Windows Forensics lab

Introduction

In this practical you will use the Autopsy to examine a case

By the end of this lab you will be able to

- Use Autopsy to find various Windows artefacts

Task 1: Windows Forensics

Create a new case by using the Mantooth.E01 image and answer the following questions

Windows users information

1. What are the user accounts of the system?

2. Within the "Wes Mantooth" user directory, locate 10 files that are suspicious

Thumbs.db

3. Locate the thumbcache.db files for user "Wes Mantooth" and extract images that are stored in those files. Thumbcache viewer can be downloaded via https://thumbcacheviewer.github.io/

Recycle bin information

4. Identify a pair of $I and $R files which can be used to retrieve a file

5. What is the original file path for the deleted Camerashy.exe file? When was it recycled? Could it be recovered? Research on how camerashy could be used.

Prefetch

6. Find various information about the Xcopy application within the prefetch folder, including file name, file path, times run and last time run

Link files

7. Locate a number of link files for user Wes Mantooth and write down their link target information

Spool files

8. Identify spool files in the given image.

Event information

9. locate the **Security.evtx** file and export it to your desktop. Open the **Security.evtx** file and find out when the user Wes Mantooth logged on/logged off the computer.

Task 2: Viewing the browser history

Download the BrowsingHistoryView tool from https://www.nirsoft.net/utils/browsing_history_view.html; then extract the files within the downloaded zip file and run the BrowsingHistoryView tool to complete the following question.

1. List the top 10 most visited URLs along with the following information: title, visited time, visit count, Visited From, Web Browser, and Typed Count.

Task 3: Viewing browsing history within Google Chrome

Download the ChromeHisotryView tool from https://www.nirsoft.net/utils/chrome_history_view.html; then extract the files within the downloaded zip file and run the ChromeHisotryView tool to complete the following question. **Note down the location of the history file.**

1. List the top 10 most visited URLs along with the following information: title, visited time, visit count, and Typed Count.

Task 4: Viewing Cache within Google Chrome

Download the ChromeCacheView tool from https://www.nirsoft.net/utils/chrome_cache_view.html; then extract the files within the downloaded zip file and run the ChromeCacheView tool to complete the following question.

Also, within the ChromeCacheViewNote interface, go to "File", then "Select Cache Folder" and then note down the location of the Cache file and various configurations.

1. List 10 random cached files along with the following information: URL, Content Type, File size, Last Accessed, Server Last Modified, Expire time, Server Response, Content Encoding, and Server IP Address

Task 5: Viewing Cookies within Google Chrome

Download the ChromeCookiesView tool from https://www.nirsoft.net/utils/chrome_cookies_view.html; then extract the files within the downloaded zip file and run the ChromeCookiesView tool to complete the following question.

Also, within the ChromeCacheViewNote interface, go to "Options", then "Advanced Options" and then note down the location of the cookie file and various configurations.

1. List 10 random cookie entries with the following information: Host Name, Value, Last Accessed, Created On, and Expires

Task 6: Viewing Browser Search history

Download the MyLastSearch tool from https://www.nirsoft.net/utils/my_last_search.html; then extract the files within the downloaded zip file and run the MyLastSearch tool to complete the following question.

1. List 10 Searched items with the following information: Search text, Search time, and Web Browser