Computer Science Department University of Crete

CS457.1: Digital Forensics
Assignment 1 - Windows Forensics

Deadline: 15/4 23:59

Note: The questions that have the screenshot icon (📷) require screenshots to be considered correct.

Scenario

A couple days ago, secret agents of the counterintelligence branch apprehended a foreign national named Charles Kingston at the Kazantzakis International Airport before his flight. Charles is a person of interest in a major operation launched by the Intelligence service that aims to uncover and foil foreign espionage operations in Greece. Although he didn't confess and claimed to be a tourist fascinated by Greek antiquity, the agents are pretty sure that Charles is involved in espionage in some capacity.

Among the personal things that Charles had on him at the time of his arrest was a laptop which was seized and imaged by police officers. You are a member of the digital forensics team assigned to this case and you are tasked with analyzing the laptop in order to uncover the capacity of Charles's participation in the spy ring.

Setup

For this assignment you can use either a Windows or a Linux Forensic Workstation as shown in the first tutorial of the course. You can download all the required files for the assignment from the course's page:

https://www.csd.uoc.gr/~hy457-1/assignments.html

Before moving on to the next sections, you should create a directory in the workstation. This directory will be used to store the files and, consequently, solve the case. It is important that the name of the directory, the username (on Linux) and the autopsy case name contain your own name or your university registration number. This is necessary for the screenshots that you will provide in your final report.

Assignment files

Name	Description	Size
laptop.E01,2,..8, laptop.E01.csv laptop.E01.txt	Laptop fragmented image files and helper files Used in section 1 and 3	11,4 GB
thumbdrive.img	Image file used in section 2	348,1 MB
acquisition_details.txt	File hashes, used for verification	274 bytes

1. Computer Analysis

For this exercise use the **laptop.E01** file. Load the image in autopsy and answer the questions below.

1. Before analyzing the image the first step should be to verify that the image was not altered in any way after the acquisition process. Compute the **MD5** and **SHA1** hashes 📷 and compare them with the ones from the acquisition process, you will find the hashes in the **acquisition_details.txt.**

   Hint: E01 is a compressed file format, so simply running hashing tools will yield different hashes. You will need to find hashes from the loaded image in autopsy.

2. What is the username of the Windows user?

3. Unfortunately we don't know in which hotel the suspect stayed at. Perhaps the suspect searched for available hotels in Heraklion, that might help the investigators narrow down the list of hotels they need to search. Find and report all the hotels the suspect searched for in Google maps.📷

4. Investigators believe that the suspect may have received operational security training regarding concealing electronic messages. Can you corroborate this theory by analyzing his searches? 📷

5. Did the suspect install anything on the computer? 📷

6. Perhaps the suspect might employ encryption to conceal his work. Did you find any encrypted files in his laptop?

2. FAT analysis and file recovery

Police officers managed to find a usb thumbdrive that the suspect has hidden in his hotel room prior to his arrest. Unfortunately, the initial investigator didn't find anything useful.

For this exercise use the **thumbdrive.img** file.This section is to be done by utilizing only **CLI** tools. You will need to provide a screenshot for each command that you run.

If you are on **Windows** you might need to install the following tools:
fsstat: can be found in "The Sleuth Kit" [1]
dd / dcfldd: Git for Windows [2] comes with dd or download dc3dd [3] (requires cygwin)

1. Use the fsstat tool to answer the following questions: 📷
   i. What is the type of the file system?
   ii. What is the sector size?
   iii. What is the cluster size?
   iv. What are the sector addresses of the first copy of the FAT table (FAT 0)?
   v. What are the sector addresses of the root directory?
   vi. What are the sector addresses of the data area?
   vii. What is the last sector of the file system?

2. Use the dcfldd tool to extract the first sector of the root directory:
   i. Report the command that you used.
   ii. Are there any deleted files? If so, report the byte offset of the start of the directory entry. 📷
   iii. What is the size of the file?
   iv. How many clusters does it take to store the content of the file?

Hint: Use Table 1 to answer the above questions.
You can assume **little-endianess** and ignore the entries for the long name [4]

Table 1: Data structure for a FAT32 directory entry

Byte offset in hex (within directory entry)	Length in bytes	Byte range (decimal)	Content
0x0	1	0-0	First Character of the file name in ASCII and allocation status (0xe5 or 0x00 = unallocated, 0x2e = not a normal file)
0x1	10	1-10	Characters 2-11 of file name in ASCII
0xb	1	11-11	File attributes
0xc	1	12-12	Reserved
0xd	1	13-13	Creation time
0xe	2	14-15	Creation time (hours, minutes, secs)
0x10	2	16-17	Creation date
0x12	2	18-19	Accessed date
0x14	2	20-21	High 2 bytes of first cluster address
0x16	2	22-23	Modified time (hours, minutes, secs)
0x18	2	24-25	Modified date
0x1a	2	26-27	Low 2 bytes of first cluster address
0x1c	4	28-31	Size of file (0 for directories)

3. Make the appropriate changes in the directory entry of the deleted file, so the file is not marked as deleted.📷

4. Use the dcfldd tool to extract the first copy of the FAT table. How long should the cluster chain be? Make the appropriate changes📷. You can read more about the cluster chains here [5].

5. Use dcfldd to put back the original image and the modified root directory in order to create a new image. Report the commands that you used.

6. Mount the image and check if the file has been recovered. Compute its **sha256** value. Is there anything interesting particular to the case in this file📷?

7. (**Anti-forensics**) How would you securely erase a storage device in order to minimize the chance of file recovery using the above method?

   This is a critical thinking question unrelated to the case. Explain in detail why your proposed method will work and link any references that support your hypothesis when you answer this question.

3. Image analysis

For this exercise use the **laptop.E01** file.

1. Use the password that you found in step 2.6 in order to decrypt the archive.

2. Can you find when *vacation.jpg* was taken?

3. Can you find where *vacation.jpg* was taken? Find the location on a map 📷(e.g. Google maps) and include it in your report.

4. Is there anything interesting in the other picture? 📷

Submission

- Create a single **PDF** document containing all your answers along with the required screenshots. The screenshots should include as much information from your workstation as possible to differentiate them from the ones submitted by other students. When answering questions try to elaborate and explain how you reached the respective conclusion.

- Submissions will be done through **elearn**, you will be notified when they open.

- This assignment is an individual creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.

- You are encouraged to post any questions you may have in the elearn forum.. If however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at *hy457-1@csd.uoc.gr.*

References

[1] The Sleuth Kit Download: https://sleuthkit.org/sleuthkit/download.php

[2] Git for Windows Download: https://gitforwindows.org/

[3] dc3dd sourceforge download :https://sourceforge.net/projects/dc3dd/files/dc3dd/7.2.646/

[4] Long file entries: *https://www.codeguru.com/cplusplus/long-file-name-lfn-entries-in-the-fat-root-directory-of-floppy-disks/*

[5] FAT Cluster Chains: *https://en.wikipedia.org/wiki/Design_of_the_FAT_file_system#Cluster_map*