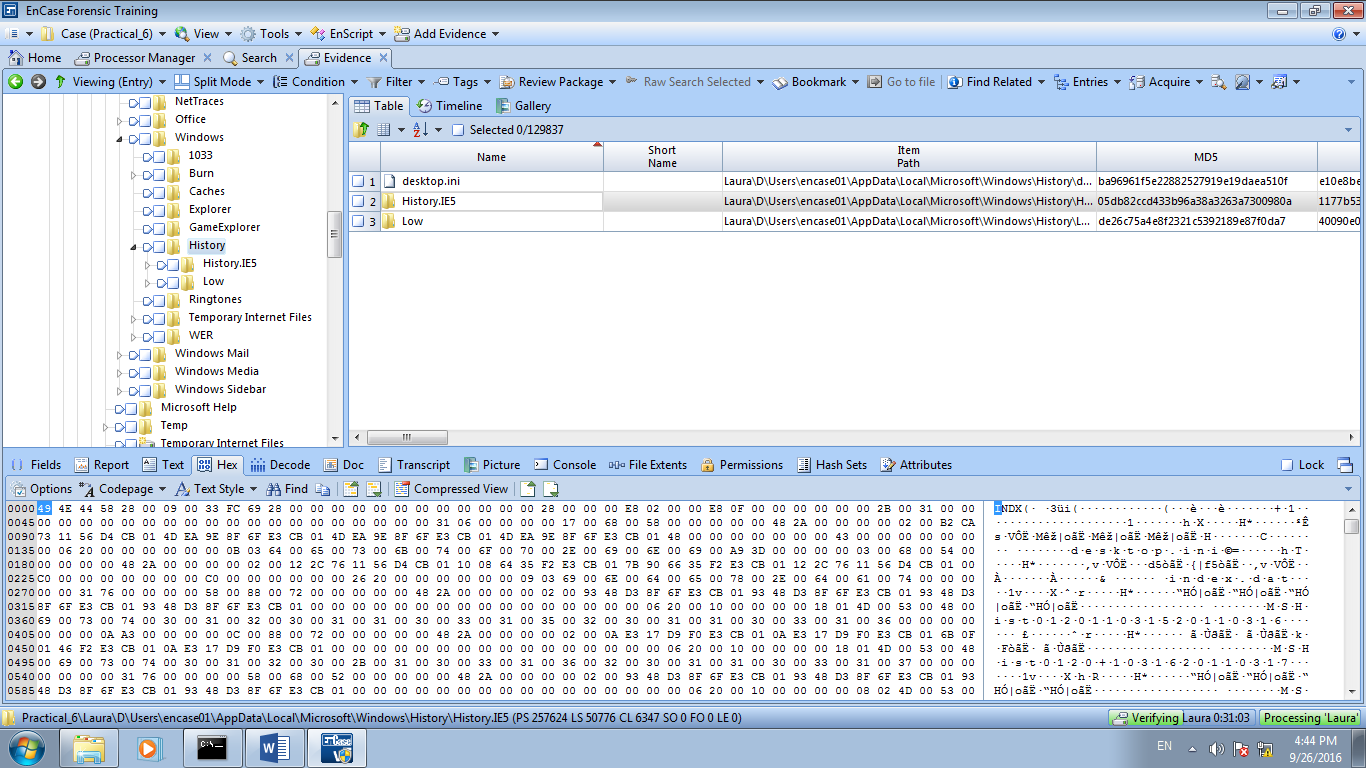


Figure 7: History folder

**8. Favorites Folder**

Favorites Folder is located at C:\Users\%UserName%\Favorites

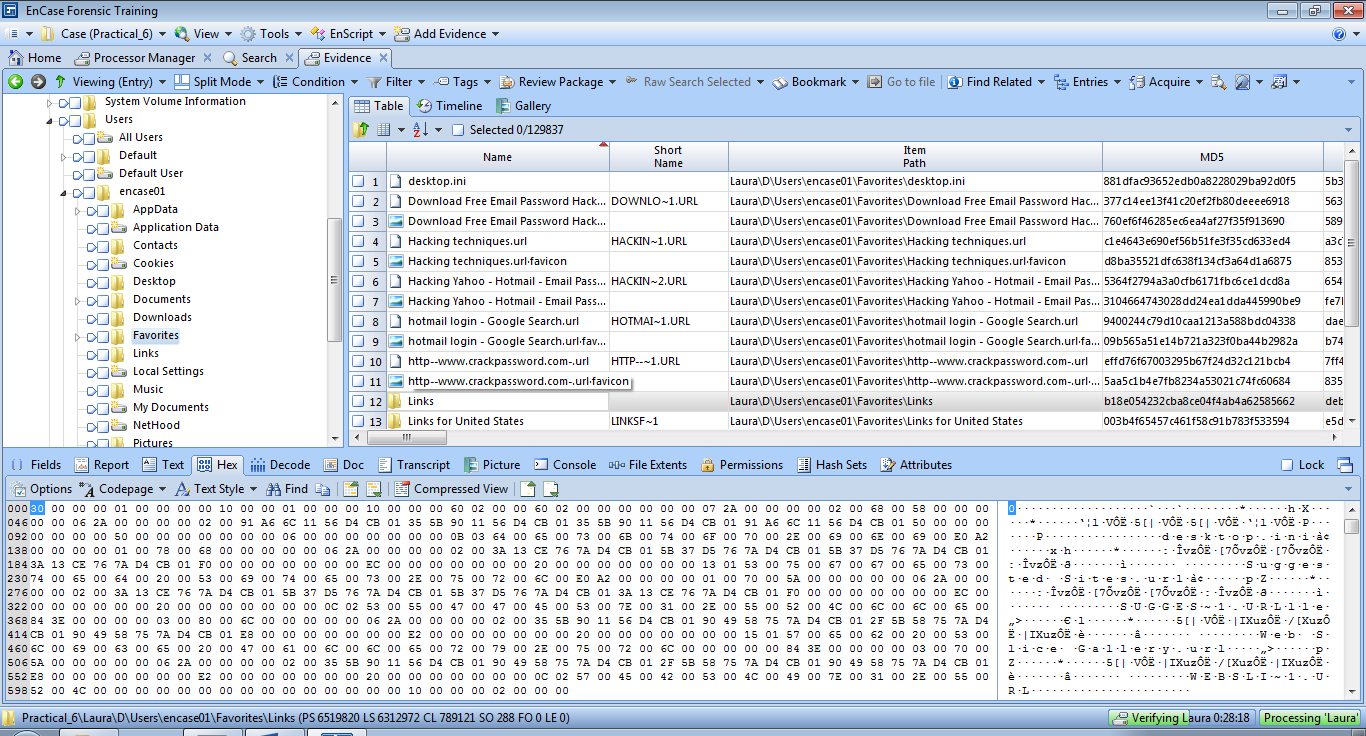


Figure 8A: Favorites folder

**Use the following text style to view:**

Text Style ISO Latin @ 100

Book mark some of the URLs that the user visited.

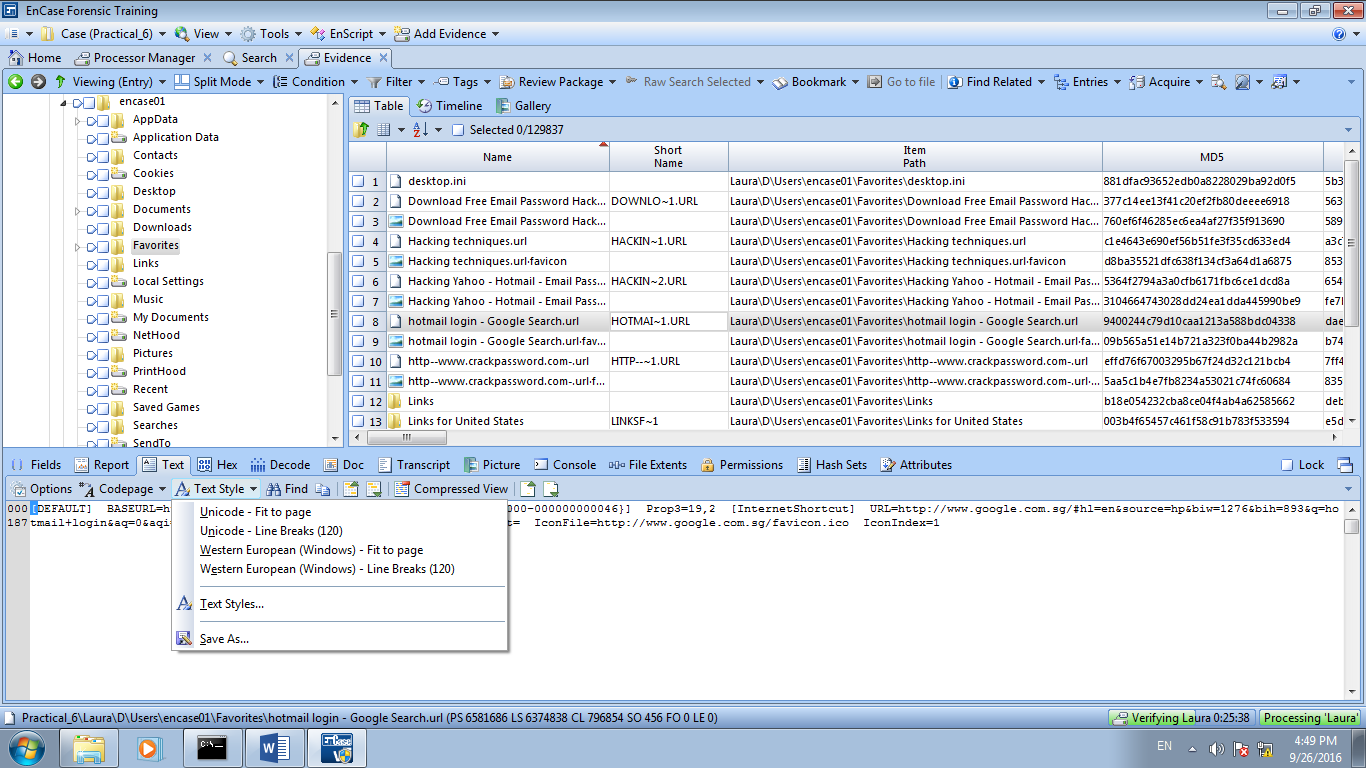


Figure 8B: Changing Text Styles to view Favorites Folder

Choose Option 4 Western European

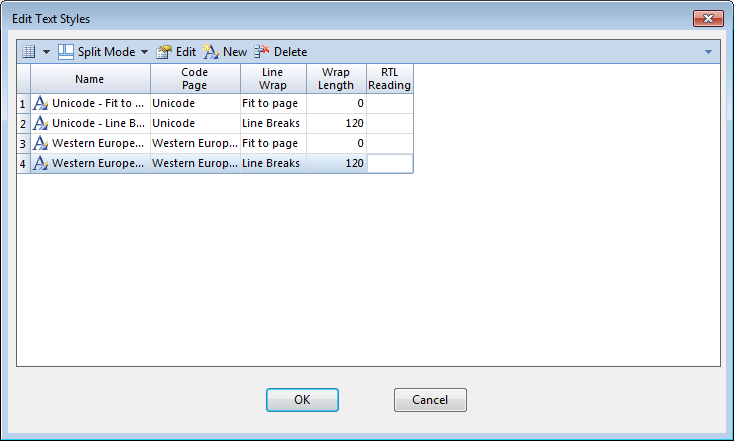


Figure 8C: Choose Text Styles Western European

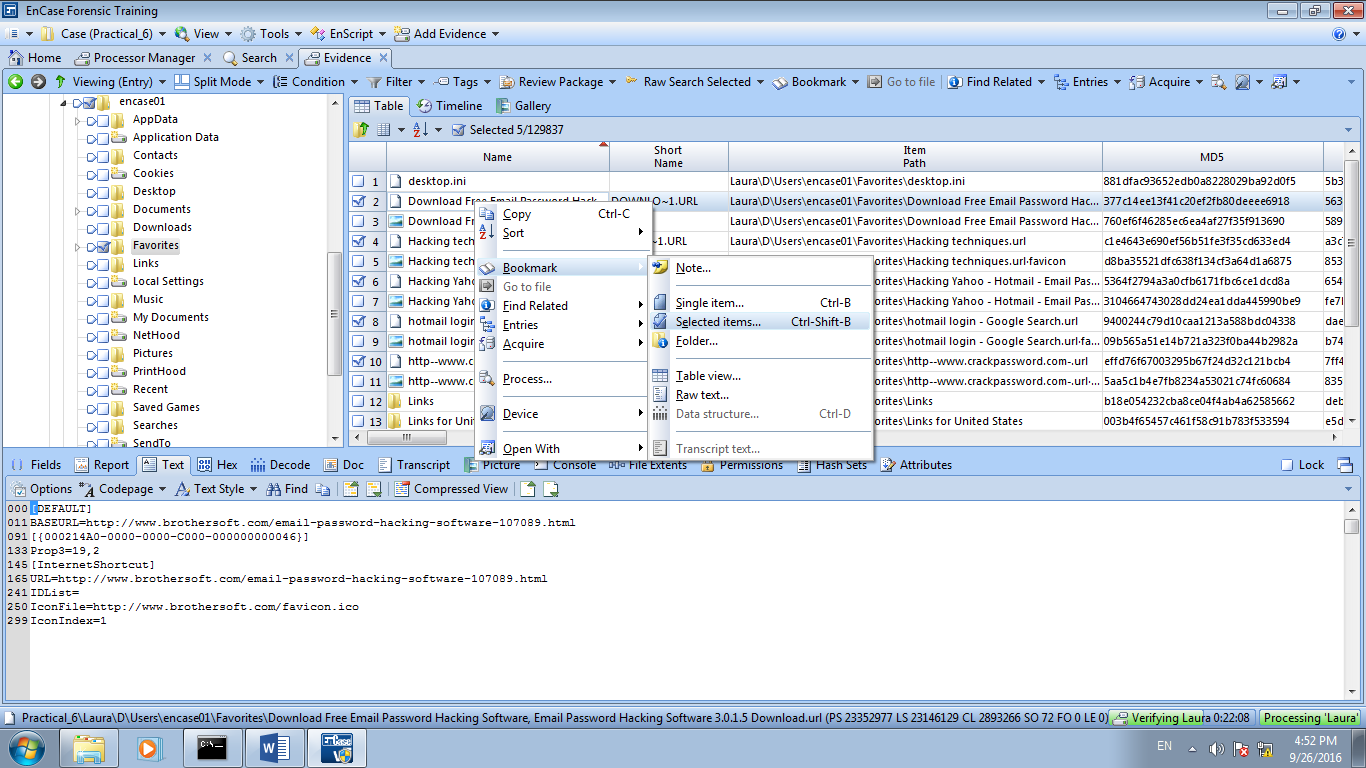


Figure 8D: Bookmark selected favorites to new folder

Created a new folder name Favorites under the folder Bookmarks | Internet Artifacts folder.

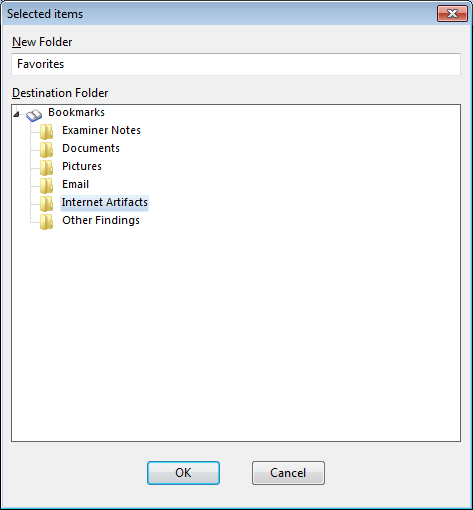
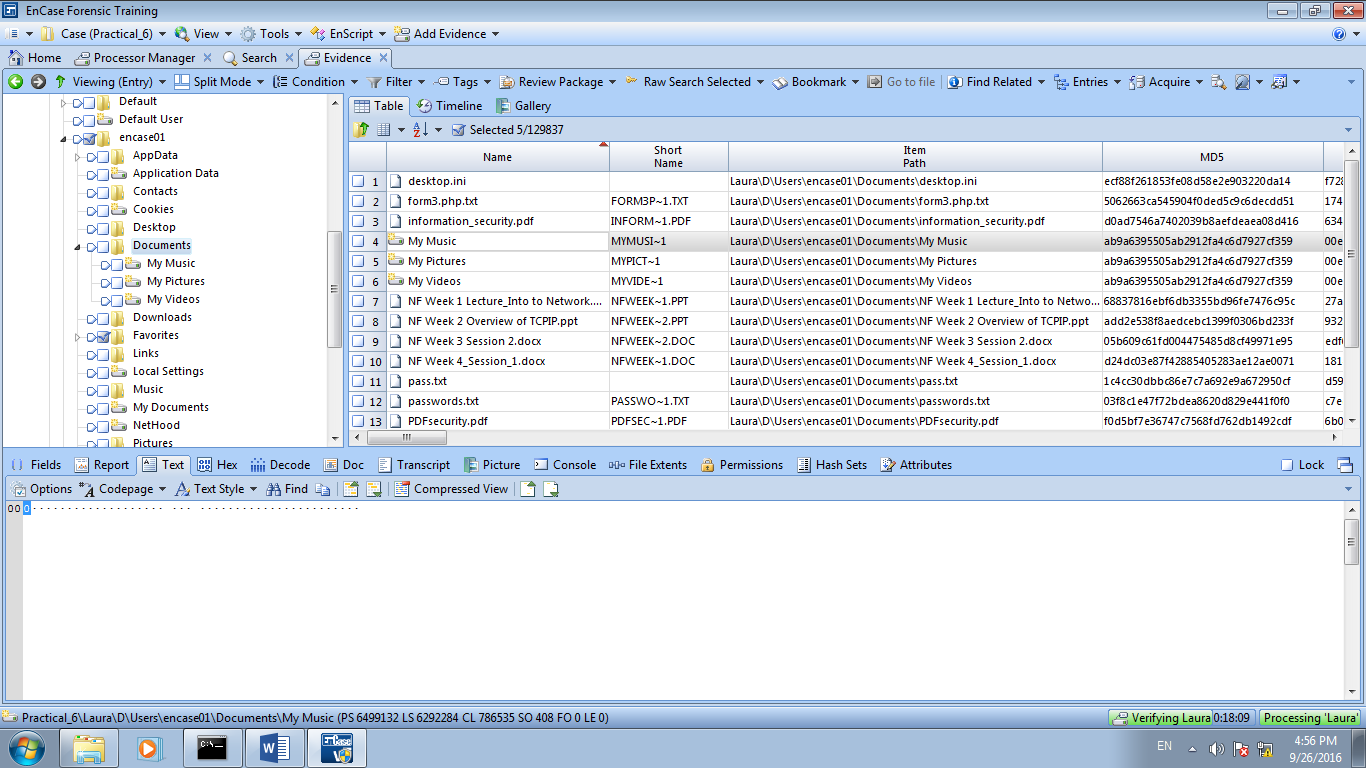


Figure 8E: New Bookmark folder, Favorites

**9. My documents**

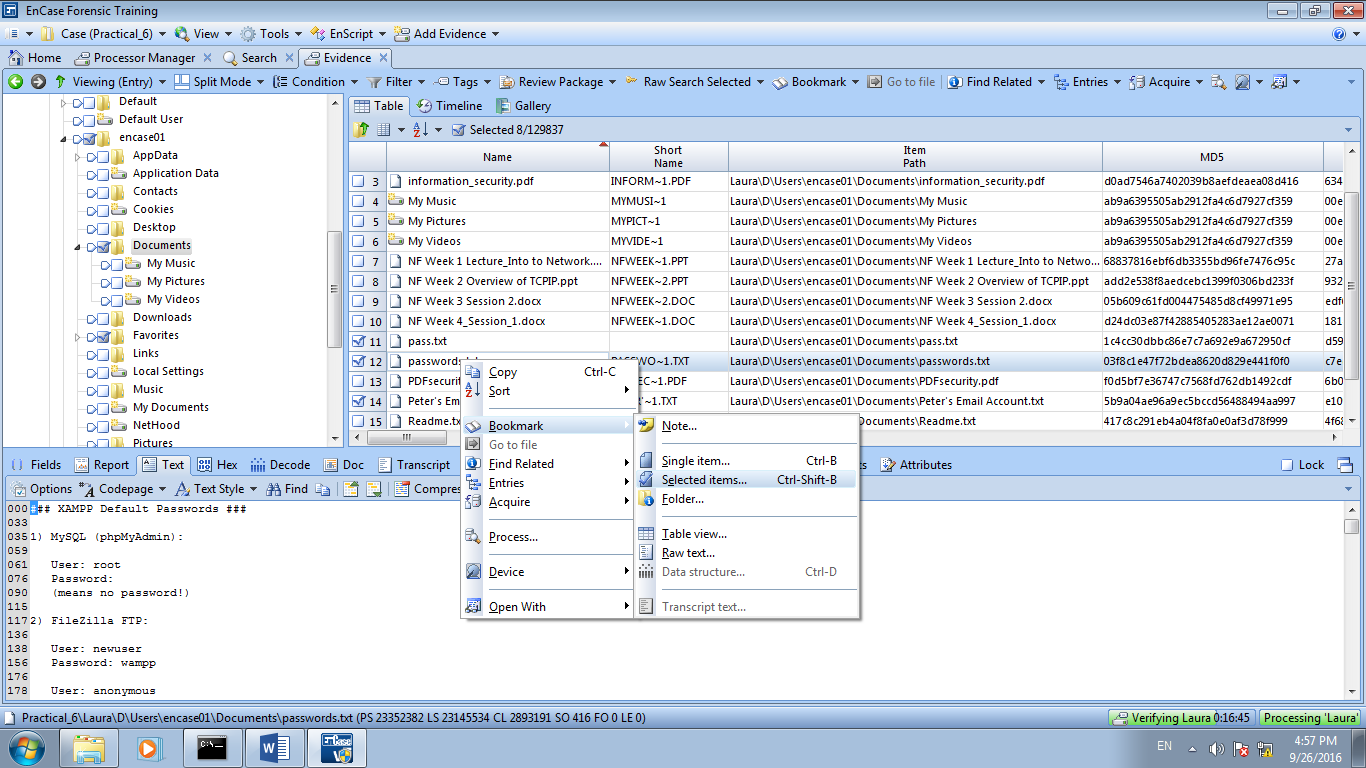
In older versions of Windows, under each root user folder there is, by default, a folder names My Documents. By default, it contains a subfolder My Pictures and most likely My Music and my eBooks.

In Windows Vista and Windows 7, this folder is replaced by folder named “Documents”. It is still directly under the root user folder.

Figure 9A: Documents folder

Bookmark the selected documents

Create a new folder name **Suspected Passwords** under the folder Bookmarks | Documents.

Figure 9B: Bookmark selected documents

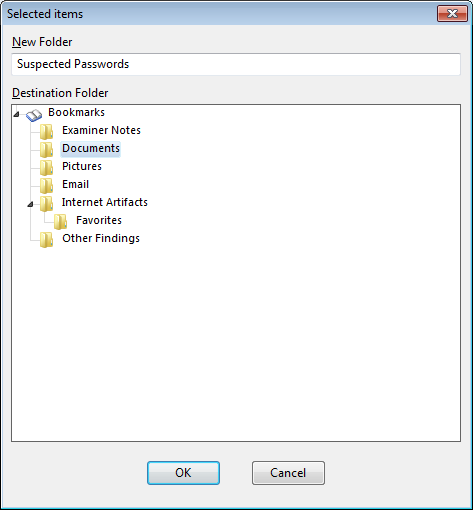


Figure 9C: Bookmark selected documents into Suspected Passwords folder

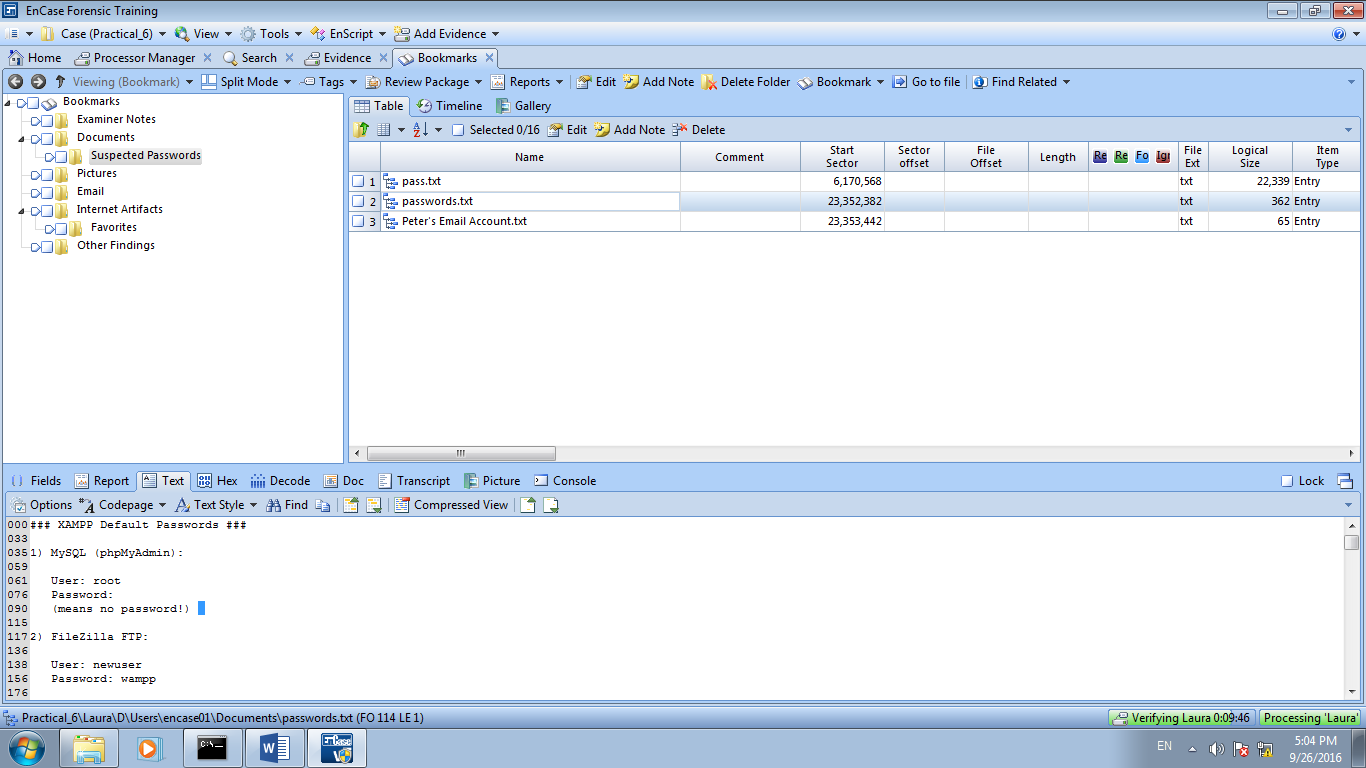


Figure 9D: Selected documents bookmarked into Suspected Passwords Folder

**10. Sent To folder**

The Send To folder contains the objects or links that will appear in the Explorer interface under the right-click option Sent To.

It is located at C:\Users\%UserName%\AppData\Roaming\Microsoft\Windows\SentTo

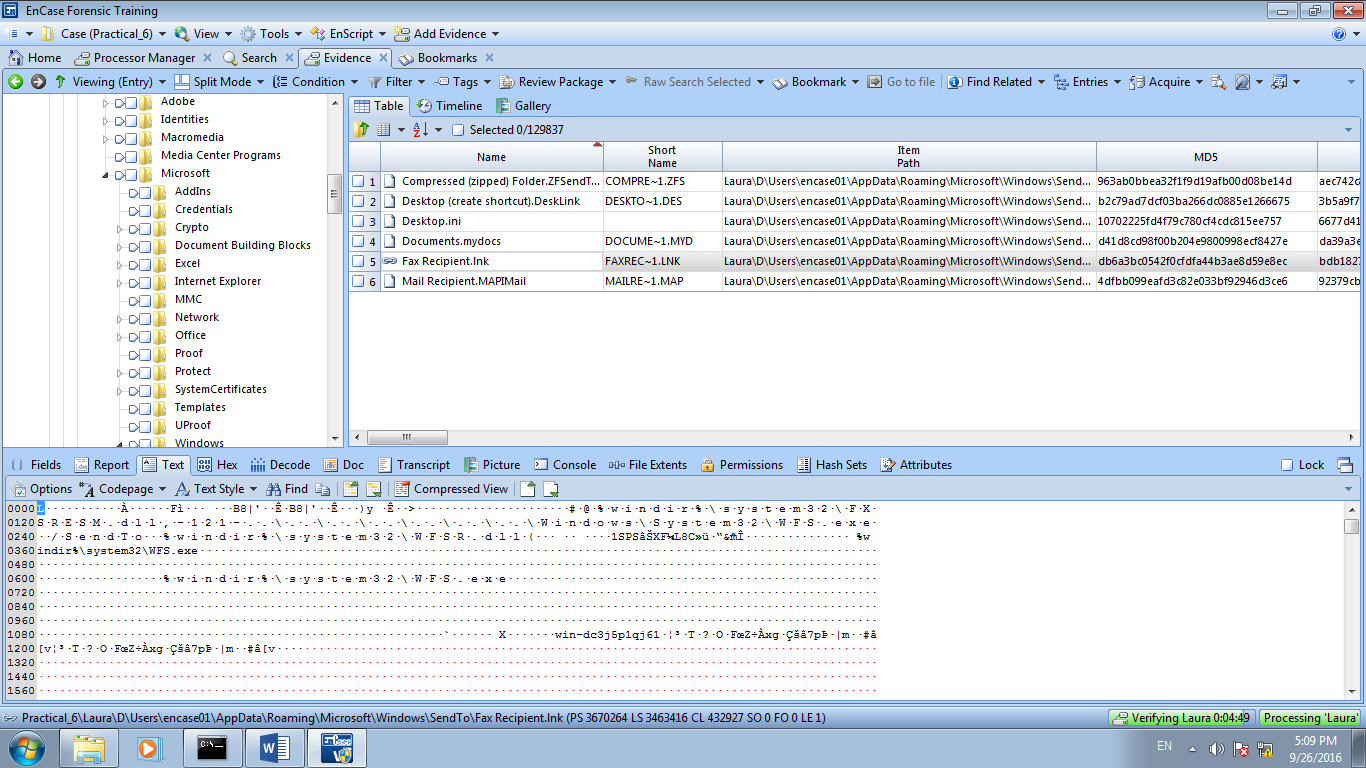


Figure 10: Sent To folder

**11. Temp Folder**

This is a subfolder of the Local Settings folder. In Windows Vista and Windows 7 this folder is located at C:\Users\%UserName%\AppData\Local\Temp. This folder is to temporary store files. This folder can contain temporary files from program installation that are often overlooked when removing programs.

We may be able to find evidence here that refutes a claim that a user never had a given application installed on his/her system.

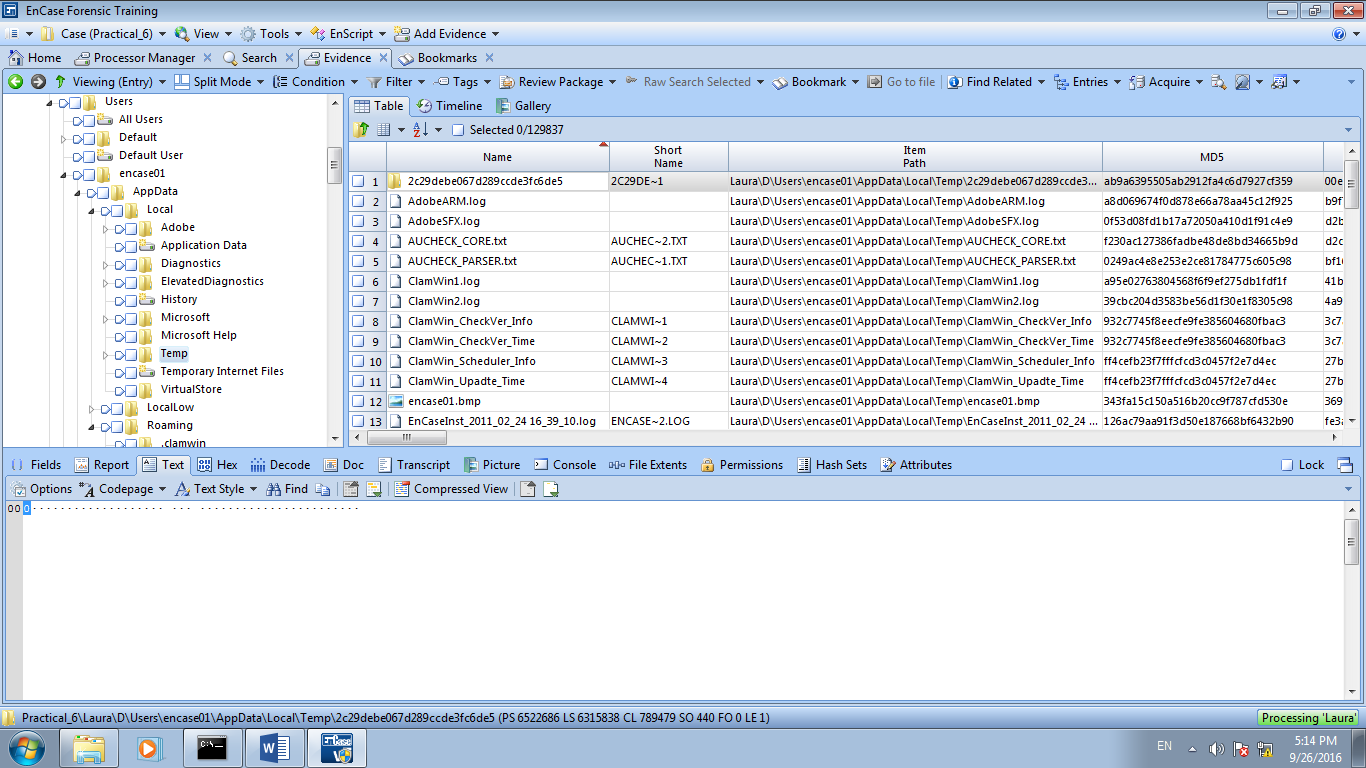


Figure 11: Temp folder

**12. Desktop Folder**

This folder contains items that populate the user’s Desktop. The items within this folder will be those that the user has intentionally placed or those which applications have generated during installation. The Desktop folder of All Users account must be evaluated as well as any items present within the All Users Desktop folder can appear on the Desktop of the specific user.

In Windows Vista and Windows 7, the All Users folder has been replaced with a folder called “Public.” The user’s Desktop is located at the following path:

C:\Users\%UserName%\Desktop

The operating system can also be configured to place items on the Desktop that will not be listed within the Desktop folders, including icons for My Computer, Recycle Bin, My Network Places, My Documents, and others.

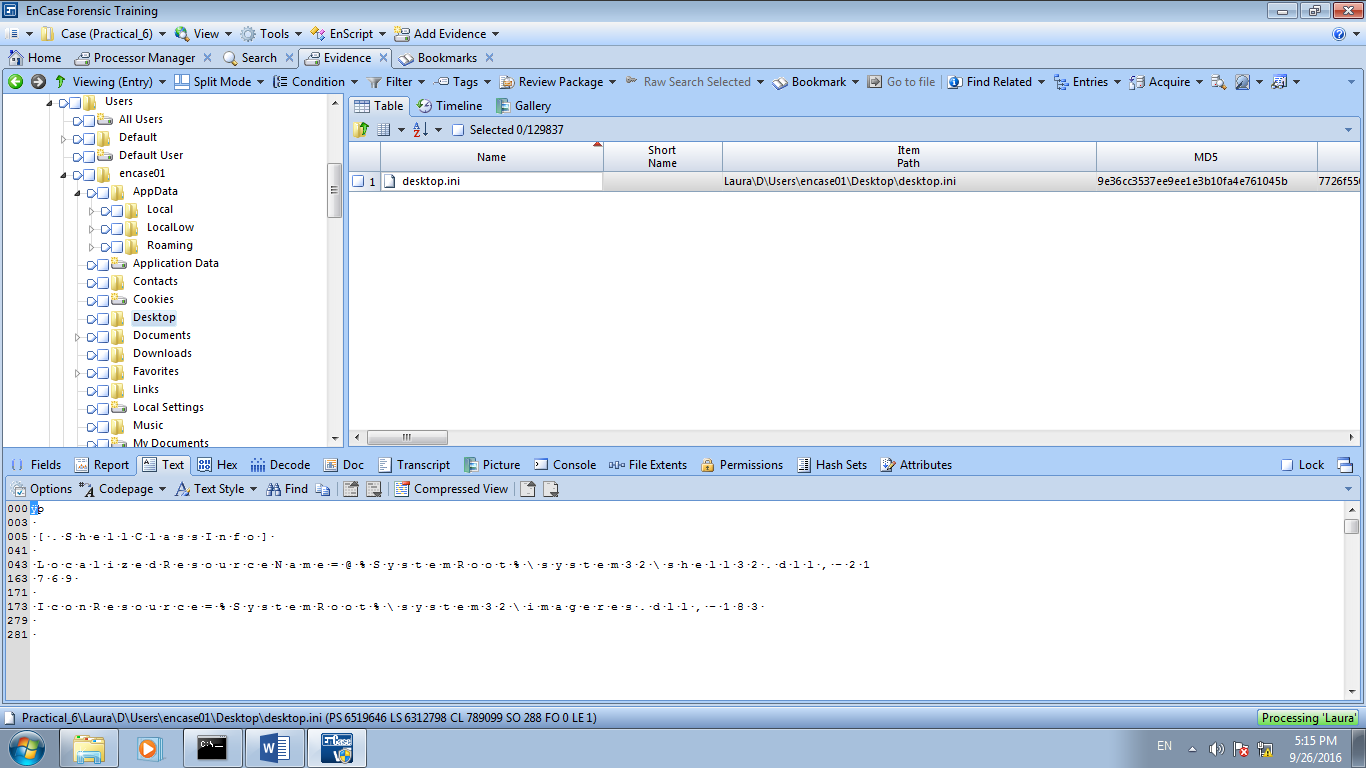


Figure 12: Desktop folder

**Part B: Exporting Event (Security) Logs**

Locate Security log file from Laura’s case

**Show the location of Security.evtx**

D:\Windows\System32\winevt\Logs

Check-select the file, right-click and select **Entries**, **Copy Files**.

Click Next, Next to accept all default settings. Use the default/base folder as destination folder (take note of the location). Click Finish.

Navigate to the default/base folder location to retrieve the file. Open the file with MyEventViewer at C:\Users\MyEventViewer.

Note: The FI will normally attach the exported file with forensic/examiner report for submission to court.

- The End -