Mission Name

LibrarianTest

Background

Claire and Ethan are at ACADEMIUM (PARIS), locating to THE LIBRARIAN. THE LIBRARIAN has answers about code snippets.

Technical High-Level Overview

The Librarian is going to make a special test to Claire, in order to get the Librarian Card. For completing the test, Claire will be provided a forensic image to recover a deleted file "Librarian Card".

Short Mission Description

You´re going to analyse a forensic imaged provide from The Librarian. Your goal is to identify Library Card ID.

Mission Description

The Librarian is going to make a special test to Claire, in order to get the Librarian Card. You´re going to analyse a forensic imaged provide from The Librarian. Your goal is to identify Library Card ID.

Location

FRANCE, PARIS | THE ACADEMIUM

Tools
- FTK Imager

Questions

Which is the SHA256 hash of ZIP file deleted?
- 457B7DBEE2C3606FAB242EBCD66AF673D222360A5C793BD26E8638613F947A4C

Which is the BMP version? Please provide full version
- Windows V3

Items
1. Use Access Data FTK Imager to open the evidence provided.
2. Recover deleted files using Access Data FTK Imager.
3. Extract ZIP file recovered.

Write Up

Linux Method.

1. ewfmount IMAGE.E01 ./rawimage/
2. tsk_recover -I raw -e /home/tools/rawimage/ewf1 /home/recon
3. ls -la /home/recon

Open ZIP file, open BMP file:

Librarian Card ID: 85478941234

Finally player will able to get Librarian Card ID: 85478941234

Windows Method
Player must mount the filesystem provided using Access Data FTK Imager and the select the evidence, selecting "Add evidence Item"
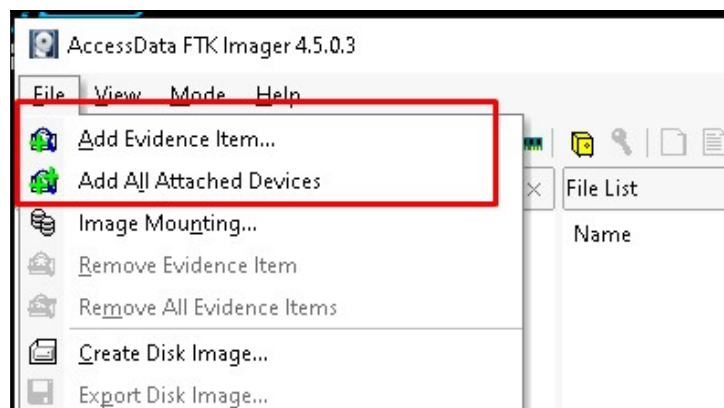

Figure 1

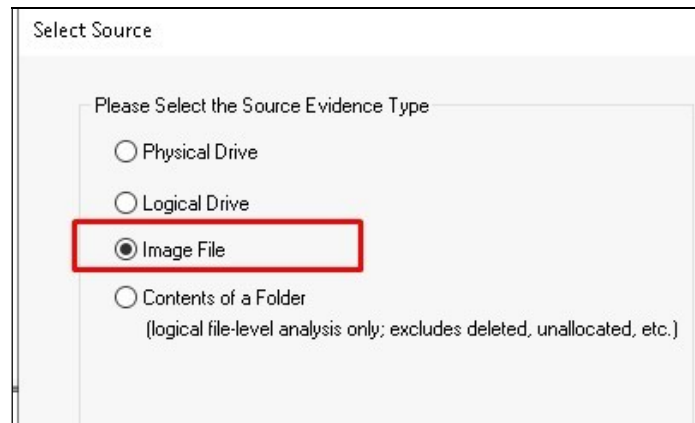Then, you must select "Image file" and after, select the evidence downloaded:

Figure 2

Once selected, open the evidence, expanding it on FTK:
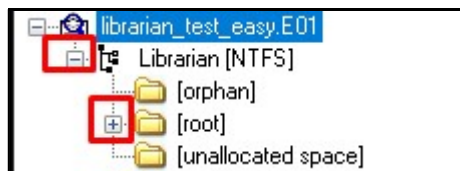

Figure 3

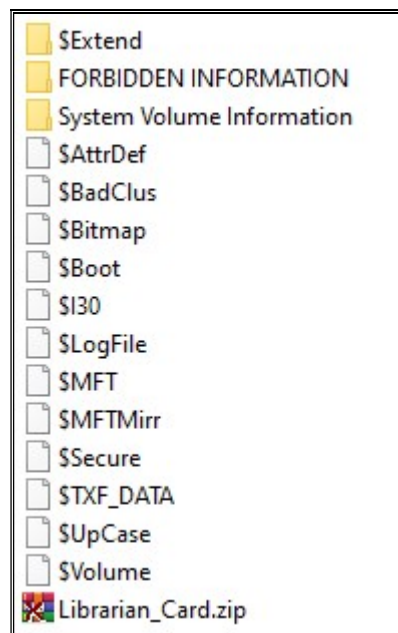Open root folder, and you will get deleted files marked with a red cross:

Figure 4

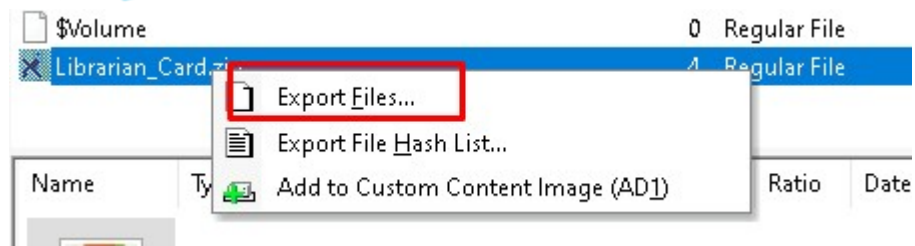Select "Librarian_card.zip", right click to show "Export files" option, and you must export the ZIP file to open it.

Figure 5

Open ZIP file, open BMP file:

Librarian Card ID: 85478941234

Finally player will able to get Librarian Card ID: 85478941234

Flag Information

flag{85478941234}