1. DELETED FILES

One important aspect when collecting digital evidence are files which have been deleted. It is better to destroy evidence than hiding them. As such for digital data, deleting the data is a way of destroying the data. Therefore during computer forensic analysis, it is important to recover the deleted files since they can become a crucial piece of evidence.

When a file is created in an operating system, the file is saved in a file system. The file allocation table keeps track of the file created in the file system. Examples of a file allocation table include the FAT, FAT32 and MFT (master file table). The file allocation table allows the operating system to know where the files are located. When a file is deleted, an entry for that file is removed from the file allocation table. Hence the operating system assumes that the file does not exist. However, even if an entry is removed from the file allocation table, the file may still be physically present on the hard disk. Depending on how a file has been deleted, there is still a chance to recover that file.

Before understanding how to recover deleted files, we will go through different ways of deleting a file. One of the most common ways of deleting a file is via the Delete button found on the keyboard. However there are other ways of deleting a file.

1.1 Command Prompt

In Windows, a file can be deleted by using the command **DEL** or erase in command prompt. Below is an example of the DEL command.

A folder contains two files as shown in Figure 3.1

```
C:\Users\Avi\Desktop\Sample>dir
 Volume in drive C is OS
 Volume Serial Number is F896-E8AD

 Directory of C:\Users\Avi\Desktop\Sample

09/04/2018  13:36    <DIR>          .
09/04/2018  13:36    <DIR>          ..
09/04/2018  13:36                39 hacker.txt
09/04/2018  13:36                58 test.txt
               2 File(s)             97 bytes
               2 Dir(s)  446,549,147,648 bytes free
```

Figure 3.1

Figure 3.2 shows how to delete the file test.txt using **DEL** command.

```
C:\Users\Avi\Desktop\Sample>DEL test.txt

C:\Users\Avi\Desktop\Sample>dir
 Volume in drive C is OS
 Volume Serial Number is F896-E8AD

 Directory of C:\Users\Avi\Desktop\Sample

09/04/2018  13:37    <DIR>          .
09/04/2018  13:37    <DIR>          ..
09/04/2018  13:36                39 hacker.txt
               1 File(s)             39 bytes
               2 Dir(s)  446,549,147,648 bytes free
```

Figure 3.2

Figure 3.3 shows how to delete a file, hacker.txt, using *erase* command in command prompt.

```
C:\Users\Avi\Desktop\Sample>erase hacker.txt

C:\Users\Avi\Desktop\Sample>dir
 Volume in drive C is OS
 Volume Serial Number is F896-E8AD

 Directory of C:\Users\Avi\Desktop\Sample

09/04/2018  13:46    <DIR>          .
09/04/2018  13:46    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  446,546,448,384 bytes free
```

Figure 3.3

The **DEL** and erase commands are also used to delete folders, directories and partitions. As stated earlier, the DEL and erase commands remove the file from the file allocation table but the file will still be present on the hard disk which can be recovered using forensic tools.

1.2. Disk Cleanup

Disk Cleanup is a computer system utility software designed to delete files in order to free up disk space on the hard disk. Disk Cleanup searches and analyses files which are rarely or no longer used and, then removes them. Disk Cleanup will look for the following files for deletion:

- Temporary Internet files
- Temporary Windows/System files
- Recycle Bin
- Old Compression files
- Setup log files
- Offline caches
- Downloaded programs
- Unused installed software

Disk Cleanup utility can be accessed in Windows 10 as follows:

Control Panel\All Control Panel Items\Administrative Tools

To Launch Disk Cleanup, click on the icon **Disk Cleanup** and the screen in Figure 3.4 is shown:

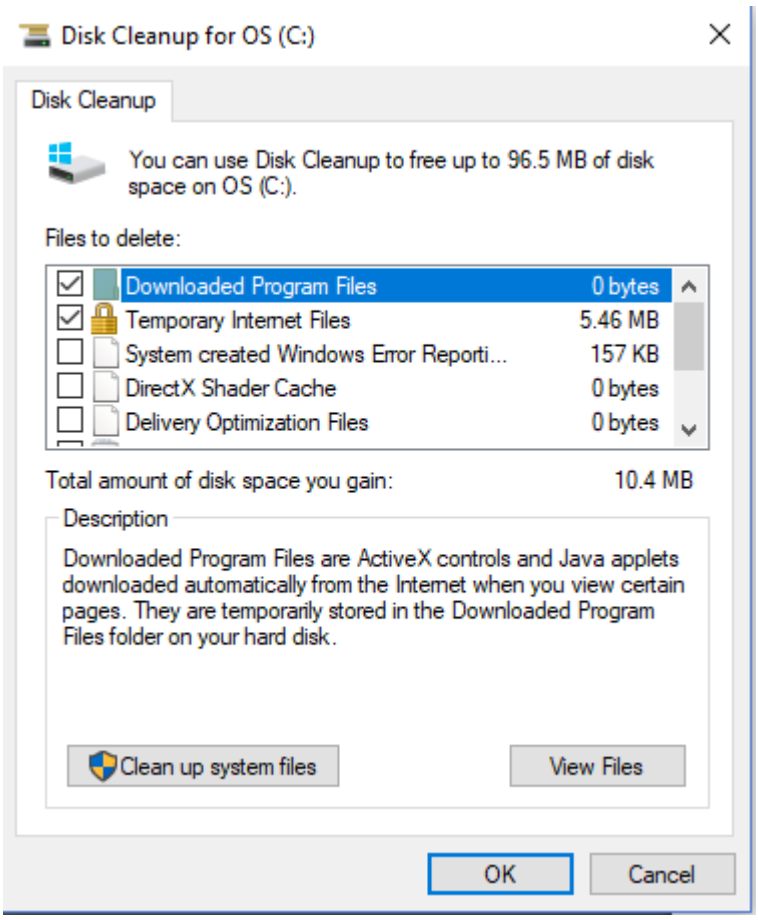


Figure 3.4

Then select the categories of files which you want to be removed and click **OK**. Once again the file will be removed from the file allocation table.

1.3 Keyboard Delete and Right-Click Delete

Most users delete a file by pressing the "**Delete**" button. The file will be removed and sent to the Recycle Bin.

Then the Recycle Bin can be emptied by Right-Clicking on the "**Recycle Bin"** Icon and then select the "**Empty Recycle Bin**" as shown in the Figure 3.5. The process of empting a Recycle Bin, will remove the file found in the Recycle Bin from the file allocation table. The file can still be restored through the use of computer forensic tools.

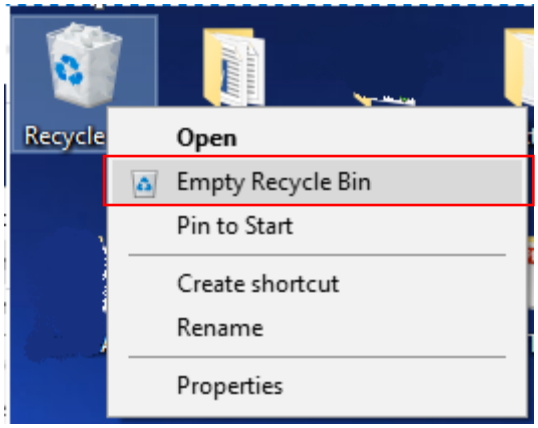


Figure 3.5

1.4 Right-Click on the file and “Delete

The other common way of deleting a file is to Right-Click on the file and then select “**Delete**” as shown in Figure 3.6. Like the keyboard delete, the file will be sent to the Recycle Bin.

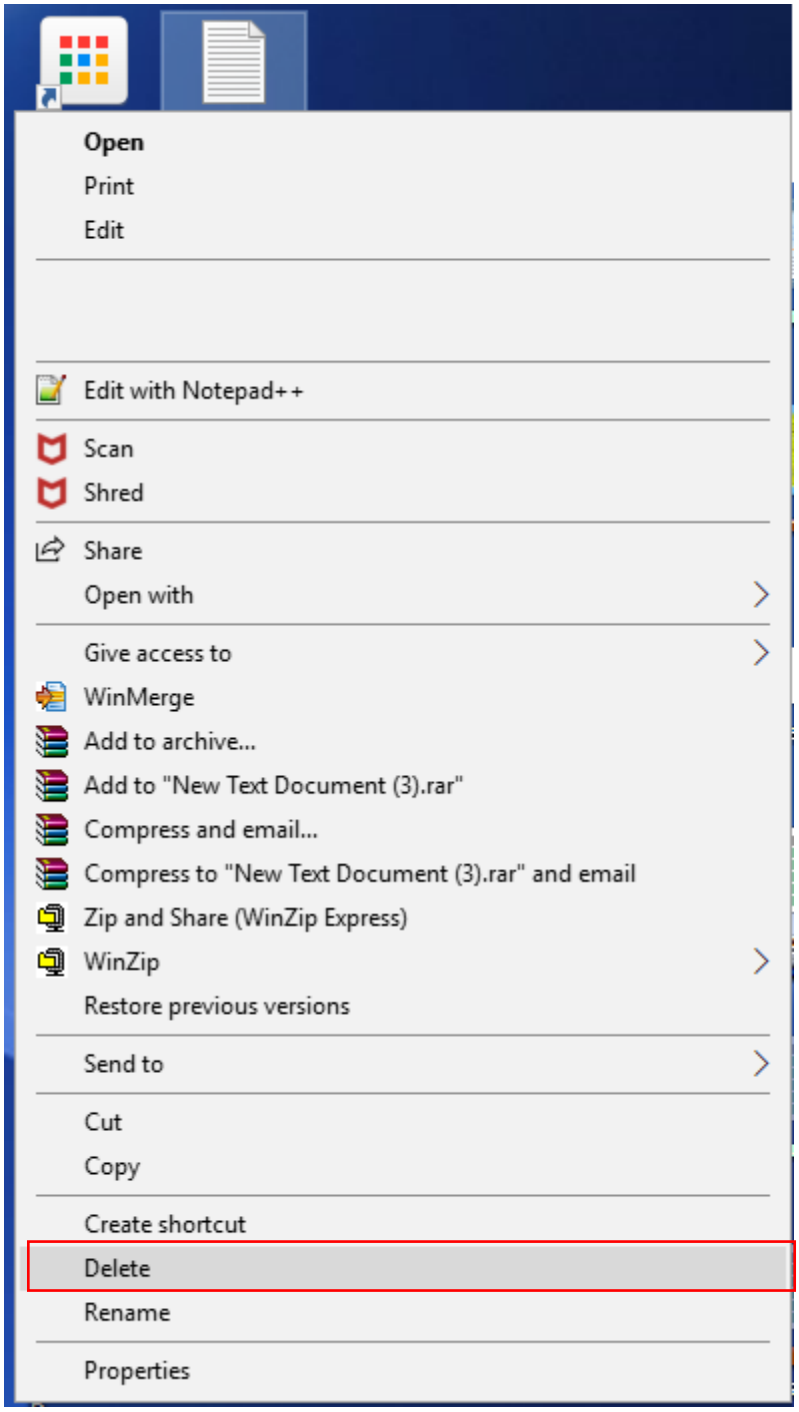


Figure 3.6

1.5 "Shift+Delete"

Another popular keyboard command which users perform is the "Shift+Delete". The following message is shown when the "Shift+Delete" is performed on a file:

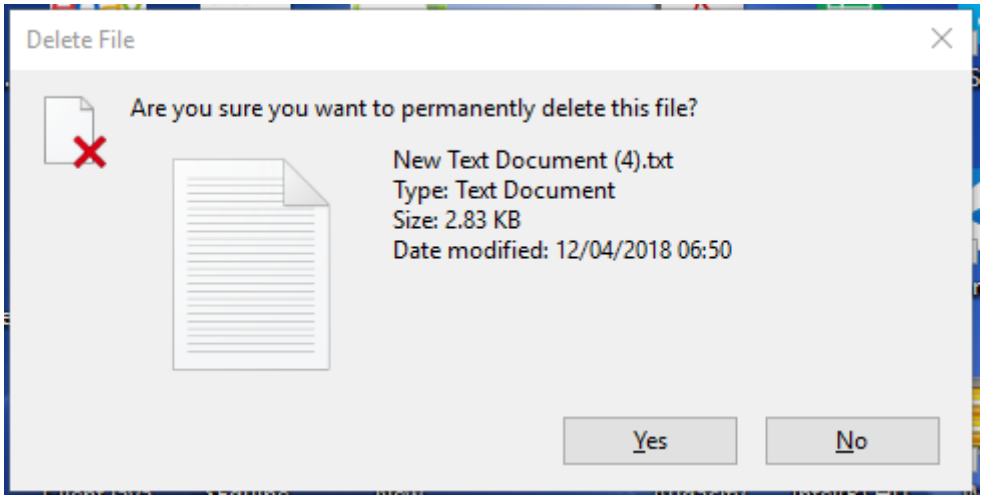


Figure 3.7

If the user clicks on "YES", the file will bypass the Recycle Bin and will be removed from the file allocation table. The file is not permanently deleted (as suggested by the Figure 3.7) until the file is overwritten on the disk space. However the file will still be available on the hard disk and can be restored using computer forensic tools.

2. REMOVING DIGITAL INFORMATION

We have seen different ways of deleting data. Deleting data does not remove the data from the hard disk permanently. It only removes the data from the file allocation table but the data still reside on the hard disk. Using computer forensic tools, those data can be recovered or restored. Even formatting the hard disk will not erase the data permanently considering the amount of computer forensics tools available to recover the data.

So how do we permanently erase the digital data without being able to recover the data? There are two ways to remove the data permanently.

- The first way is to use Erasing software which will delete the files from the file allocation table and overwrite the file location on the disk with a series on zeros and ones. By overwriting the data on the disk, the data will not be restored even using computer forensic tools.
- The second way is to use a degausser. The degausser is a magnet which wipes out all data stored on a magnetic storage device such as the flash drives and storage tapes. The data will permanently be lost.

3. COMPUTER FORENSICS TOOLS

This section introduces a series of tools which can be used to restore a file and is used during the process of acquiring evidence.

3.1 Deleted Digital Data Restoration Tools

Restoration Tools are used to recover data that have been accidentally or intentionally deleted or corrupted. Depending on the software used, different features are available to perform the recovery of the data. However recovery of the data can only be performed if the file has not been overwritten on the disk space.

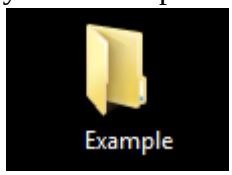
3.1.1 Data Recovery Pro

Data Recovery Pro software (Data Recovery Pro, 2018) is a free evaluation software which can be used to recover deleted files. To use the Advance features, the users need to make a purchase. For example, to recover a file, the user needs to register for this feature. The software provides the following features:

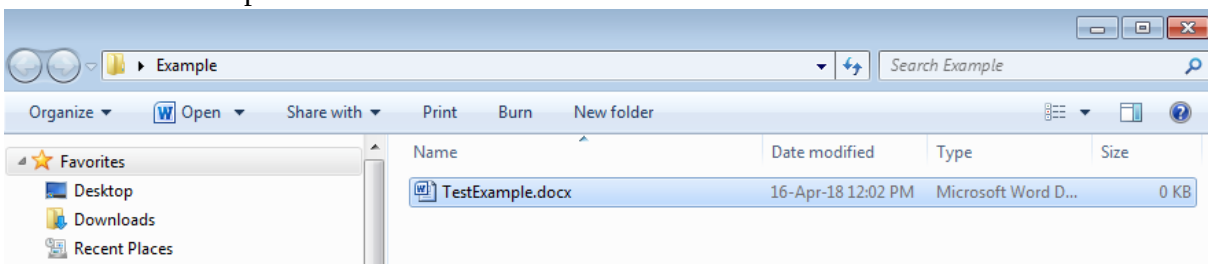
- Restoration of deleted email and deleted email attachments
- Recovery of files from a recently formatted or partitioned disk
- Restoration of a large variety of file types (Binary files or compressed files)
- Restoration of files from peripheral storage devices (such as USB)
- Recovery of Windows system files.

Below are screen shots of searching and recovering a deleted file.

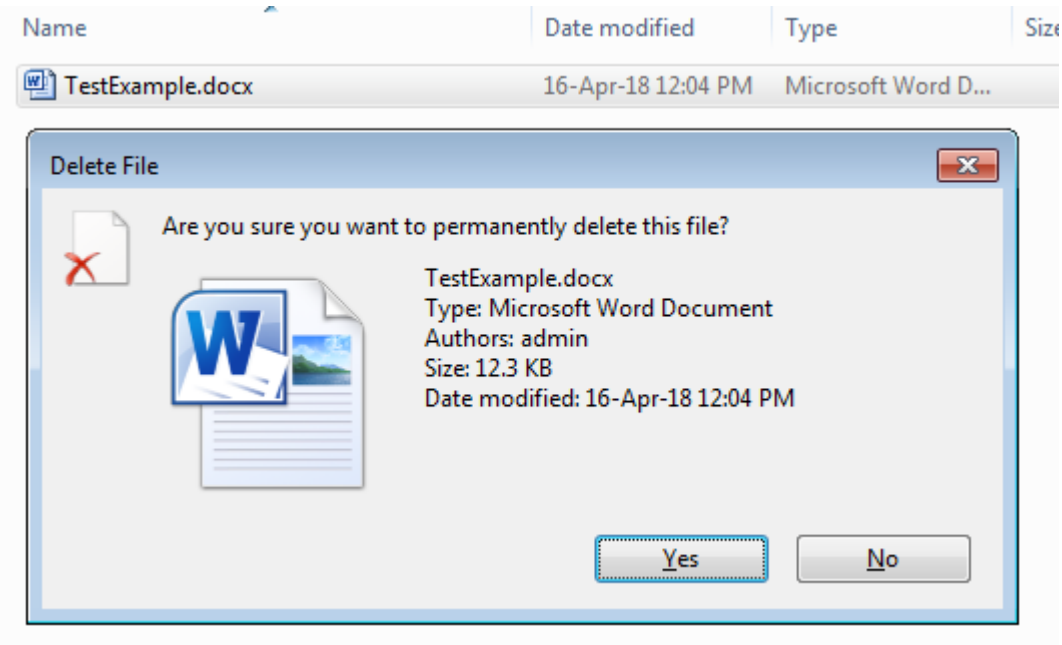
1. Download and install the software from http://www.datarecoverydownload.com/download/
2. As an example, create a folder on your Desktop and rename it as “Example”.



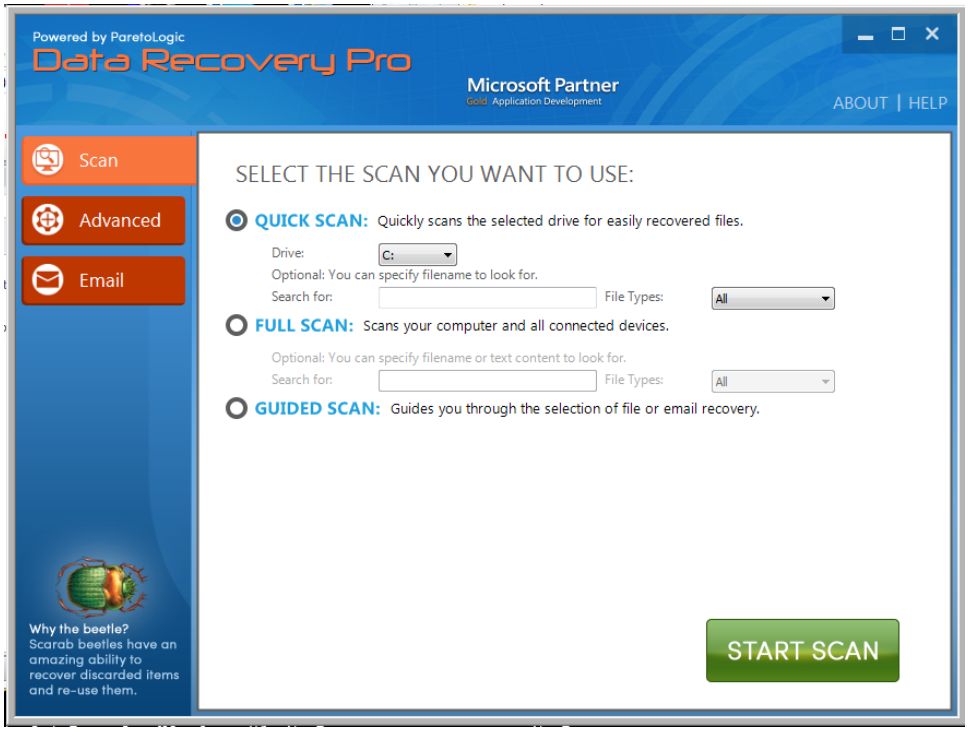
3. In the folder “Example”, create a Word Document file and name it as “TestExample.doc”.



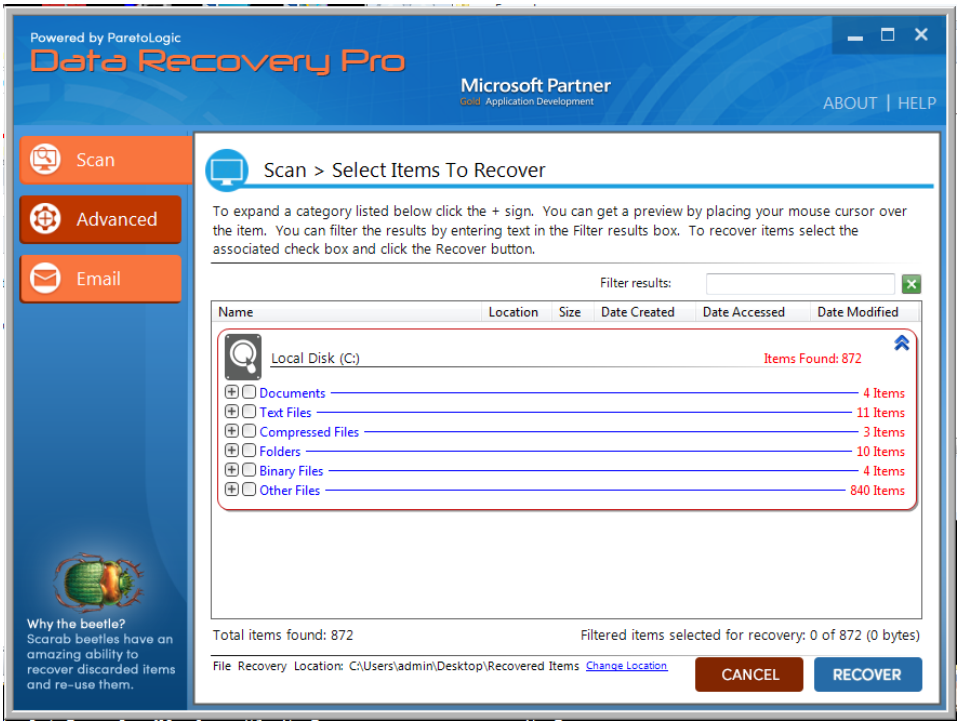
4. On the TestExample.doc, click on the file and press “Shift+Delete”



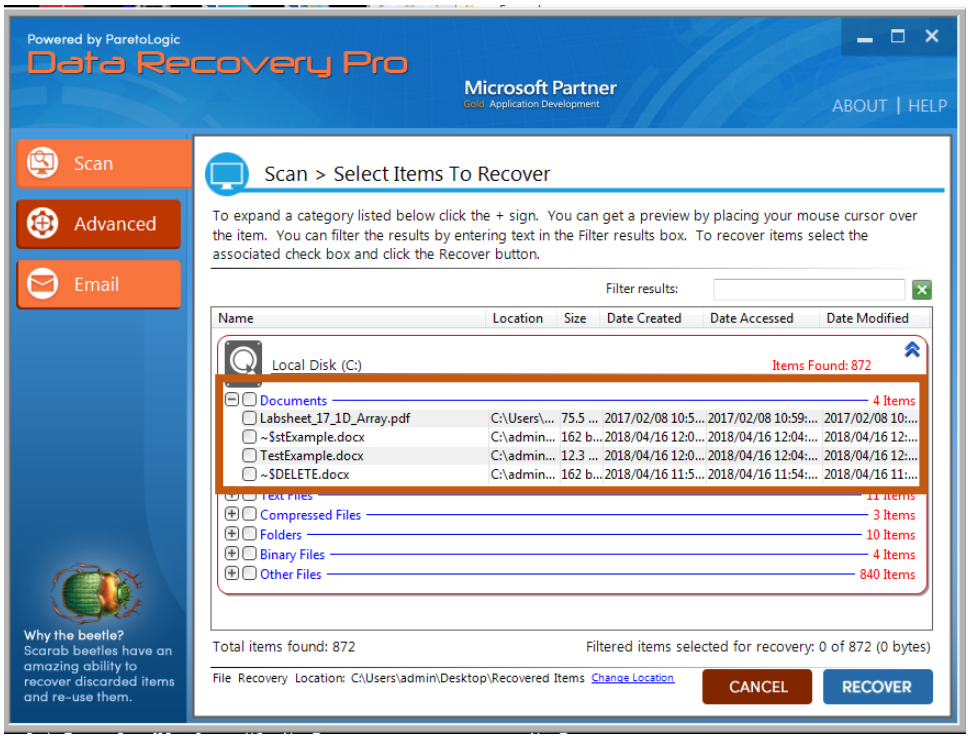
5. Press “Yes”. The file will not be sent to the Recycle Bin, and the folder Example will be empty. At this moment, we may think that we have “permanently” lost the file. However, at this stage we can still restore the file using the tool Data Recovery Pro. As mentioned, the file has an entry removed from the file allocation table and is still on the disk space unless the file is overwritten. To recover the file, run the program Data Recovery Pro.



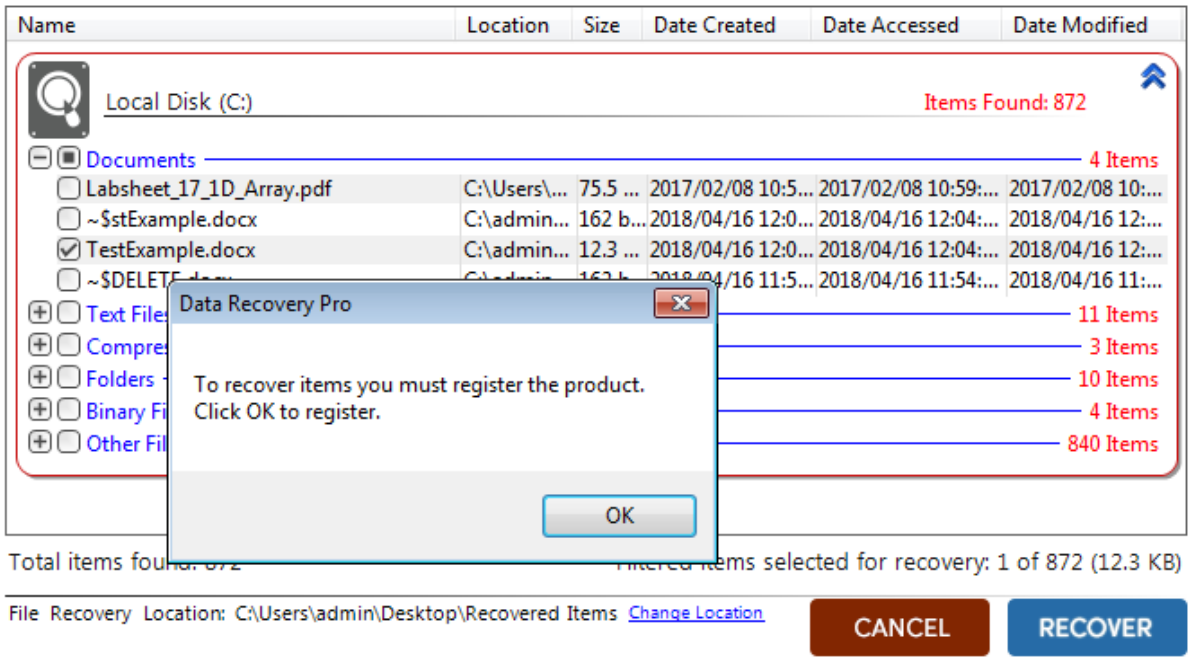
6. Press “Start Scan”. After the software has scanned the disks, the following screen will be presented:



7. Expand the "Documents" and the TestExample.docx will be available.



8. Click on TestExample.docx and press the button "Recover". Since we are using a free version, this feature will not be available until we register the product. But we have illustrated how tools can recover deleted files.



3.1.2 Recuva

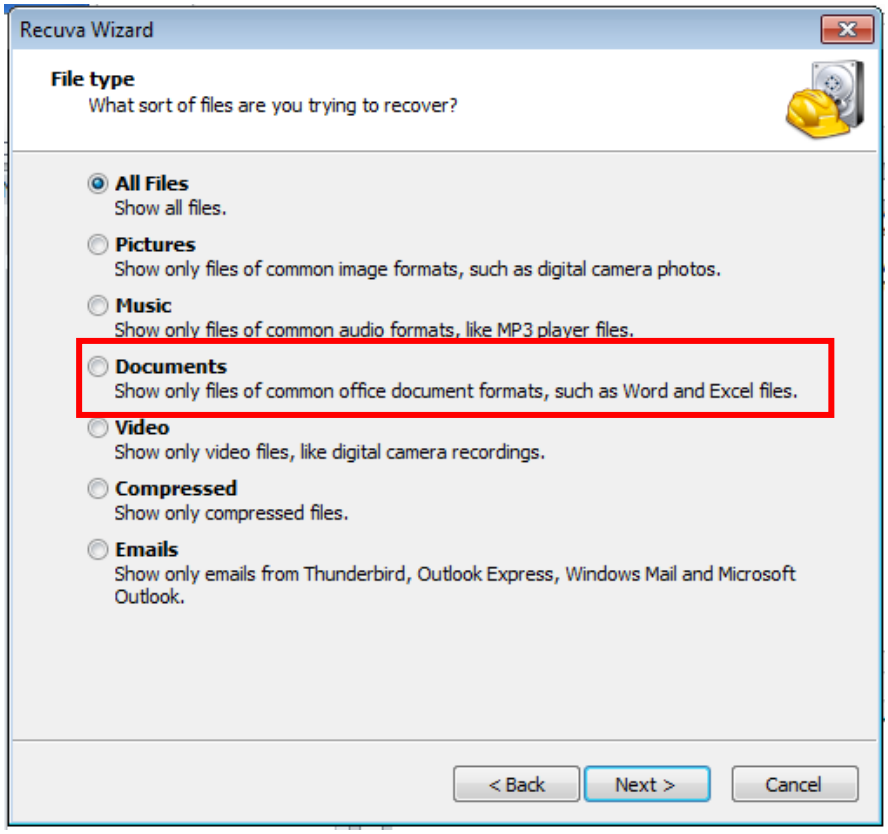
Recuva (CCleaner, 2018) is a freeware for Windows which allows the restoration of files which have been deleted from the computer. Files which have been deleted from the Recycle Bin, Memory cards and external drives can be recovered. Recuva allows users to destroy files such that they are not recovered by other software restoration tools (it overwrites the disk space where the file is located.) Below are the features which Recuva offers:

- Graphical User Interface to scan the disk to select files to be recovered.
- The software can be run on a flash drive.
- Recover all types of files.
- Supports different file allocation table systems such as FAT16, FAT32, NTFS, NTFS5.
- Recover files from removable memory cards.

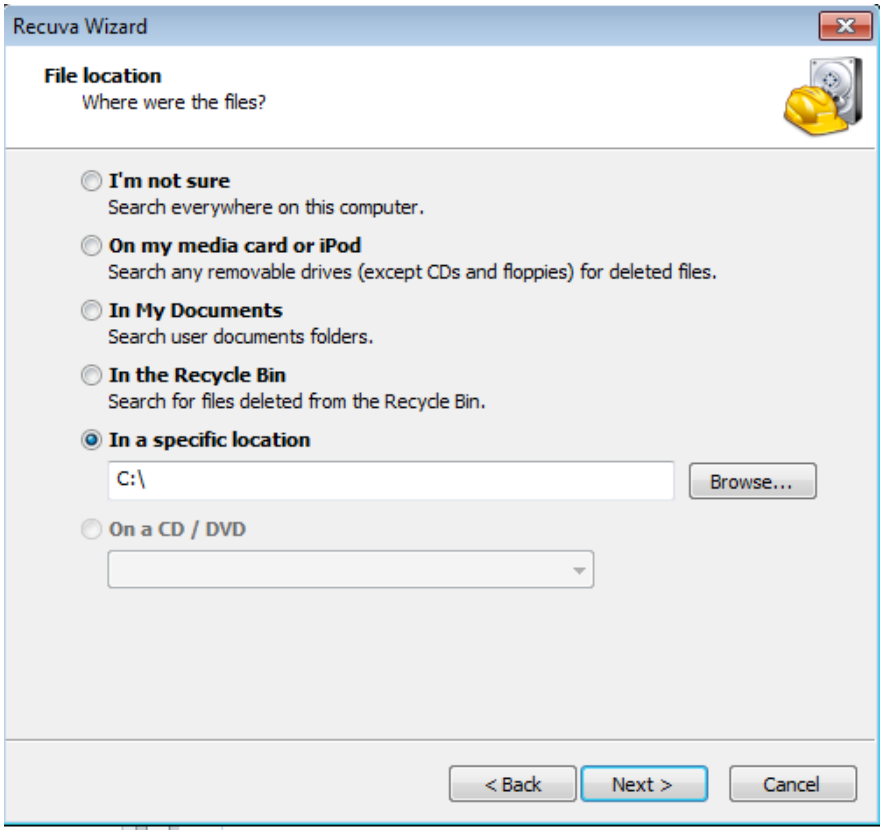
Let's now see how Recuva works:

1. Download and Install Recuva from https://www.ccleaner.com/recuva. Select the Free Version.
2. Following from the previous example (of the deleted file TestExample.docx), we would like to recover the later file after the "Shift+Delete" has been pressed.
3. Run Recuva and Press "Next".

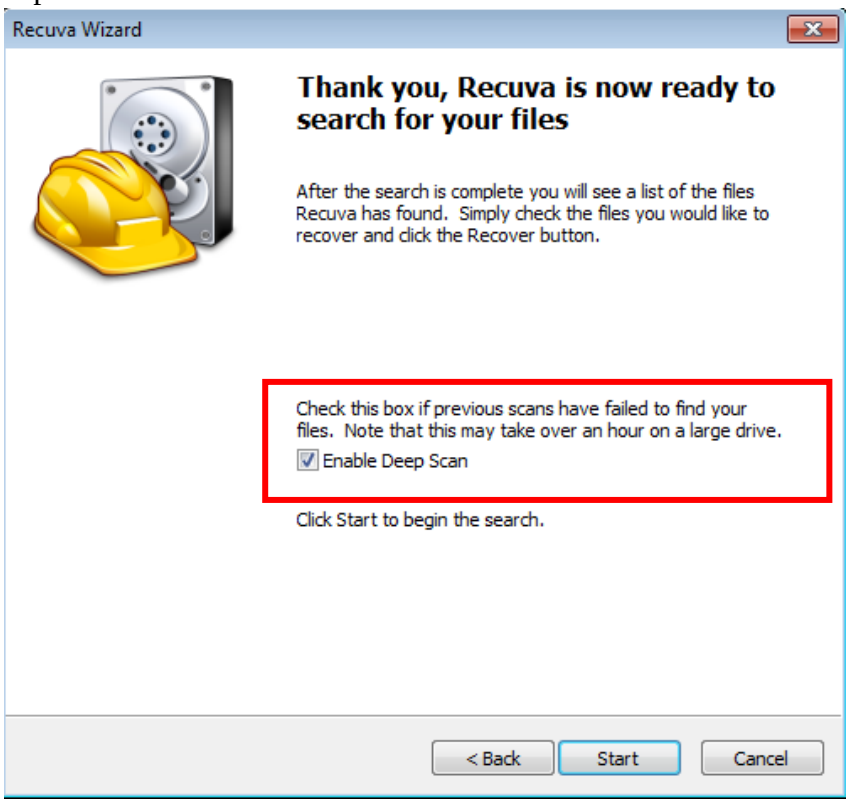
4. Select “Document” and Press “Next”.



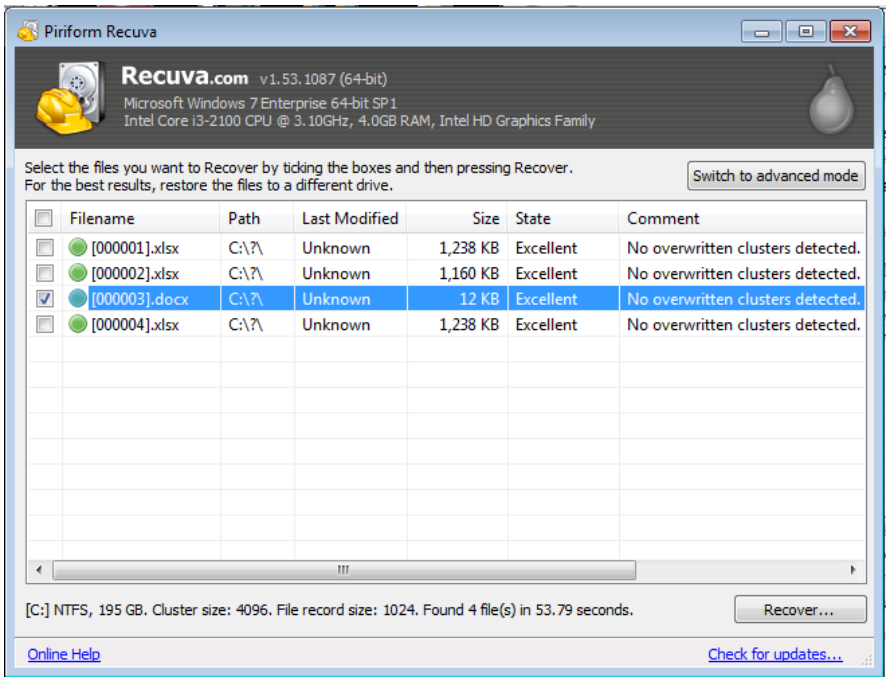
5. Select “In a Specific Location” and press “Next”.



6. Enable “Deep Scan” and Press “Start”.



7. The results are shown below. To recover the file, check the file to be recovered and press “Recover” button.



3.1.3 Autopsy

Autopsy (Carrier, B. 2018) is a computer forensic tool to analyse hard disk and smart phones. Autopsy is an Open Source Digital Forensic tool which allows the user to develop customised modules in Java or Python. Autopsy uses the Sleuth Kit which contains a collection of command line programs and C library in order to analyse hard disk and to recover files. Autopsy provides a range of features to enable a computer forensics analyst to conduct his/her investigation. Autopsy also provides Analysis and Reporting features.

Some of the features provided in the Analysis part are listed below:

- Registry Analysis
- Email Analysis
- Geo location analysis of JPEG files.
- Web Analysis
- Video Analysis
- File Recovery
- Multi-User collaboration
- File Type Detection.
- SMS, Call logs Analysis.

3.1.4 WinUndelete

WinUndelete (WinRecovery Software, 2018) is a recovery tool which enables users to recover their deleted files. The deleted files can be recovered from the hard disk, external drive, floppy disk and memory card from a digital device. It supports both the FAT and NTFS file system.

Below is a list of situations which WinUndelete can be used to recover files:

- Restores files after the recycle bin has been emptied.
- Restores files after a command prompt delete or a “Shift+Delete”.
- Restores files from a network share.
- Restores files after a Move or Cut command.

3.1.5 Ontrack EasyRecovery

Ontrack (Ontrack, 2018) provides a series of software recovery tools on a trial basis and allows users to recover deleted files and data from formatted and corrupted disks. Furthermore Ontrack provides software for email recovery, SharePoint recovery, SQL recover and Mobile phone recovery software for Windows and Mac.

As we can see, there are many software available to recover delete files. However recovery is only possible if the disk space where the file is residing has not been overwritten.

4. DELETED PARTITIONS RECOVERY

Dividing a hard disk into different volumes is known as partitioning. Each partition is labelled as a drive letter by the operating system and becomes a logical drive as shown in Figure 3.8. Each logical drive can be formatted to support different operating systems as well as to use different file systems (either FAT16, FAT32, NTFS). Partitioning is performed for increased performance and management of data. For each partition created, an entry is performed in the partition table. Therefore when a partition is deleted, the entry is removed from the partition table (and the space becomes unallocated). To restore the partition, forensic software tools can be employed. Those tools usually search for the boot sector in order to restore the partition. This section introduces some of the tools used to restore a partition.

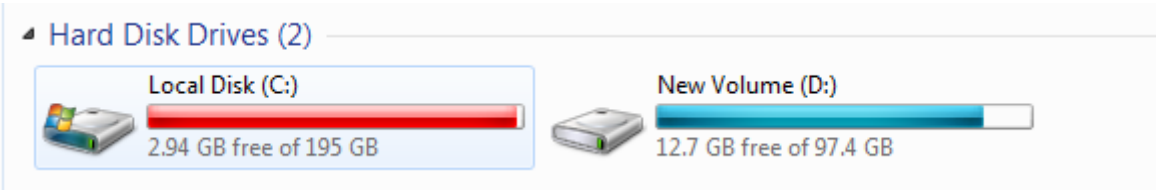
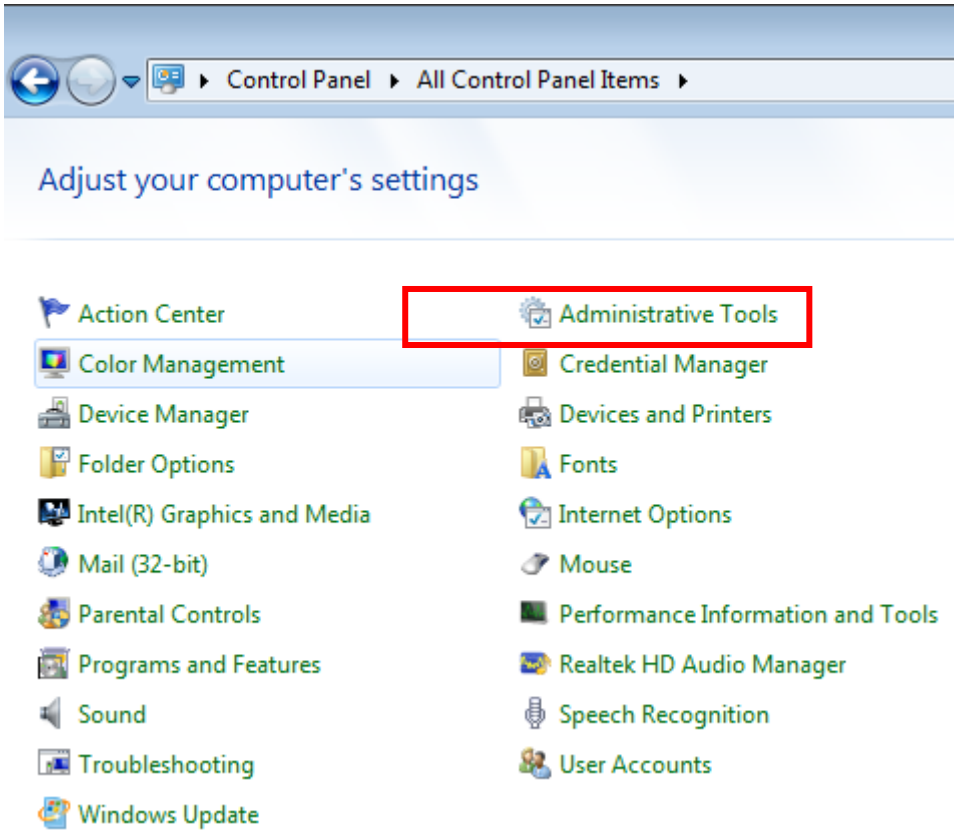


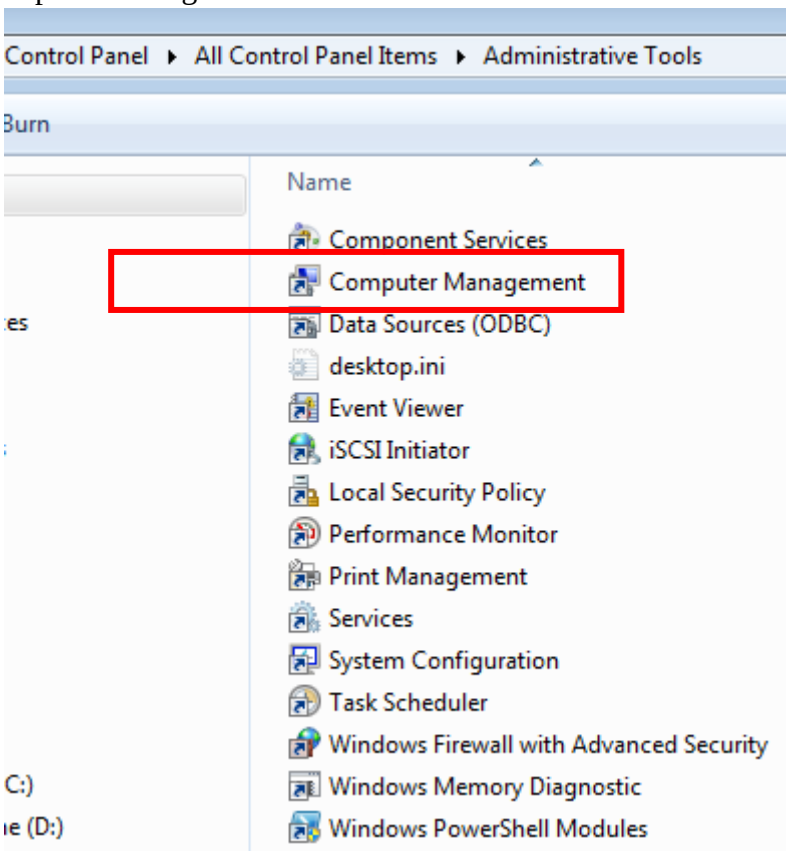
Figure 3.8

To manage and view the partitions on a hard disk in Windows, follow the steps below:

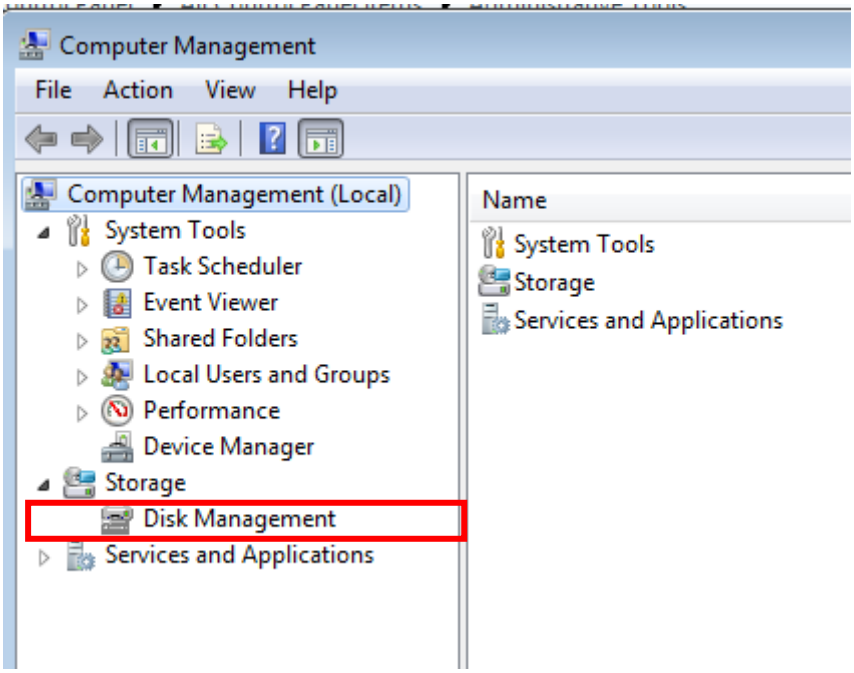
- Go to Control Panel
- Select Administrative tools



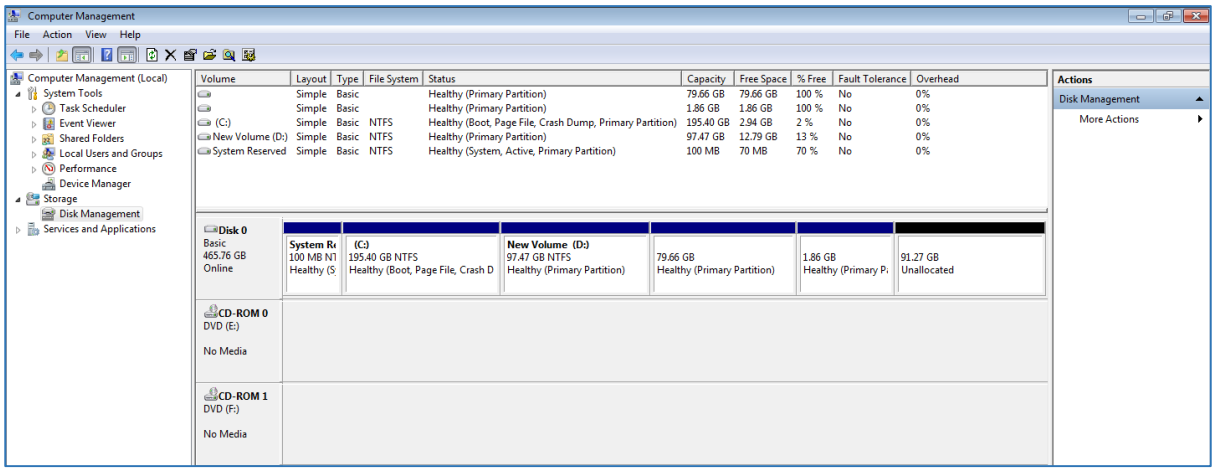
- Click on “Computer Management”.

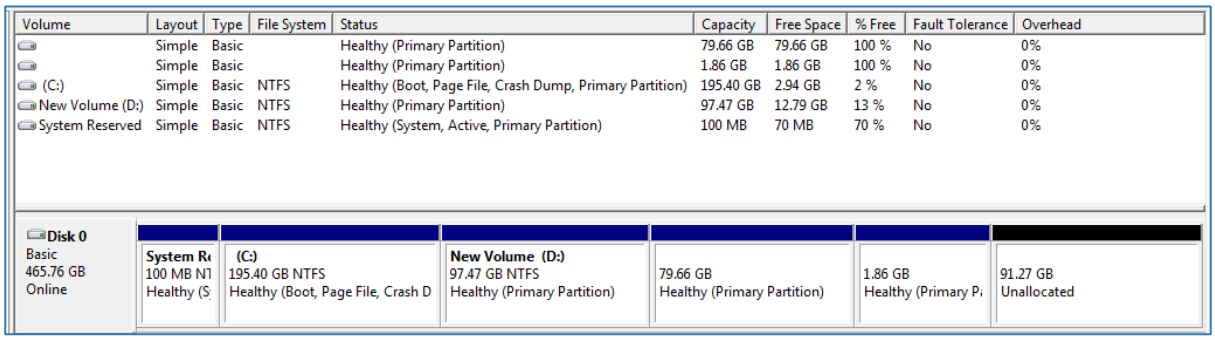


- Select “Disk Management”.

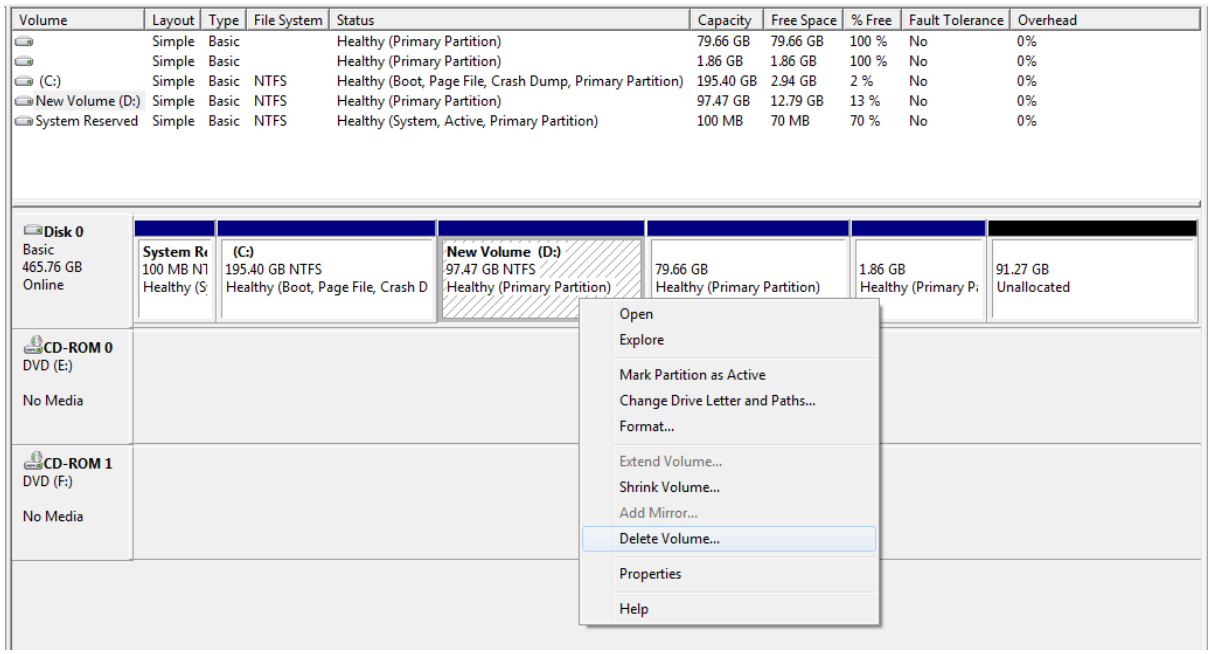


- Upon clicking on “Disk Management”, the utility will show all the logical drives available and their properties. In this example, there are five partitions (System Reserved, C:, D:, two healthy partitions and an unallocated partitions). The C: logical drive is the Boot volume, that is, it contains the files to start up the computer. The C: logical drive is also the Page File and Crash Dump volume, meaning that it contains all the memory dump output.





- To delete a partition, Right-Click on the "volume" and select "**Delete**". As stated earlier, deleting a partition or volume, does not necessary mean that the partition has been permanently removed. It can still be recovered through the use of computer forensics recovery software.



4.1 Deleted Partitions Restoration Tools

When a partition or volume is erased/deleted, the entry in the partition table is removed. Removing an entry from the partition table does not mean that the partition has been purged permanently. The partition may still be available on the disk. The partition can be recovered through the use of partition recovery software tools as long as the partition has not been overwritten on the disk space. The main thrust of the partition recovery software tool is to find the boot sector of the deleted partition and restore the partition by making an entry in the partition table. This section will highlight some of the partition recovery tools by computer forensic analyst to recovery deleted partitions.

4.1.1. EaseUS Partition Recovery Wizard

EaseUS (EaseUS, 2018) is a partition recovery tool used to restore deleted partitions. This tool scans several areas in the disk to search the location of the deleted partition. The software recovers deleted, lost and damaged FAT, NTFS, HFS, HFS+, HFSX, Ext2, Ext3 partitions under Windows.

4.1.2 Active@ Partition Recovery

Active@ Partition Recovery (LSoft Technologies, 2018) is a freeware to restore deleted and damaged partitions in Windows, Linux and DOS. Some of the main features of Active@ Partition Recovery are as follows:

- Partition Recovery- Restore deleted, lost and damaged partition.
- Provide three types of scanning: QuickScan (for searching and restoring recently deleted partitions), SuperScan (searching and restoring for partitions which have been deleted a long time ago) and Last Chance (searching and restoring severely damaged partitions).
- Backing up of partitions.
- Fixing damaged Partition Table and Master Boot Record (it contains all information on the disk partitions).
- Recover IDE, SATA, eSATA, SSD, SCSI, RAID, USB Flash Disks and Memory Cards.

4.1.3 Partition Find and Mount

Partition Find and Mount (A-FF Labs, 2018) is a software tool to search and mount lost partition in a read-only mode in order to prevent malware from altering the information.

The main features of Partition Find and Mount are as follows:

- It supports all versions of NTFS and FAT file systems.
- The software scans the hard disk for specific signatures belonging to the deleted or lost partition.
- It scans both the Master Boot Record and other information which will lead to the deleted or lost partition. As such, three scans are provided: Fast Intellectual Scan, Normal Scan and Thorough Scan,
- It does not work with badly damaged disk.

5. DATA ACQUISITION SOFTWARE

During computer forensic analysis, the analyst needs to use software tools in order to examine the data/information/evidence without modifying the data. Most of the data acquisition tools will duplicate the data/information/evidence such that it can be analysed without the risk of tampering the data/information/evidence. This section will preview some of the data acquisition tools used by computer forensic analyst.

5.1 Forensic Toolkit

Forensic Tookit (AccessData, 2018) is a computer forensics tool used to scan the hard disk for searching, and locating deleted files and emails. The Forensic Toolkit provides a standalone disk imaging tool (FTK Imager) used to duplicate the hard disk information. The FTK Imager replicates the hard disk as an image and then calculates the hash value using Message Digest algorithm: 5 (MD5). The MD5 ensures the integrity of the data. The image can then be used for analysis purposes. The image can be transferred to another machine for examination and can be saved under different image file format (for example DD/RAW).

5.2 EnCase Forensics

EnCase Forensics (Guidance Software, 2018) is a computer forensic tool used to collect information, analyse the data, report the findings and preserve the data. For preservation of the data, EnCase Forensics duplicates the original drive or media and then generates a MD5 hash values for the image as well as providing a Cyclic Redundancy Check (CRC) values to the data. The MD5 and CRC ensure that the data have not been modified and ensure the validity of the information. While duplicating the original drive, the analyst can specify which part of the drive (for example the C: or D: drive) or the types of files to be duplicated

Once the image has been produced, the computer forensics analyst can replicate the image to be analysed simultaneously by different examiners. Furthermore, EnCase Forensics provides the following features:

- Automation tools in order to speed up the investigation process
- Analysis features such as file signature, hash and log analysis
- Scanning in Unicode, binary Big Endian/Little Endian
- Reporting features
- Email and Internet Analysis

5.3 Data Dumper

Data Dumper (dd) is a UNIX utility tool for imaging a hard drive. dd replicates a computer's hard disk as an image for examination purpose. It is a command line tool and requires an understanding of the syntax to execute the command. dd can replicate information across files, devices, partitions and volume. Table 3.1 shows a list of command which can be executed by dd.

Table 3.1: dd Command

Data transfer forms of dd	
`blocks=$(isosize -d 2048 /dev/sr0)` `dd if=/dev/sr0 of=isoimage.iso bs=2048 count=$blocks status=progress`	Creates an ISO disk image from a CD-ROM, DVD or Blu-ray disk.[8]
`dd if=system.img of=/dev/sdc bs=4096 conv=noerror`	Restores a hard disk drive (or an SD card, for example) from a previously created image.
`dd if=/dev/sda2 of=/dev/sdb2 bs=4096 conv=noerror`	Clones one partition to another.
`dd if=/dev/ad0 of=/dev/ad1 bs=1M conv=noerror`	Clones a hard disk drive "ad0" to "ad1".

Source: dd Command (Wikipedia, 2018)

5.4 Mount Image Pro

Mount Image Pro (GetData, 2018) is a computer forensic tool which enables the computer forensic analyst to mount different forensic images or physical devices under Windows. The mounted image can then be analysed thoroughly by allowing the investigators to quickly browse the content in the image and running third party programs (virus scanners, keyword indexing tools and data restoration software) on the mounted image. Mount Image Pro supports a large variety of file image format such as

- EnCase .E01, EX01, .L01, .LX01
- AccessData .AD1
- DD and RAW images (Unix/Linux)
- Forensic File Format .AFF
- NUIX .MFS01
- ProDiscover
- Safeback v2
- SMART
- XWays .CTR
- VMWare
- Xways Container File

6. WINDOWS REGISTRY ANALYSIS

During an investigation, a computer forensics analyst needs to examine the Microsoft Windows Registry. The Microsoft Window Registry contains a large variety of information pertaining to the computer system. It contains useful information after someone has utilised the computer system. According to Microsoft, *"the registry is a system-defined database in which applications and system components store and retrieve configuration data. The data stored in the registry varies according to the version of Microsoft Windows. Applications use the registry API to retrieve, modify, or delete registry data*" (Microsoft, 2018).

Apart from storing valuable information on devices (hardware), it can also store a variety of information on the user's activity (such as which devices are connected to the computer system, which software was installed and uninstalled on the computer system by the user, to which wireless access point the computer has been connected to). Collecting these information is significant during an investigation.

The Windows Registry is a hierarchical database which contains information which is essential for the operation of the operation system (OS) and applications running on the computer system. The information is arranged in a tree structure and each node in the tree is known as a *key*. Each *key* contains both the *subkeys* and data entries known as *values (the values can be 0, 1 or hexadecimal)*. However, there are five main *key* nodes known as hives.

The five hives are:

i. HKEY_USERS: maintain all the user profiles on the computer system
ii. HKEY_CURRENT_USER: maintain the profile of the currently logged-on user
iii. HKEY_CLASSES_ROOT: Application configuration data to open files
iv. HKEY_CURRENT_CONFIG: startup system hardware information
v. HKEY_LOCAL_MACHINE: hardware and software configuration settings.

Figure 3.9 shows the Windows registry structure. To access the registry, type "regedit" in the "search windows"

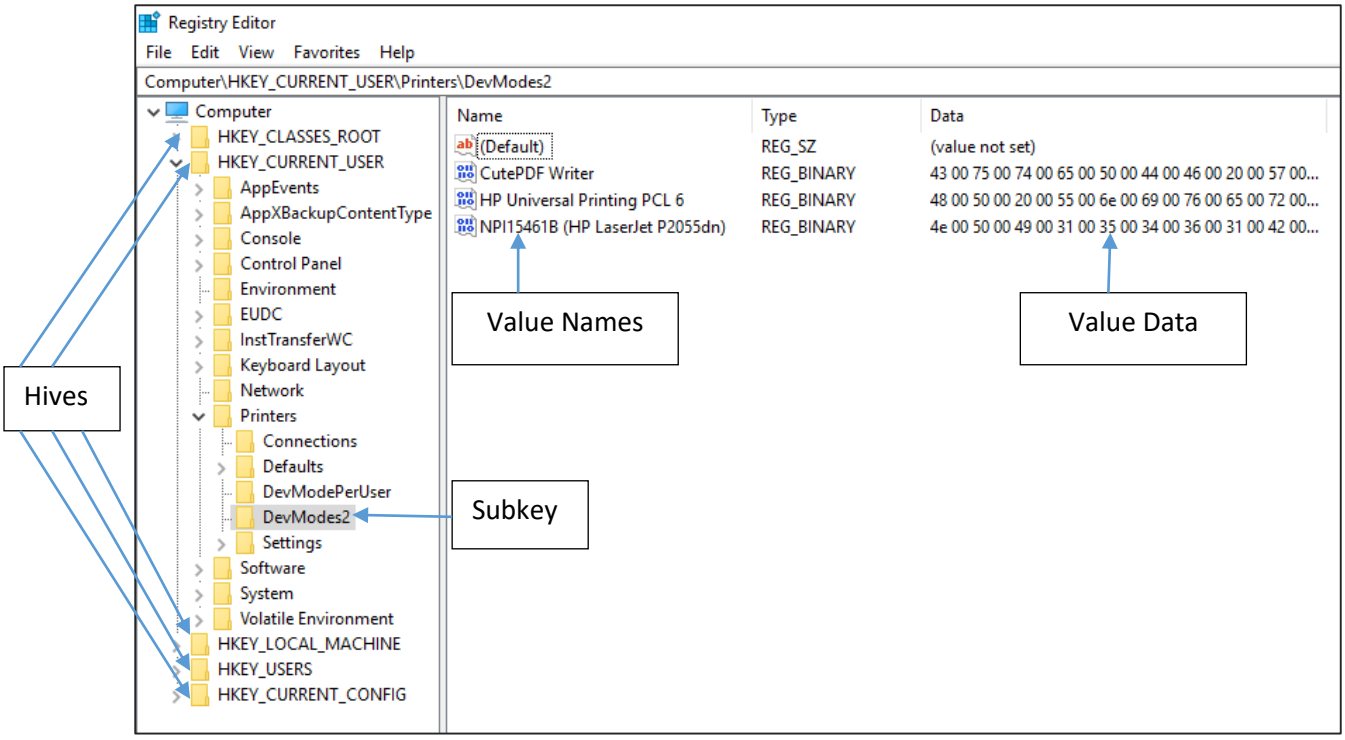


Figure 3.9: Windows Registry

6.1 Investigating the Windows Registry

During an investigation process, examining the Windows Registry will provide valuable information which can assist the investigation or can be used as a piece of evidence. This section will provide the common location which the computer analyst examines to retrieve information.

6.1.1 Autorun Programs

Autorun programs are programs which are launched during the bootup of the computer system. The Windows Registry provides all the programs which are launched during the booting of the computer system as well as the location where the program resides on the computer system. It is important to look at the registry in order to search for malware in the computer system which could have compromised the computer system or the computer system has been used to launch an attack through the use of a Trojan. Below is a list of paths where a computer forensic analyst will examine the registry:

- HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Runonce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

– HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Figure 3.10 shows an example of HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Run output.

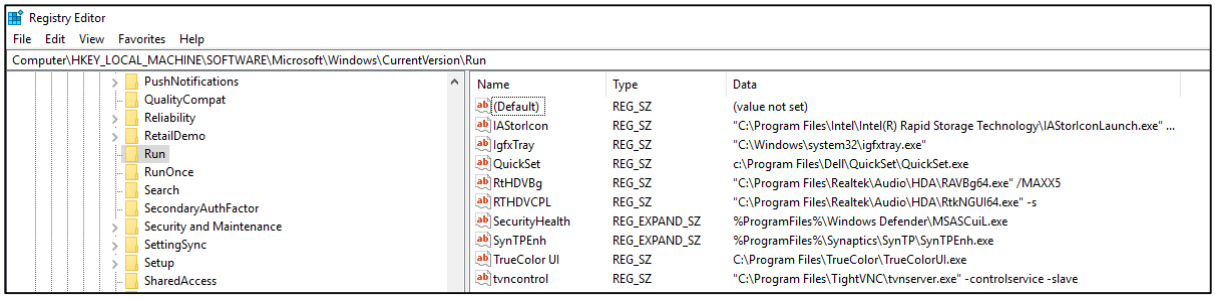


Figure 3.10: Example of Location for Autorun Program

(HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\Run)

6.1.2 Most Recently Used Entries

Most Recently Used contains all the entries made by the user while performing a specific action. For example, if the user has been using the RUN command (Figure 3.11), the following Registry Entries, HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU will show all the actions the user has been performing while using the RUN program. Figure 3.12 illustrates the RunMRU access in the Windows Registry.

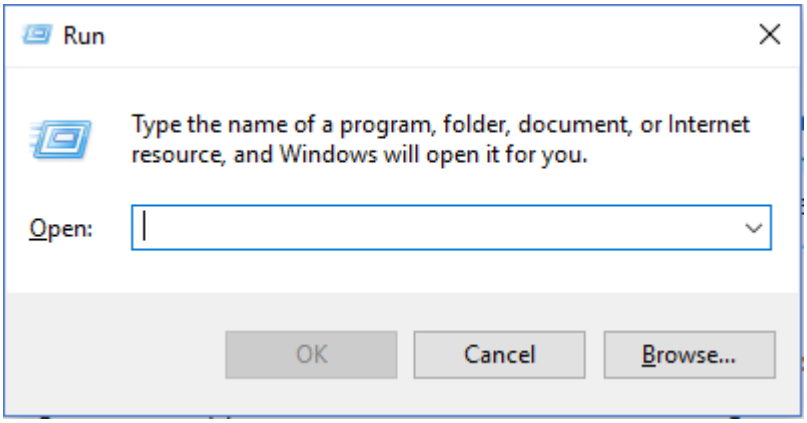


Figure 3.11: RUN Command

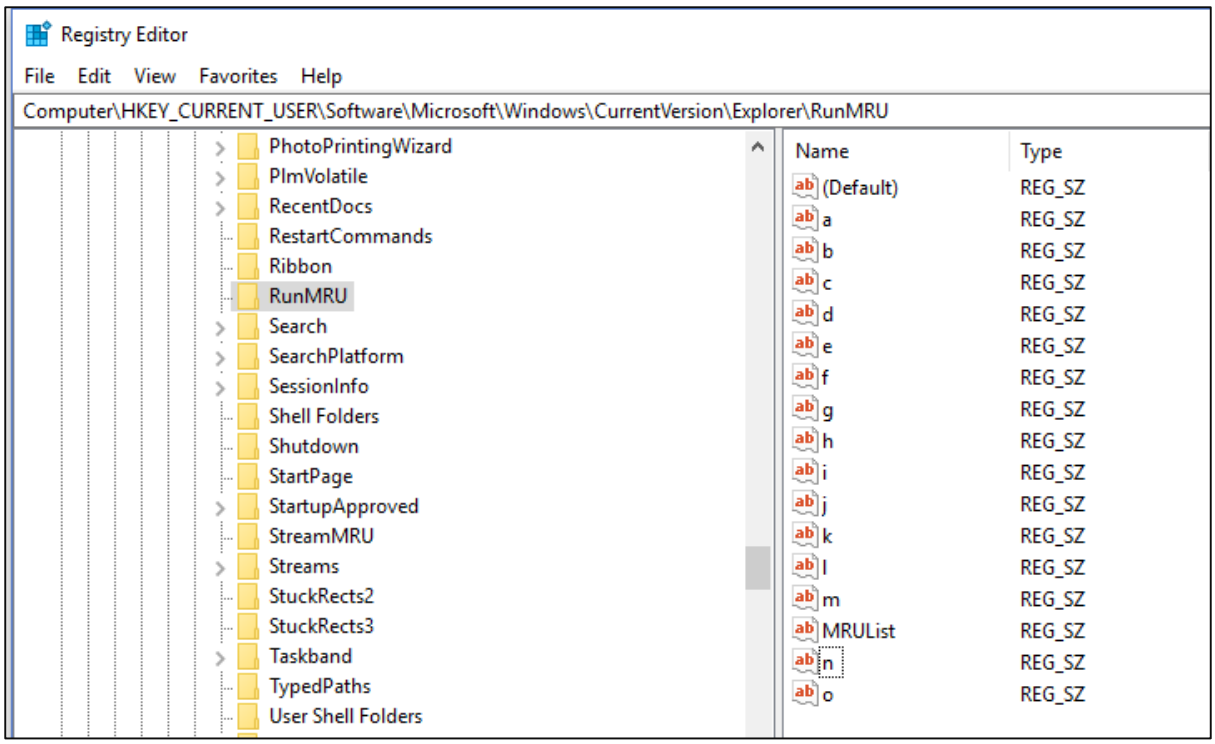


Figure 3.12: RunMRU Registry

6.1.3 Wireless Network Access

The Windows Registry records all the access points which the computer system has been connected to. It records the network SSID (Service Set Identifier). The latter information can be accessed as follows:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles.

Figure 3.13 shows all the SSID which the computer system has connected to. The Profile Name shows the SSID.

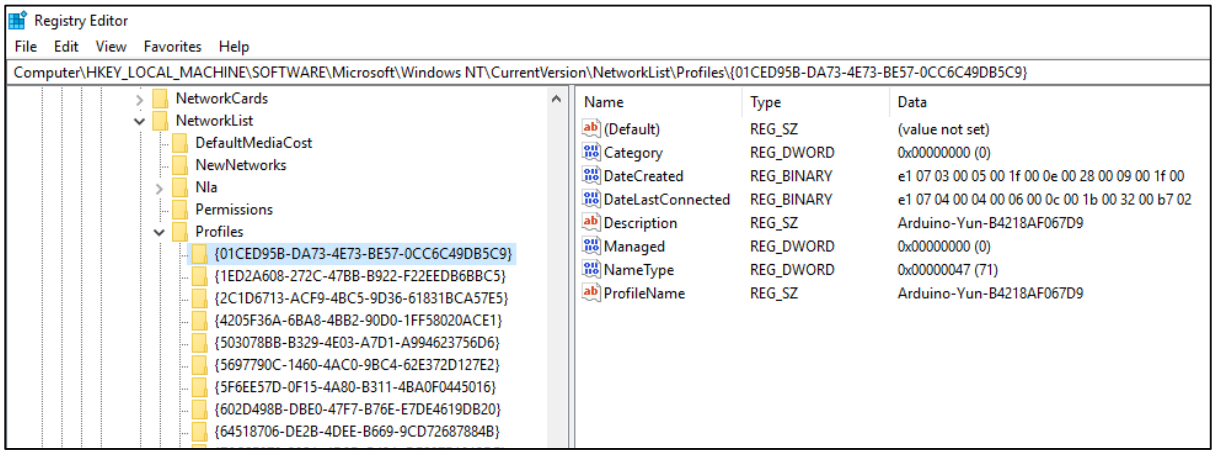


Figure 3.13: Wireless Network Access.

6.1.4 Connected USB Devices

To know all the USB devices which have been connected to the computer system, the following path is used on the registry: HKEY_LOCAL_MACHINE \SYSTEM\ControlSet00x\Enum\USBSTOR. The latter stores all the information with respect to the USB devices as shown in Figure 3.14. One important piece of information is the Device ID. The Device ID is a unique number which is provided by the manufacturer. Hence it is possible to trace the USB.

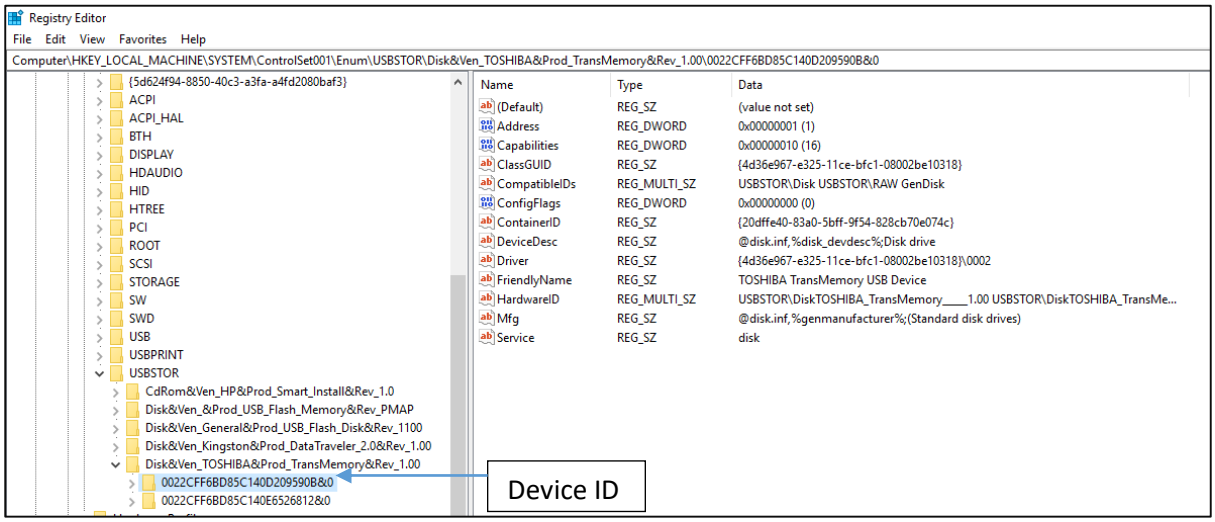


Figure 3.14: USB Devices

6.1.5 Browser (Internet Explorer)

The default browser proposed by Windows is Internet Explorer. To obtain some initial information on the Internet Explorer used on the computer system, this can be obtained as follows: HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\Main. The latter provides the user default settings such as the default search page and start page information as illustrated in Figure 3.15.

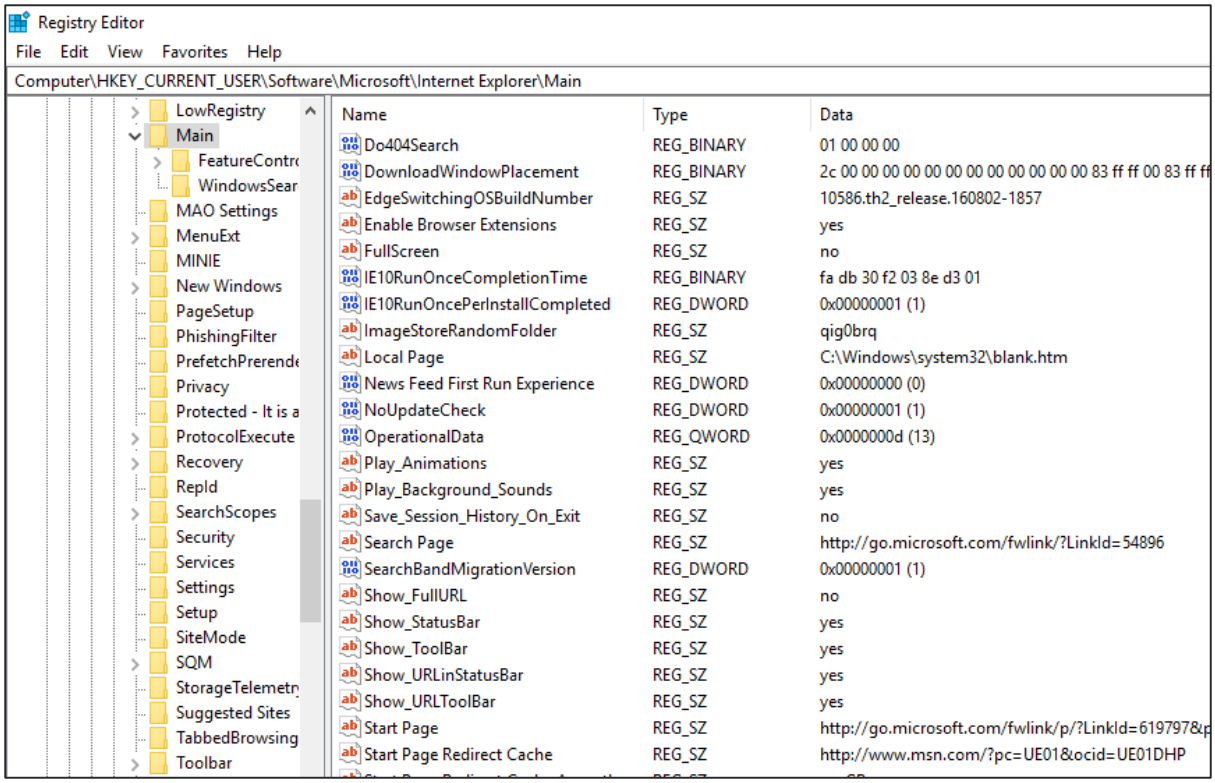


Figure 3.15: Internet Explorer

Besides to obtain information on the URL typed, the following registry path can be examined:

HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\TypedURLs.

6.1.6 Recently Used Documents

The Windows registry provides information on the user activities such as recent used document on the computer system. To obtain the latter information, the following registry path should be used: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs as illustrated by Figure 3.16.

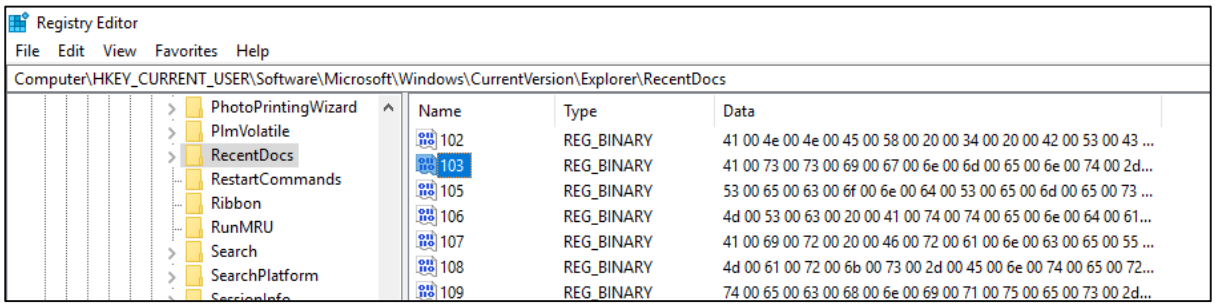


Figure 3.16: Recently Used Documents

To obtain further information on a particular document, right-click on the Name (for example 103) as shown in Figure 3.17. On the right hand side, you can have the document name and thus you may search for this document.

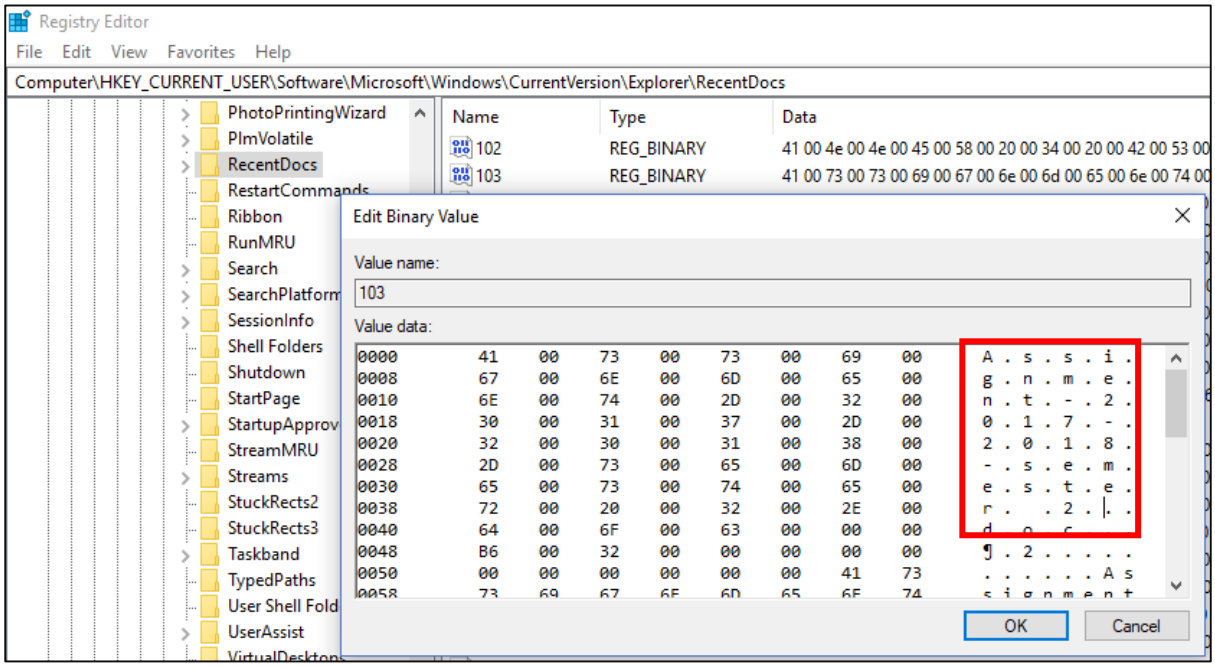


Figure 3.17: In depth Information for a Particular File