

# File system analysis on NTFS

## Introduction

In this practical you will perform analysis on NTFS by using the HxD hex editor and AccessData Imager.

By the end of this lab you will be able to

- Perform basic file system analysis on forensic images within a hex editor and AccessData Imager

## Task 1: Analysis NTFS system

This is an individual exercise. Download the NTFS practical image (<https://drive.google.com/file/d/1JK3i52Xp74veUfqZaUKSin0ECS2fGI5t/>) within FORFUN week 2 section from moodle, explore the image in the evidence tree pane within AccessData Imager and answer the following questions:

1. How many bytes per sector for the image?  
512 bytes
2. How many sectors in total on the image?  
245,760
3. What is the type of the image?  
raw
4. How many partitions does the image have?  
1
5. What is the starting sector number of the NTFS partition?  
32
6. Within the NTFS partition, regarding the MFT file
  - a. What is its size?  
262,144 bytes
  - b. What is its start cluster  
81909
7. Within the NTFS partition, regarding the MFTMirr file
  - a. What is its size?  
4096 bytes
  - b. What is its start cluster  
16
  - c. What is the MFT record number for the MFTMirr file?  
1

- d. How many records does the MFTMirr contain?  
4
8. What is the volume serial number of the NTFS partition?  
64-bit:86 E8 B5 92 E8 B5 80 CB  
  
32-bit:E8 B5 80 CB
9. The file within the MFT record number of 44, is it a resident file or not?  
yes
10. Now, download a picture from the Internet, save it onto the desktop, open to check if it displays properly and close it (assuming you use Windows). Note down the MAC times for this file (hint right click on the file, go to the properties and focus on the General tab).
11. Wait for 1 minute, open the downloaded image file to check again if it displays properly and close it. Note down the MAC times for the file
12. Compare the answers from the previous two steps.  
For most of the cases the MAC times are the same.

### **Further work**

Can you find a deleted file, along with its metadata information from the NTFS practical image?