# NTFS Bit by Byte worksheet

## Your turn 1 - NTFS Boot Sector

Bytes per sector: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

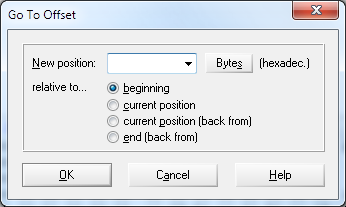
Sectors per cluster: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hidden sectors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Total Sectors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ size of volume in: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_bytes, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_GiB

$MFT start cluster: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ $MFTMirr start cluster: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Your turn 2 - Find the $MFT on PFIC\_01

Bytes per sector: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sectors per cluster: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

$MFT start cluster: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

$MFT byte offset: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

in hex: 0x\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

confirm this by jumping to this location in winhex. Hold down <alt>+g and enter the desired offset, make sure you enter the value in hex.

If you have time, jump to the end of the volume, can you see the backup boot sector?

## Your turn 3a - Decode the first record header for the $MFT on PFIC\_01

This is the first entry in the $MFT.

Offset to 1st attribute: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Flags: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is this a directory? yes no

Used size of this MFT record: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Next attribute ID? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MFT record number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ What is the name of the file? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Your turn 3b - Decode the first attribute for the $MFT on PFIC\_01

Attribute type: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Length: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Resident or non resident? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Content length: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Content offset: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Created: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Modified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Flags: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Type of next attribute: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Your turn 4 - Find small\_file.txt

## Your turn 5 - Find big\_file.txt

Decode a directory entry

Find a file in a directory

Identify the deleted file

Identify the compressed file & directory

Identify the resident text file and resident data in non resident text file.