

**Assignment Coversheet**

|  |  |
| --- | --- |
| Unit Code | **9074** |
| Unit Name | **Introduction to Digital Forensics** |
| Group Number | **120** |

**I/We declare that this assignment is solely our work, except where due acknowledgements are made. I/We acknowledge that the assessor of this assignment may provide a copy of this assignment to another member of the University, and/or to a plagiarism checking service whilst assessing this assignment. I/We have read and understood the University Policies in respect of Student Academic Honesty.**

|  |
| --- |
| **STUDENT ID** |
| u3284513 |

# CREATING THE VIRTUAL HARD DISK

To create a virtual hard disk, begin by opening the Disk Management program on Windows. Navigate to the Action dropdown menu and select the Create VHD option. The menu will then prompt the user to specify the output path for the VHD file, the size and if we want the disk size to remain constant. For this task, the file path will be in “C:\Users\student\Documents”, 40MB in size and will be of fixed size **(Figure 1)**. To use the VHD, a primary partition must be made. To achieve this, open the Command Line with Administrator privileges and type “Disk Part” to open the disk part tool. Typing “list disk” will allow the user to see active disk and will show us the newly created VHD listed as Disk 2. Type “select disk 2” to select the disk and “create part pri size=36” to create a 4MB primary partition on the disk. **(Figure 2)**

Go back to Disk Management. In the Volume window, there should be a new Disk labelled Disk 2 partition 1 which is the newly created hard disk. Right click on this disk, click on Format and a pop-up box will allow the user to specify the details for the disk. For this task, the volume name will be “U3284513FAT”, choosing the FAT file system and assign it the letter X **(Figure 3)**. For the NTFS drive, repeat the above steps, changing the disk size to 50MB, make the primary partition size be 46MB and format it with the volume name “U3284513NTFS” with NTFS file system and assign it the letter Y. After performing these steps, both FAT and NTFS disk should be ready to use **(Figure 4)**.

# FILLING THE DISKS

For the next task, open the “IDF home” folder on the Desktop which contain several text files of various size. To achieve fragmentation of both disks, meaning forcing the system to store the file in non-continuous data block, start by copying some small files over to the disk. Proceed to delete these files and copy over a large file with its size being larger than the size of all deleted files. To help with the process, open DiskView to see the changes in the disk. Repeat a few more time and refreshing DiskView after each cycle. The result should be visible in DIskView, with the disk showing white spaces in between the blue data blocks and a segmented file coloured in red **(Figure 5)**. After this result is achieved in either disk, begin the process again in the other disk.

# IDENTIFYING RESIDENT AND NON-RESIDENT FILE ON NTFS DISK

A resident file is one whose data fits entirely within its MFT entry, while a non-resident file stores its data outside the MFT (NTFS, 2025). Both types use a $DATA attribute, which begins with the hex string 80 00 00 00. Within this attribute, the Nonresident flag—found at the 17th byte—indicates the type: 00 for resident and 01 for non-resident.

To inspect this, open the virtual disk in WinHex. Right-click a file, go to Navigation > Seek FILE record, and locate the $DATA header. If the file is non-resident and fragmented, it will contain a data run, which lists the starting cluster and length of each file fragment. Fragmented files will have multiple data runs, showing where the remaining parts are stored on disk **(Figure 6)**. Else if the file is resident, the file content can be seen in its MFT entry **(Figure 7)**.

# HIDING THE SECRET KEY

For this step, the secret string “IDF2025\_CTF” will be used. In the FAT file system, navigate through the file system until a slack space is visible. A slack space is the unused space within the cluster it occupies but is not big enough to fill the entire cluster. Using a hex editor, in this report Hex Workshop will be used, insert the secret string into the space and verify the changes with the help of WinHex **(Figure 8)**. Next, navigate to a cluster of a file that has been deleted, that is moved to the recycling bin. Since the file has been marked as “deleted” by the system but has not been removed from the storage, it still occupies that cluster for recovery purposes. Once such cluster has been found, insert the secret string and verify the changes **(Figure 9)**.

References:

1. NTFS 2025, NTFS File Types - NTFS.com, Ntfs.com, available at: <https://ntfs.com/ntfs-files-types.htm>

APPENDICES:

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: Creating the VHD

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2: Making a partition

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3: Formatting the FAT drive

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4: FAT and NTFS disk ready to use

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5: Both disks showing sign of fragmentation

A close up of a grid

AI-generated content may be incorrect.

Figure 6: Hex dump of a non-resident file with the $DATA attribute and flag highlighted. In this case, it is the 01-flag signifying a non-resident file

A close up of a grid

AI-generated content may be incorrect.

Figure 7: Hex dump of a resident file with the 00-flag. in this case, the entire file content is visible in the MFT

A close up of a grid

AI-generated content may be incorrect.

Figure 8: Secret string inserted in slack space

A screen shot of a computer

AI-generated content may be incorrect.

Figure 9: Secret string inserted in the cluster of a deleted file. The right panel show the file path in the Recycling Bin, signifying that the file has been deleted