**Chapter 4**

**Recycle Bin Forensics and Link Files**

**V1**

**A blue outline of a bird with a crown and text

Description automatically generatedSID: 2103022**

**Anglia Ruskin Final Project**

**Table of Contents**

[**Introduction** 2](#_Toc160296624)

[**Objective** 2](#_Toc160296625)

[**1.0** **Recycle Bin Forensics** 3](#_Toc160296626)

[**2.0 Link Files** 7](#_Toc160296627)

# **Introduction**

The fourth chapter covers Recycle Bin Forensics and Link Files (LNK) which allows an investigator to gather large amounts of important information on a suspect’s file deletion usage and application, file or folder opening. The chapter aims to teach the reader how to firstly see the date the file was deleted, the location of the drive and name, file size in bytes and OS version all this information can be used as contributing evidence and see the full path, times of creation and modification along with other evidence that could help an investigator create a timeline of events.

# **Objective**

* See ‘$’ names of deleted files.
* Expand said files to the desktop and parse them to see details.
* Find LNK files to know when an application, file or folder was last opened or edited.

1. **Recycle Bin Forensics**

1.Login as Digital-Forensics and use the password **‘password’** to login to the VM.

A login screen with a beach and rocks

Description automatically generated

2. Search for ‘cmd’ in the search bar and click on ‘Run as administrator’ and click ‘Allow’.

A screenshot of a computer

Description automatically generated

3. Type ‘cd ..’ twice to return to the C:\ drive.

A screen shot of a computer code

Description automatically generated

4. Type ‘dir /a’ to list all in the current directory, here we can see $Recycle.Bin.

A computer screen shot of a black screen

Description automatically generated

5. To enter the recycle bin type ‘cd $Recycle.Bin’.

A black background with white text

Description automatically generated

6. List all in directory with ‘dir /a’ to list the users.

A computer screen with white text

Description automatically generated

7. The names are hidden so to reveal the account we are using ‘Digital-Forensics’ type ‘wmic useraccount get name,sid’.

A screenshot of a computer screen

Description automatically generated

8. Copy the SID of ‘Digital-Forensics’ like the figure below.

A screenshot of a computer screen

Description automatically generated

9. On the desktop right click and create a folder called ‘Outcome’.

A screenshot of a computer

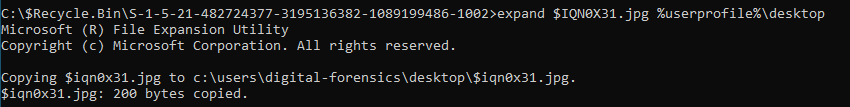
Description automatically generated

10. Return to the command prompt and let’s go into the account so type ‘cd’ click space and copy the SID then click enter, you will now see the parses of deleted files.

A computer screen shot of a black screen

Description automatically generated

11. Copy/expand one of those to the desktop using ‘expand $IQN0X31.jpg %userprofile%\Desktop\Outcome’



12. Open the ‘$l\_Parse.exe’ application located in the tools folder on the desktop.

A person reaching into a bucket

Description automatically generated

13. Click the first browse button and find the ‘Outcome’ folder you made in step 10. Click the second browse and locate the desktop and name it text then click ‘Parse!’.

A screenshot of a computer

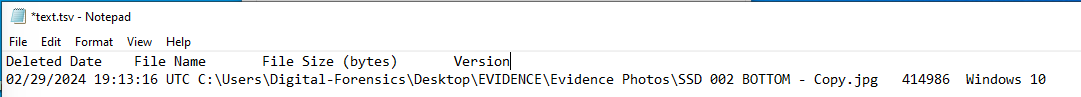
Description automatically generated

14. A ‘.tsv’ file will appear on the desktop, double click to open it.

A computer screen shot of a calendar

Description automatically generated

15. You can now see the date the file was deleted, the location of the drive and name, file size in bytes and OS version all this information can be used as contributing evidence.



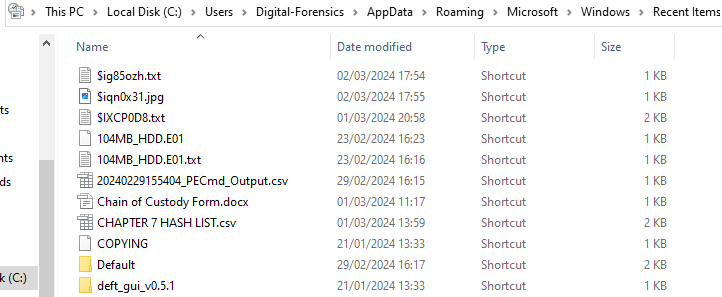
# **2.0 Link Files**

1. Open File explorer by searching for it in the search bar or locating it on the taskbar.

A screenshot of a computer menu

Description automatically generated

2. Locate the Recent Items folder by following the file path from the figure below which allows us to see the full path, times of creation and modification along with other evidence that could help an investigator create a timeline of events.



4. The chapter is complete, and you can now see the date the file was deleted, the location of the drive and name, file size in bytes and OS version all this information can be used as contributing evidence and see the full path, times of creation and modification along with other evidence that could help an investigator create a timeline of events. You can close all applications and return to the desktop for Chapter 5 or shutdown if you wish to continue later.