German International University
Faculty of Informatics and Computer Science
Digital Forensics
Dr. Marwa Zamzam
Eng. Salma Abubakr

Digital Forensics Assignment 1

Question 1:

The objective of this exercise is to examine the Master Boot Record (MBR)

Before you start: Prepare the working environment.

1. Find the disk file 'diskimage.vhd'.
   https://drive.google.com/file/d/1ibKh8xnf6PD45VSqGv_lu68LUygVuA6t/view?usp=sharing
2. Download and install Active@Disk Editor.
3. Open the editor and choose 'Open disk image' then press 'customize'.
4. Edit the 'Image type' to be 'Virtual machine (VMWare) disk image'.
5. Press 'Add' and select the path of the 'diskimage.vhd'.

Hint: What is that vhd file?
A VHD (Virtual Hard Disk) file is a file format used to represent a virtual hard disk drive (HDD) in a virtualized environment. It is a file that **emulates the physical hard disk drive** and contains all the dataand information required to create a virtual machine (VM) on a host

The partition table is in the Master Boot Record (MBR), located in sector 0 of the disk drive. You can find the first partition starting at offset 0x1BE. The second partition starts at 0x1CE and so on.
The file system's hexadecimal code is offset 3 bytes from 0x1BE for the first partition.

- The sector address of where this partition starts on the drive is offset 8 bytes from 0x1BE.
- The number of sectors assigned to the partition are offset 12 bytes for position 0x1BE.
- These offsets are duplicated for any additional partitions created on the disk

Reference the information provided above and locate the MBR and answer the following questions:

a) How many partitions did you find in the MBR? Justify your answer
b) Fill the following table, where Start: show the starting sector of the partition, End: show the ending sector of the partition (hint: to be calculated), Sectors: the total number of sectors in the partition.

Partition	File system Type	Start	End	Sectors

Question 2:

The objective of this exercise is to examine the NTFS

Before you start: Prepare the working environment.

1. Find the disk file 'Emily removable disk'. https://drive.google.com/file/d/1085hSZe_3l87EF9yWxqGt41UHdOqmVrf/view?usp=sharing
2. Open FTK Imager/ Autopsy/ Active@Disk Editor.
3. Mount hard disk image and start working.

As a forensic examiner, you received a storage image file with its SHA256 hash code.

81F6900532E192C941D3DAB1FCD6ED4730F6151CDDA319CD9EA3DCB3D22D463C

a) Forensically speaking, what should be done before attempting to investigate the storage image file?

b) Is this file considered intact? Justify your answer.

c) Load the image file, analyze the output of the extraction and answer the following questionsmentioning the bytes that represent the answer.
Hint: Example of the answer: 20/11/2010 – 6:10:00 am
The bytes: 47 AF EE 00 58 66 23 AB

i) When was this disk image created?
ii) What is the last modification date?
iii) What is the size of MFT?
iv) How many attributes are there in MFT? What is the size of each attribute? Explain your work with screenshots.

d) Are there pictures in this image file? If yes, when did they create? What are their last modification dates? Are they resident files or not? And why? Extract these images.

Instructions:

1. Teams can have 3 students at most.
2. You are asked to write a report answering all questions and upload it on:https://forms.gle/HpzBqaSbCeWRUzQE9
3. Deadline will be on Friday 17/11/2024 at 11:59 pm.