

MODERN EDUCATION SOCIETY'S WADIA COLLEGE OF ENGINEERING, PUNE

Fourth Year of Computer Engineering (2019 Course)

410247: Laboratory Practice IV

410244(C): Cyber Security and Digital Forensics

NAME OF STUDENT:	CLASS: BE
SEMESTER/YEAR: VII	ROLL NO:
DATE OF PERFORMANCE:	DATE OF SUBMISSION:
EXAMINED BY:	EXPERIMENT NO:

TITLE: Permanent Deleted Files

AIM/PROBLEM STATEMENT: Computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions

OBJECTIVES:

- To understand various vulnerabilities and use of various tools for assessment of vulnerabilities

OUTCOMES:

- Identify various vulnerabilities and demonstrate using various tools.

PRE-REQUISITES:

1. Knowledge of C, C++, python programming
2. Basic knowledge of computer, network and security information

THEORY:

1. 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.

1.1 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.

1.1.1 Data Recovery Pro

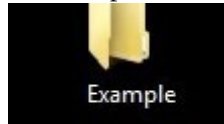
Data Recovery Pro software (Data Recovery Pro, 2018) is a free evaluation software which can be used to recover deleted files. To use the Advance features, the users need to make a purchase. For example, to recover a file, the user needs to register for this feature. The software provides the following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

- Restoration of deleted email and deleted email attachments
- Recovery of files from a recently formatted or partitioned disk

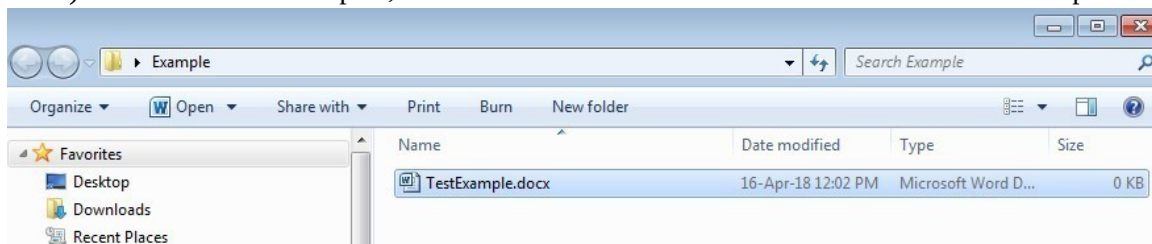
- Restoration of a large variety of file types (Binary files or compressed files) Restoration of files from peripheral storage devices (such as USB) Recovery of Windows system files.

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

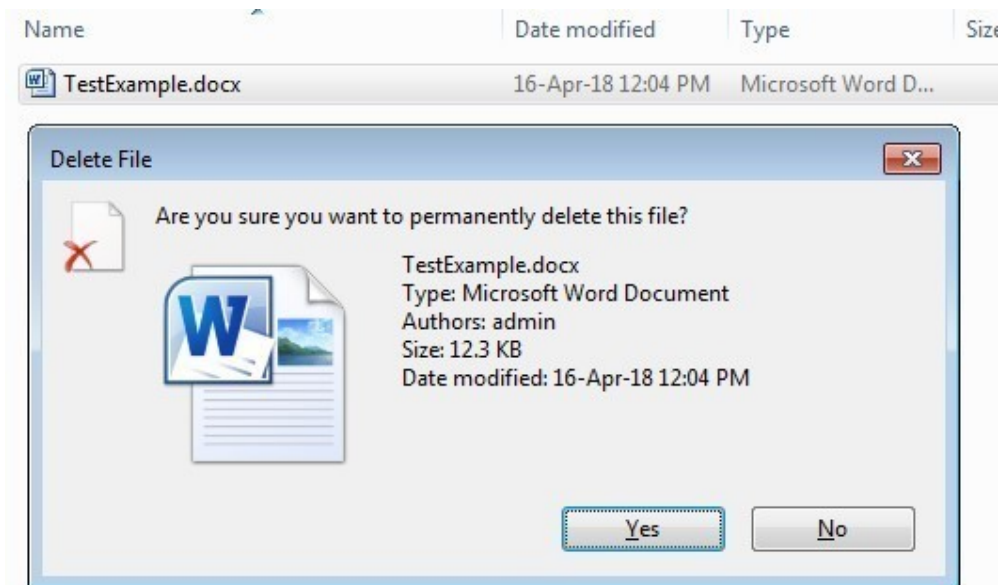
- 2) Download and install the software from <http://www.datarecoverydownload.com/download/>
- 3) As an example, create a folder on your Desktop and rename it as “Example”.



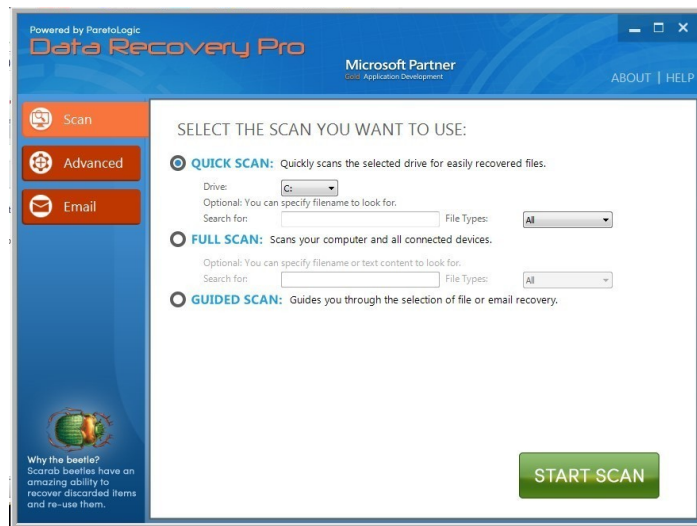
- 4) In the folder “Example”, create a Word Document file and name it as “TestExample.doc”.



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



- 6) 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.



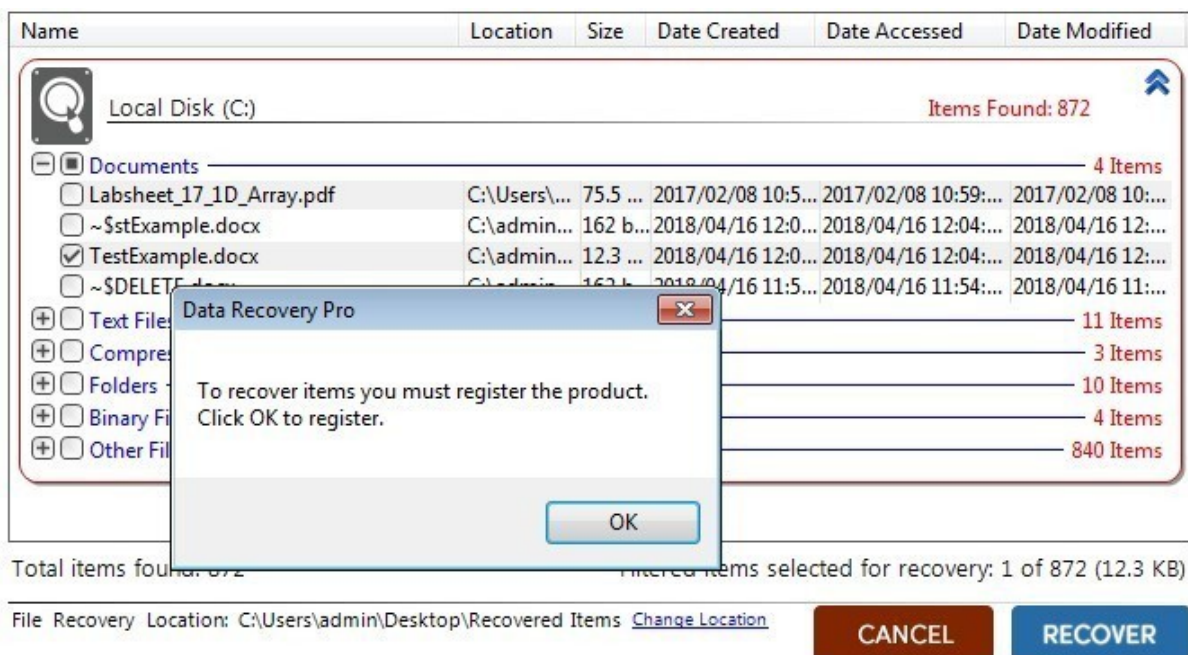
- 7) Press “Start Scan”. After the software has scanned the disks, the following screen will be presented:



- 8) Expand the “Documents” and the TestExample.docx will be available.



- 9) 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.



2. 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

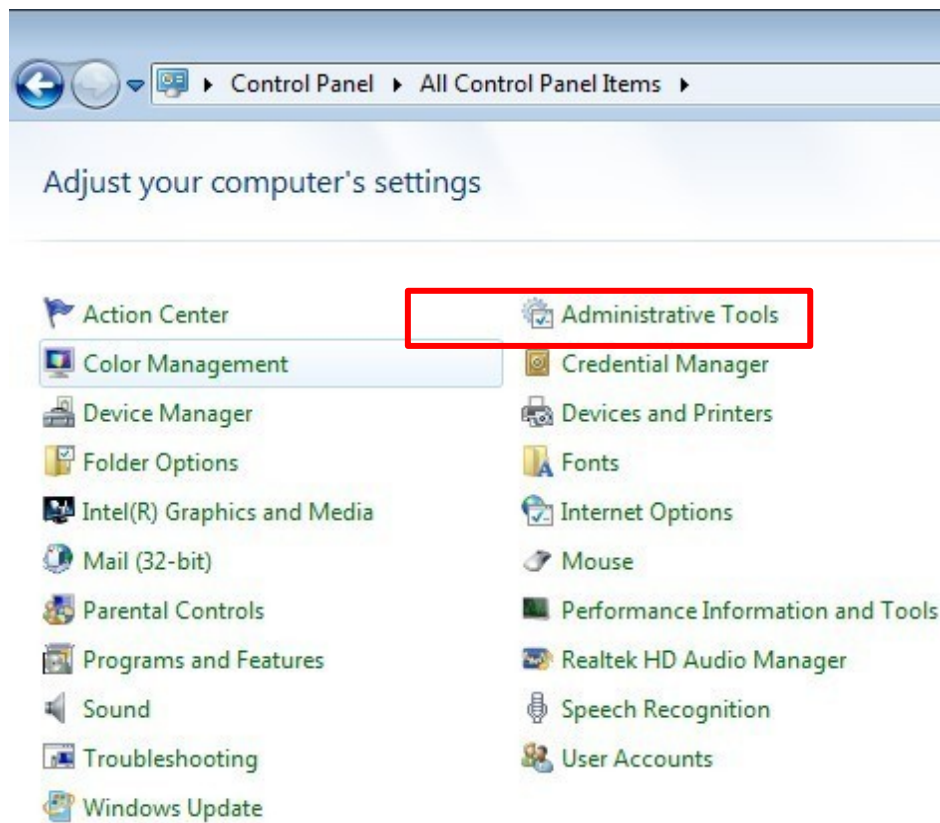
as to use different file systems (either FAT16, FAT32, NTFS). Partitioning is performed for increased performance and management of data. For each partition created, an entry is performed in the partition table. Therefore when a partition is deleted, the entry is removed from the partition table (and 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.



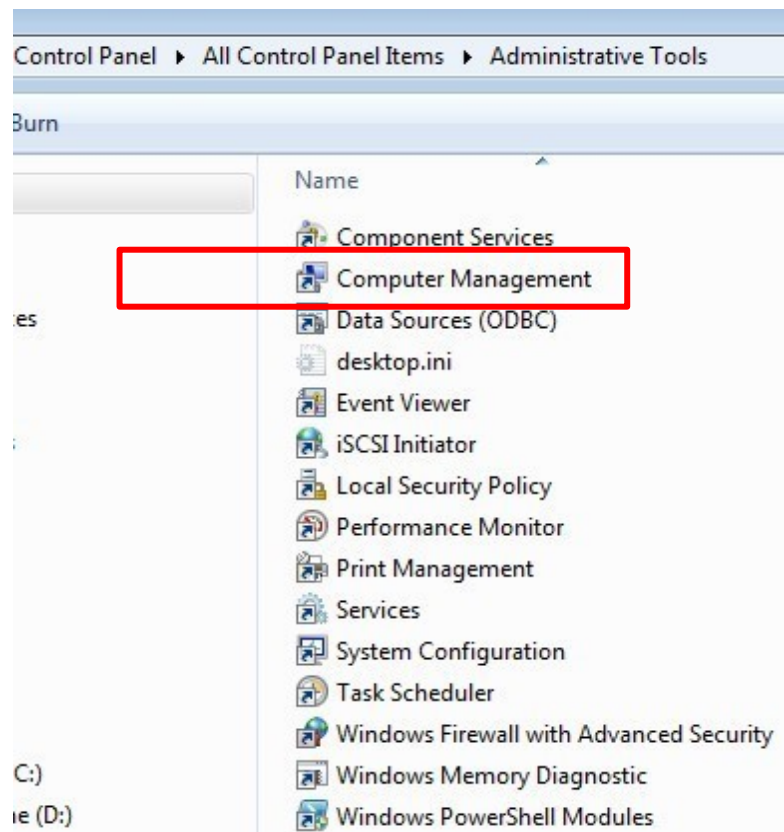
Figure 3.8

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

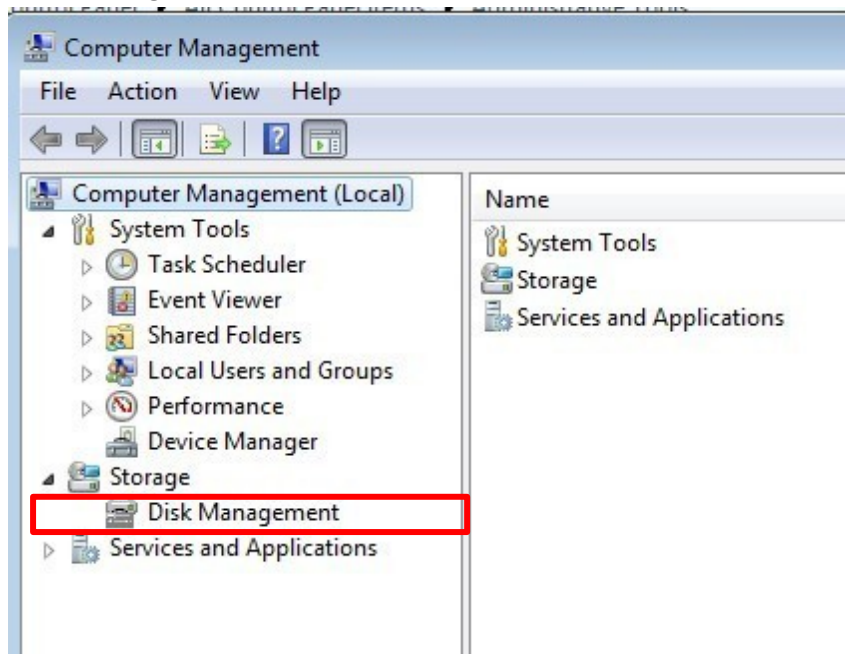
- Go to Control Panel
- Select Administrative tools



- Click on "Computer Management".ent

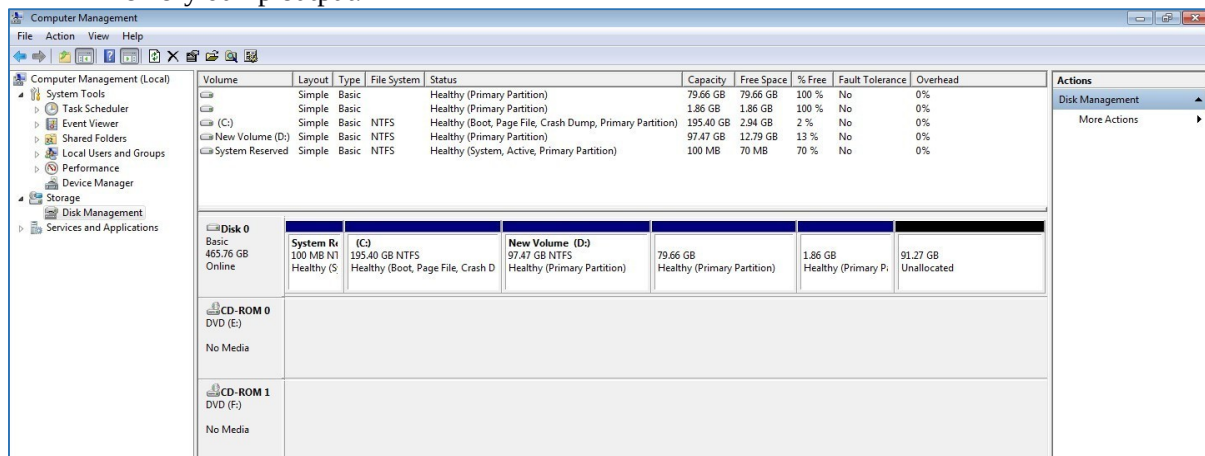


- Select “Disk Management”.



- 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.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	70 MB	70 %	No	0%
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	195.40 GB	2.94 GB	2 %	No	0%
New Volume (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	97.47 GB	12.79 GB	13 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	70 MB	70 %	No	0%

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	70 MB	70 %	No	0%
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	195.40 GB	2.94 GB	2 %	No	0%
New Volume (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	97.47 GB	12.79 GB	13 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	70 MB	70 %	No	0%

- 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.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
	Simple	Basic		Healthy (Primary Partition)	79.66 GB	79.66 GB	100 %	No	0%
	Simple	Basic		Healthy (Primary Partition)	1.86 GB	1.86 GB	100 %	No	0%
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	195.40 GB	2.94 GB	2 %	No	0%
New Volume (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	97.47 GB	12.79 GB	13 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	70 MB	70 %	No	0%

Disk 0 Basic 465.76 GB Online	System Reserved 100 MB NTFS Healthy (S)	(C:) 195.40 GB NTFS Healthy (Boot, Page File, Crash D	New Volume (D:) 97.47 GB NTFS Healthy (Primary Partition)	79.66 GB Healthy (Primary Partition)	1.86 GB Healthy (Primary P	91.27 GB Unallocated
-----------------------------------------------	------------------------------------------------------	--------------------------------------------------------------------	------------------------------------------------------------------------	-----------------------------------------	-------------------------------	-------------------------

CD-ROM 0 DVD (E:) No Media	
CD-ROM 1 DVD (F:) No Media	

2.1 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.

2.1.1. 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.

Conclusion: Thus we have coded computer forensic application for Recovering permanent Deleted Files and Deleted Partitions

Questions:

1. List some of the softwares for recovering deleted files?
2. List some examples of file systems