|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 4 |
| Tutorial 4 |
| **Windows Artifacts** | |

**OBJECTIVES**

After completing this topic, you should be able to:

1. Identify locations where evidence may be located;
2. Explain what happen when files are deleted in Windows operating systems.

Q1 Where can you find the date and time of when a file was sent to the Recycle Bin on Windows 7 OS?

A. INFO2 file

B. Original file name’s last access date

C. DOS directory or MFT

D. $I index file

Q2 In NTFS, information unique to a specific user is stored in the \_\_\_\_\_\_\_\_ file.

A. USER.DAT

B. NTUSER.DAT

C. SYSTEM.DAT

D. None of the above

Q3 Most of a user’s desktop items on a Windows 7 operating system would be located in the \_\_\_\_\_\_\_\_ directory.

A. C:\Windows\Desktop

B. C:\WinNT\Desktop

C. C:\Windows\system32\config\Desktop

D. C:\Users\%UserName%\Desktop

Q4 Where can you find evidence of web-based email such as from MSN Hotmail or Google Gmail on a Windows XP system?

A. In Temporary Internet Files under Local Settings in the user’s profile

B. In unallocated Clusters

C. In the pagefile.sys folder

D. All of the above

Q5 File names with the .url extension that direct web browsers to a specific website are located in which folder?

A. Favorites folder

B. Cookies folder

C. Send To folder

D. History folder

Q6 The Temporary Internet Files directory contains \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

A. Web pages that are cached or saved for possible later reuse

B. An index.dat file that serves as a database for the management of the cached files

C. Web mail artifacts

D. All of the above

Q7 Which of the following is NOT true regarding NTUSER.DAT file?

A. It is a registry file

B. Every user profile created on a Windows operating system has an NTUSER.DAT

file

C. It is updated by the operating system when the user logs out

D. Last accessed time can be used to possibly determine when the user last logged

out

Q8 Andy deleted a file named resume.docx in the folder C:\Users\Andy. Assuming that his machine is running Windows 7 operating system. Which of the following statement is FALSE?

A. The file is moved to \$Recycle.Bin\SID folder

B. The file resume.docx is renamed to $R followed by a set of random characters,

followed by the original file extension

C. A file is created as $I followed by the same random characters and extension as

the $R file

D. A hidden file named INFO2 is used to store resume.docx’s original file name and

path, date and time of deletion

Q9 Which of the following is NOT true regarding the following folder:

C:\Users\Andy\AppData\Roaming\Microsoft\Windows\Cookies

A. It stores the authentication information when Andy visits websites

B. It stores text files created by Andy

C. It stores Andy’s site preferences

D. It stores Andy’s shopping cart contents

Q10 Which of the following folders does NOT have the Low folder?

A. Cookies folder

B. History folder

C. Temporary Internet Files folder

D. Sent To folder

Q11 You are investigating a user’s computer. If you would like to check the details of the print jobs sent by the user, which folder should you inspect?

A. Cookies folder

B. Sent To folder

C. Temp folder

D. History folder

Q12 For an Internet Explorer user, to find out the list of Internet websites’ URL that the user often visits, you would inspect the \_\_\_\_\_\_\_ folder.

A. Desktop

B. Cookies

C. Favorites

D. Temporary Internet Files

Q13 Which folder would usually contain link files that link to recently accessed files, folders, and applications?

A. Recent folder

B. Sent To folder

C. Link folder

D. Low folder

Q14 Explain what happens when a file/folder is deleted in the following Windows Operating System:

a. Windows XP

When files or folders are sent to the Recycler they remain as live files, taking up allocated space and being protected from being overwritten. The file data is untouched but the file and folder names are amended.

In Windows XP files sent to the Recycler are relocated to a hidden directory named \Recycler\SID where SID is the SID of the user that performed the deletion. The files are renamed to D followed by the drive letter followed by an sequential index number, followed by the original file extension, e.g. Dc145.doc

There is also a file named INFO2 which contains entries, identified by the index numbers, that describe the original file and folder sizes and path/names, etc.

When a folder is sent to the recycler, the folder name is changed in the same way as a file but without any extension

b. Windows 11/10/8/7/Vista

In later Windows Oss (10/8/7/Vista), the Recycler is in a hidden directory named \$Recycle.Bin\SID, Where SID is the SID of the user that performed the deletion. When a file is sent to the Recycler it is renamed to $R followed by a set of random characters, followed by the original file extension, e.g. $Rhdxenv.doc. A matching file is created as $I followed by the same random characters and extension as the $R file. This file contains the original filename/path and file size, and the date and time that the file was moved to the Recycle Buin (There is no INFO2 file). The $I files are all 544 bytes long.

Similarly to XP, when a folder is sent to the Recycler their folder name is changed in the same way as a file but without any extension.

Q15 You were looking for Skype chat messages on a suspect’s computer. Identify the folder location and any special tools involved to extract the Skype chat messages.

Skype client store the instant messaging history in the following folder: C:\Users\%UserName%\AppData\Roaming\Skype\<aliases>\main.db

Examiner will need to make use of a SQLite database viewer to view the database files.

Q16 You are investigating a hacking case. You were told that the suspect might have used Metasploit framework to hack into a computer in the company’s intranet. When performing examination on suspect’s computer, where would you look out for evidences?

Metasploit framework is a tool for developing and executing exploit code against a remote target machine. It provides backend database support for PostgreSQL. The database stores information, such as host data, loot, and exploit results in %UserName%\metasploit\postgresql\data\ and its subfolders.

Note: PostgreSQL is an open source relational database management system (DBMS) developed by a worldwide team of volunteers.

- End -