Sanjana Asrani **DF**
D17B/01/Batch B **Lab 05: Recycle bin Forensics**

Aim: To perform Windows Recycle Bin Forensics

Theory:

1. Introduction to Windows Recycle Bin:

The Recycle Bin is an integral part of the Windows operating system, providing users with a safety net when they accidentally delete files. Instead of immediately deleting files from the system, Windows moves them to the Recycle Bin, where they remain until the Recycle Bin is emptied or the files are restored. This behavior allows for the recovery of deleted files, making it crucial in forensic investigations where deleted data might hold valuable information.

2. Structure of the Recycle Bin:

Understanding the internal structure of the Recycle Bin is essential for effective forensic analysis. Typically, the Recycle Bin is located in the root directory of each drive, such as C:\$Recycle.Bin. Within the Recycle Bin, there are subdirectories corresponding to each user's Security Identifier (SID). These directories store deleted files associated with specific user accounts. Each deleted file consists of two components:

- $I File: This file contains metadata about the deleted file, including its original name, full path, size, and deletion timestamp.
- $R File: The $R file contains the actual contents of the deleted file. It serves as the key for data recovery, as it holds the raw data of the deleted file.

3. Conducting Forensic Examination:

Forensic examination of the Recycle Bin involves several crucial steps:

- Preparation: Before starting the examination, it's important to consider potential challenges. Deleted data may have been overwritten by new files, and metadata could have been altered during deletion.
- Scanning: Use forensic software to scan the Recycle Bin for deleted files. This software should be capable of parsing $I files to extract metadata and $R files for data recovery.
- Validation: Validate the recovered data against other sources to ensure its accuracy. Cross-referencing with other artifacts or timestamps can help verify the integrity of the recovered files.

- Recovery: Extract the contents of $R files to recover deleted files. This step involves reconstructing the original files using the raw data stored in the $R files.

4. Tools for Recycle Bin Forensics:

Various forensic tools are available for analyzing the Recycle Bin and recovering deleted files:

- RecBin.exe: A command-line tool specifically designed for parsing $I files and extracting metadata about deleted files.
- FTK Imager, EnCase, Recuva, Disk Drill, TestDisk: These tools offer comprehensive features for forensic analysis and data recovery, including support for Recycle Bin examination.
- WinHex, Autopsy: These tools provide advanced capabilities for analyzing disk images and conducting detailed forensic examinations, including Recycle Bin analysis.

5. Live Machine Analysis:

In live forensic scenarios, PowerShell commands can be utilized to gather information and recover deleted files directly from the Recycle Bin. PowerShell commands such as Get-ChildItem and Get-Content allow investigators to navigate through Recycle Bin directories, view metadata from $I files, and extract data from $R files.

Practical:

1. Getting into the Recycle Bin and listing the directories

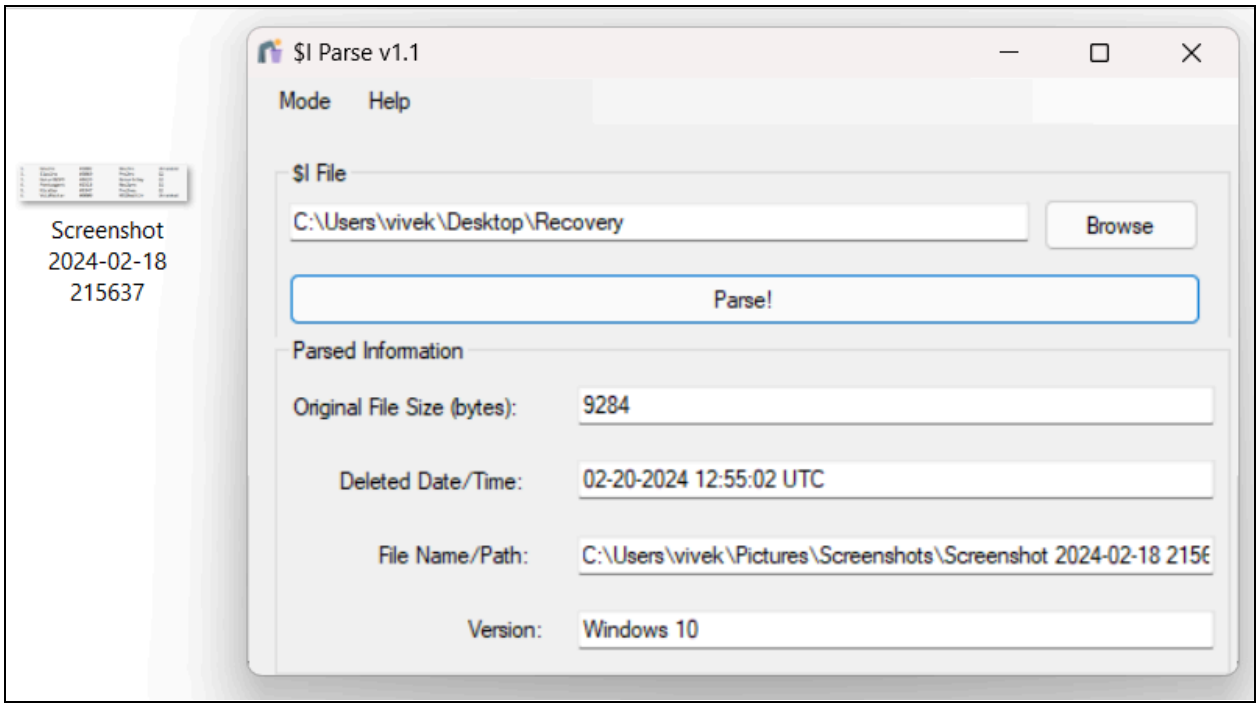
```
C:\>cd \$Recycle.Bin

C:\$Recycle.Bin>dir /a
 Volume in drive C is OS
 Volume Serial Number is F480-47BC

 Directory of C:\$Recycle.Bin

01-11-2023  20:51    <DIR>          .
22-02-2024  23:20    <DIR>          ..
01-11-2023  20:51    <DIR>          S-1-5-18
20-02-2024  18:25    <DIR>          S-1-5-21-2163609921-1118582017-2635375461-1001
               0 File(s)              0 bytes
               4 Dir(s)  287,525,826,560 bytes free
```

2. Knowing the SID of the current user and getting inside the recycle bin of the current user. Also listing the items for the current user

```
C:\$Recycle.Bin>whoami /user

USER INFORMATION
----------------

User Name    SID
============ ==============================================
neu2ro\vivek S-1-5-21-2163609921-1118582017-2635375461-1001

C:\$Recycle.Bin>cd S-1-5-21-2163609921-1118582017-2635375461-1001

C:\$Recycle.Bin\S-1-5-21-2163609921-1118582017-2635375461-1001>dir /a
 Volume in drive C is OS
 Volume Serial Number is F480-47BC

 Directory of C:\$Recycle.Bin\S-1-5-21-2163609921-1118582017-2635375461-1001

20-02-2024  18:25    <DIR>          .
01-11-2023  20:51    <DIR>          ..
20-02-2024  18:25               166 $IKVRW28.png
01-11-2023  17:22               129 desktop.ini
               2 File(s)            295 bytes
               2 Dir(s)  287,520,325,632 bytes free
```

3. Getting the $I of the data that needs to be recovered and Recovering it using the $I Parse application

```
C:\$Recycle.Bin\S-1-5-21-2163609921-1118582017-2635375461-1001>copy $IKVRW28.png \Users\vivek\Desktop\RecoveredData
       1 file(s) copied.
```


Screenshot
2024-02-18
215637
$I Parse v1.1
Mode
Help
$I File
C:\Users\vivek\Desktop\Recovery
Browse
Parse!
Parsed Information
Original File Size (bytes):
9284
Deleted Date/Time:
02-20-2024 12:55:02 UTC
File Name/Path:
C:\Users\vivek\Pictures\Screenshots\Screenshot 2024-02-18 2156
Version:
Windows 10

Conclusion: