COMP 3731: Computer Forensics
Department of Computer Science
University of Denver

ASSIGNMENT 3

This purpose of this assignment is to familiarize you with the basic structure of the NTFS file system.

Description

In this assignment, you will write a C/C++ program called *DiskPreview* that outputs some basic information about the files contained within a **NTFS partition disk image**. The disk image file name is provided as command line argument (`argv[0]`).

DiskPreview will read the provided disk image, parse through the MFT Zone (recall that each MFT record occupies 1024 bytes) and print out the following information about all file-related entries it encounters.

The output information is displayed using the following format (all numbers are in decimal).

```
NAME:
      CN :: FBCN(+OFF) [:: NDS] [:: Data Runs]
```

where,

`NAME`	= name of the file
`CN`	= cluster no. where MFT record for the file is located
`FBCN`	= cluster no. where contents of the file begins
`OFF`	= offset within cluster `FBCN` to the first byte of the file
`NDS`	= number of alternate data streams found in the file, if any
`Data Runs`	= data runs, if any, of the file formatted as `(LCN,count); (LCN,count); …`

Important Note: You should display this information ***only*** if the MFT record has both a file name attribute (0x30) and one or more data attributes (0x80). If either of them is not present, then you can ignore that record. `[ ]` implies that the information (NDS and/or Data Runs) is only printed if they exist.

Example:

```
afile.txt:
      374465 :: 374465(+288) :: 2
```

This means – there is a MFT record in cluster 374465 that has information about the file `afile.txt`. The data for this file begins from byte 288 onwards in cluster no. 374465. *This is a resident file since non-resident data typically begins from offset zero within a cluster!* Also, this file has two other data streams. Since, it's a resident file (FBCN is same as CN), there are no data runs.

```
bfile.txt:
      374467 :: 12539803(+0) :: (12539803,150); (12547933,200)
```

This means – there is a MFT record in cluster 374467 that has information about the file `bfile.txt`. The data for this file begins in cluster no. 12539803. This is a non-resident file since FBCN is different from CN. The file occupies 150 clusters starting from cluster 12539803, and then occupies 200 clusters starting from cluster 12547933. The file has no alternate data streams.

Approach

You should first go over the slides in Lecture 5 to refresh how a MFT record is structured. Some of the concepts that will be needed are:

- how to find the beginning of the MFT?

- how is the MFT header structured?
- how are attributes 0x30 and 0x80 structured?
- how to interpret data runs?

The program should analyze the partition boot sector to determine the start address of the MFT (*bytes per sector* x *sectors per cluster* x *logical cluster number of MFT*). The MFT Zone is 12.5% of the total disk space; so you can compute how many clusters you should parse for a given disk size (*0.125* x *disk size in bytes* / *cluster size in bytes*) to get through the entire zone.

Images

Two NTFS partition image files (`USB1.dd` and `USB2.dd`) are provided in the assignment page. `USB1.dd` file has one non-resident file (testfile.txt) and one resident file (usb.txt). The tree structure on the `USB2.dd` image, as seen in Windows Explorer, is also given. Both disks are about 502 MB in size.

Submission

Upload the *DiskPreview.cpp* (or *.c*) file to Canvas.

Grading

The assignment is worth **100 points:**

determination of MFT zone start: 10 pts.
extraction of all files: 20 pts.
extraction of correct filenames: 20 pts.
extraction of correct file data: 50 pts.

You should always write well-commented code. A program that does not compile is a program that you did not submit at all. Remember the GTA is not required to debug your program to give you partial points.

The late policy is available in the course syllabus. **You must work alone on this assignment.**

USB2.dd as seen in Windows Explorer

```
|------- Music
|       |-------- Kalimba.mp3 (8218 KB)
|       |-------- Maid with the Flazen Hair.mp3 (4018 KB)
|
|------- Slides
|       |-------- Lecture 1.pptx (752 KB)
|       |-------- Lecture 2.pptx (134 KB)
|       |-------- Lecture 3.pptx (162 KB)
|
|-------- Empty.txt (0 KB)
|-------- fractal.gif (217 KB)
|-------- MD5.txt (1 KB)
|-------- NTFS.txt (4 KB)
```