
Digital Forensics - Lab 10

Class No :	CH2021221000516	Slot :	L49 + L50
Course Code :	CSE4004	Faculty Name :	Nagaraj SV

Aadhitya Swarnesh

- 21 October 2021

Question 1 :

Identification of lost or deleted partitions

Create a partition in your drive (may be a USB flash drive) using appropriate tools. Make and copy files of various file types (such as jpg, mp3 etc). Then delete the partition. Check if you are able to detect the files which were there earlier. Use a utility such as TestDisk to recover the partition and then the files.

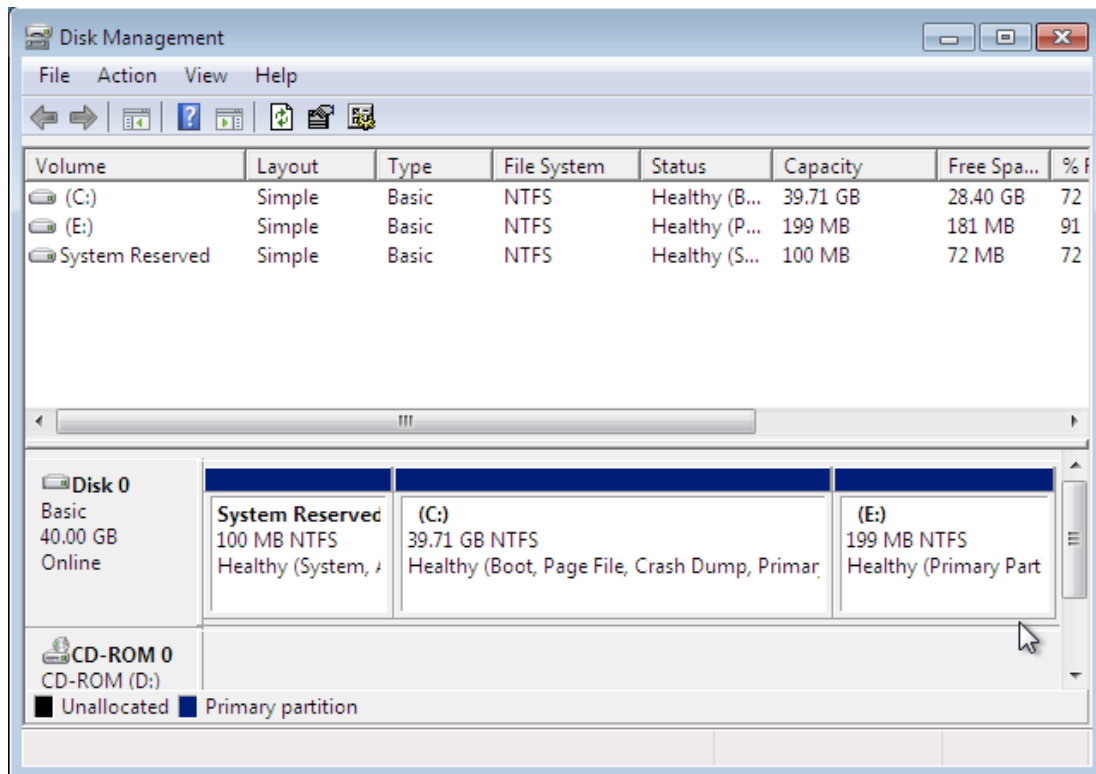
TestDisk is powerful free data recovery software! It was primarily designed to help recover lost partitions and/or make non-booting disks bootable again when these symptoms are caused by faulty software: certain types of viruses or human error.

In this lab, we will deal with many ways of viewing, recovering, restoring files or even the entire part of partitions which are inaccessible due to it being corrupted or to recover files from a partition we had deleted.

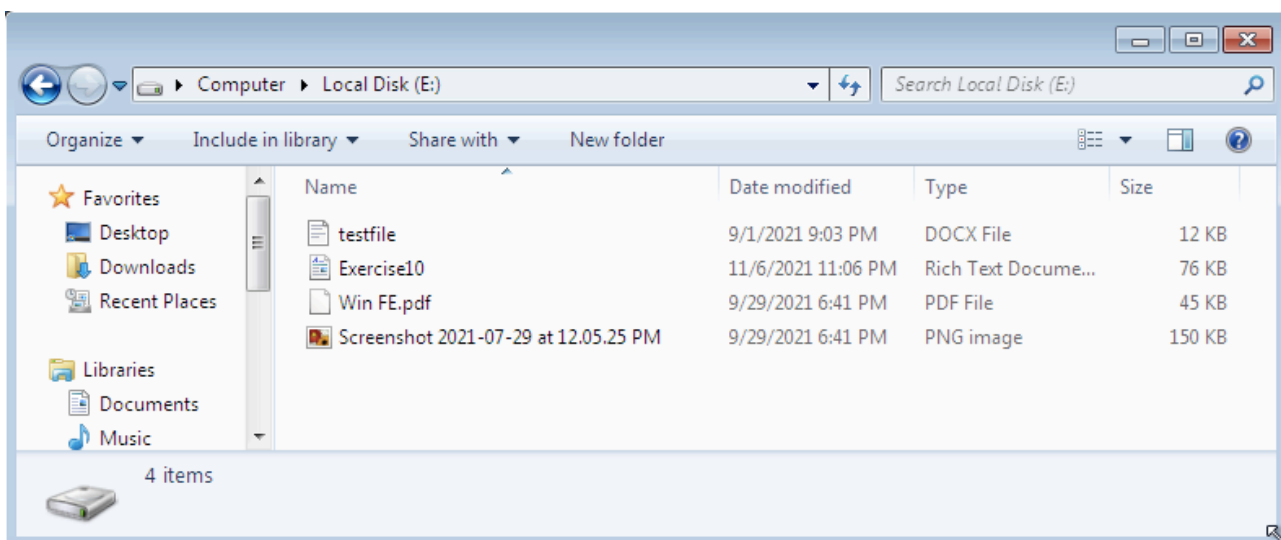
As a preface to thesis sets of experiments, files that we delete from our hard disk do not get deleted in actual sense from the disk, rather the pointers which point to such files are removed and so the files actually still exist in the disk. Keep this in mind the next time you format a disk. In case you want to delete the files completely from the disk, then a suggestion would be to use a more elaborate formatting option which writes multiple layers of 0's or 1's onto the disk to overwrite the previous content, so as to prevent any chances of data recovery at a later stage.

In this current portion of today's lab, we will use the TestDisk tool, to view the files which seem to be deleted when we delete a partition. As a setup process we will first detail the situation and the problem in our hands and then explain the recovery with test disk. The below setup procedure is just a preface and thus is the same for all the three parts of today's lab.

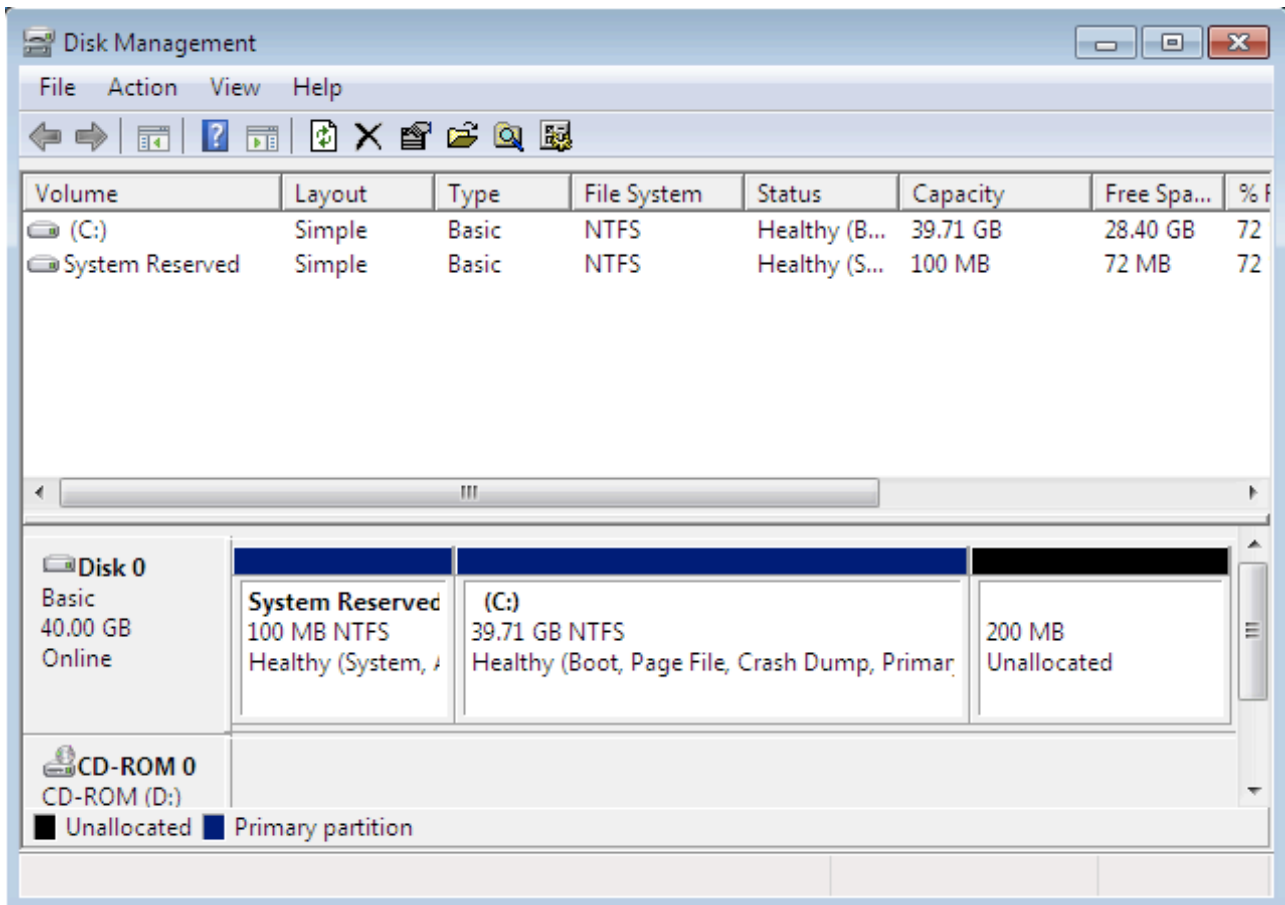
For today's lab, we will be working with **Windows 7**. We first create a new partition using Windows Disk Management Tool. As you can see below, we have created a new partition labelled 'E', of around 200MB.



We will then move files of different formats onto this partition, for the sake of this lab, we will move one file each from a set of different file formats. The files which have been moved onto the disk are as follows :



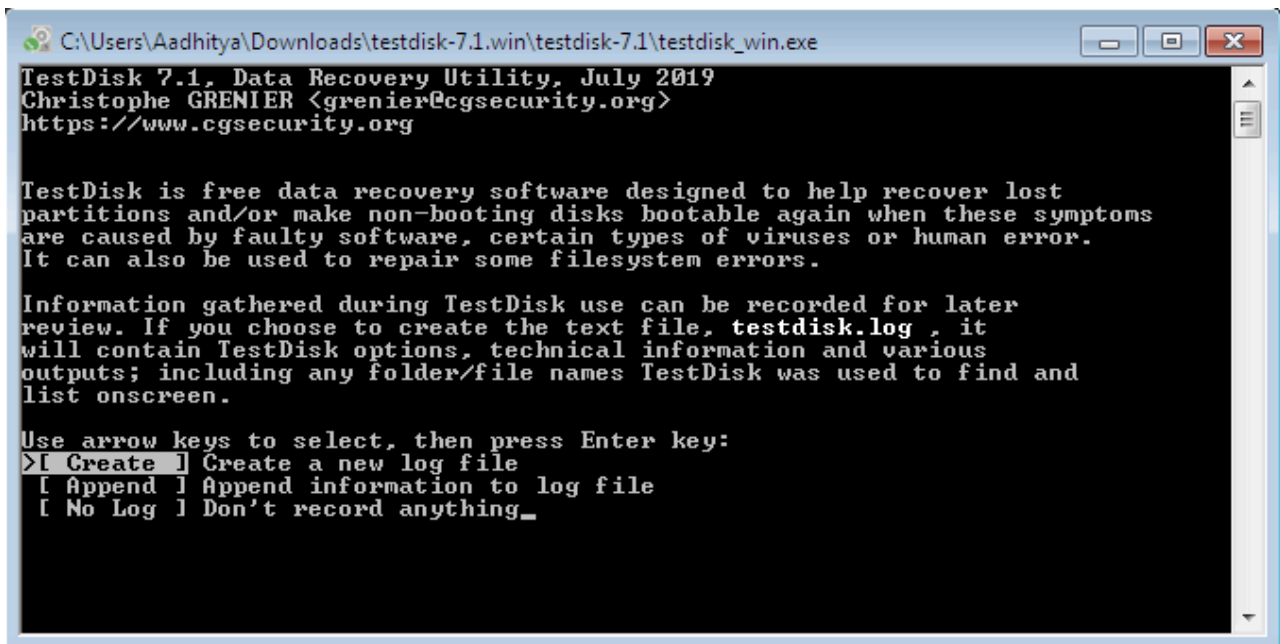
We will now move over to the disk management tool and then delete the partition. Once we do this, the partition table might look modified as shown the the following picture. Notice that the partition has been turned into **Unallocated Space**.



Note here that this is the setup process and is common for all the three portions of the lab which will be covered below.

We have downloaded the tool TestDisk and have extracted the zip file.

After extracting the downloaded compressed file, we run the application, and proceed as depicted in the following steps :



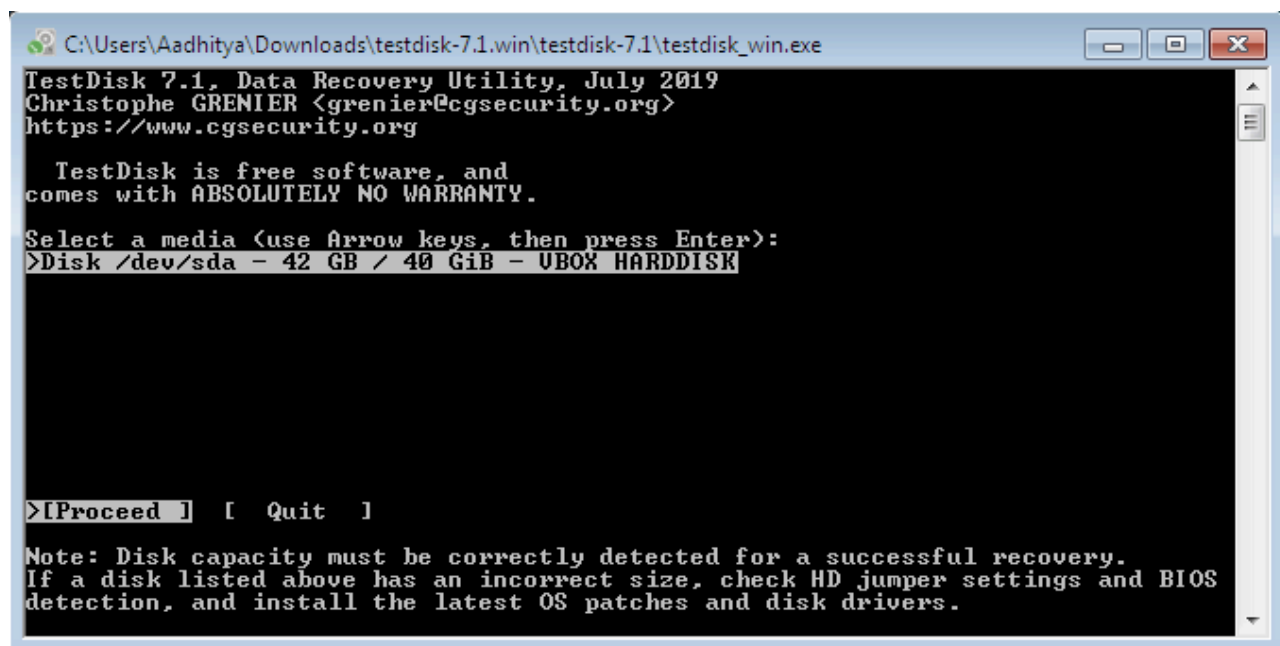
```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
[ Append ] Append information to log file
[ No Log ] Don't record anything_
```

The following diagram shows the list of all devices connected to our computer. In this case we have only the computer's hard disk.



```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 42 GB / 40 GiB - UBOX HARDDISK

[Proceed ] [ Quit ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

Let us click on this and proceed to this hard disk and then select the type of the partition table. Notice here that the tool itself has recognized the partition to be of the type Intel, and has recommended us to choose the same.

```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - UBOX HARDDISK

Please select the partition table type, press Enter when done.
>[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map <Mac i386, some x86_64...>
[Humax] Humax partition table
[Mac] Apple partition map <legacy>
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] XBox partition
[Return] Return to disk selection_

Hint: Intel partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

Let us now choose to analyse the partition table structure to find our missing or in this case deleted partition.

```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - UBOX HARDDISK
CHS 5221 255 63 - sector size=512

>[Analyse] Analyse current partition structure and search for lost partitions
[Advanced] Filesystem Utils
[Geometry] Change disk geometry
[Options] Modify options
[MBR Code] Write TestDisk MBR code to first sector
[Delete] Delete all data in the partition table
[Quit] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Once we choose to analyse the partition structure, the tool scans for any and all available and active partitions in the partition table and by scanning the disk. After the scanning process, the tool mentions the two partitions which are active partitions or in other words which are visible in the windows folder and is readily available for use.

```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - CHS 5221 255 63
Current partition structure:
  Partition              Start          End      Size in sectors
  1 * HPFS - NTFS         0  32 33      12 223 19      204800 [System Reserved]
  2 P HPFS - NTFS        12 223 20    5196 10 62    83267584

*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
>[Quick Search]  [ Backup ]
Try to locate partition_
```

We will now do a Quick search for other partitions which might be invisible and inaccessible due to reasons like it being deleted, corrupted, etc. The diagram below shows the tool searching the whole disk for such partitions.

```
C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - CHS 5221 255 63
Analyse cylinder 5221/5220: 99%

HPFS - NTFS         0  32 33      12 223 19      204800 [System Reserved]
HPFS - NTFS        12 223 20    5195 233 30    83265536
HPFS - NTFS        51  5 233 31    5221 105  4      409600 [New Volume]
HPFS - NTFS        12 223 20    5221 137 36    83677184
HPFS - NTFS        5221 137 36 10430  51 52    83677184

Stop
```

After the scanning process, we can see the partitions which cannot be recovered. The diagram below shows the same.

```

C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - CHS 5221 255 63

The harddisk (42 GB / 40 GiB) seems too small! (< 85 GB / 79 GiB)
Check the harddisk size: HD jumper settings, BIOS detection...

The following partition can't be recovered:
  Partition      Start      End      Size in sectors
> HPFS - NTFS    5221 137 36 10430 51 52 83677184

[ Continue ]
NTFS, blocksize=4096, 42 GB / 39 GiB

```

If we continue, we then get a list of all partitions which are active and also the ones which are corrupted or deleted. The below diagram shows the list of all such partitions. Notice here that the partition that we had deleted earlier is now visible here and is marked as deleted.

```

C:\Users\Aadhitya\Downloads\testdisk-7.1.win\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sda - 42 GB / 40 GiB - CHS 5221 255 63
  Partition      Start      End      Size in sectors
* HPFS - NTFS    0 32 33 12 223 19 204800 [System Reserved]
D HPFS - NTFS    12 223 20 5196 10 62 83267584
D HPFS - NTFS    12 223 20 5221 137 36 83677184
>D HPFS - NTFS    5196 10 63 5221 105 4 407552

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
NTFS, blocksize=4096, 208 MB / 199 MiB

```

We can now choose the partition that we want and then browse the files inside it. After we choose the required files and folders, we can then move them to our other active partitions by specifying a destination directory for the files we choose from the deleted or corrupted partition.

There are many other such tools which are useful in navigating through and even recovering the files which have been stored in sectors of the disk which are not accessible, due to corruption of the disk or due to any other reasons. Besides the TestDisk tool used above, there are a few other tools which are open source and free to use. One such tool is the PhotoRec which is provided bundled along with TestDisk.

The PhotoRec tool is used to perform the same task as the Undelete tool which will be explored in detail at a later stage of this lab. It completely restores the entire deleted partition to undo the delete operation on the partition and make it look like the delete never took place.

Let us explore two other functionalities and thus two other tools when we take the concept of recovery in our hands.

Question 2 :

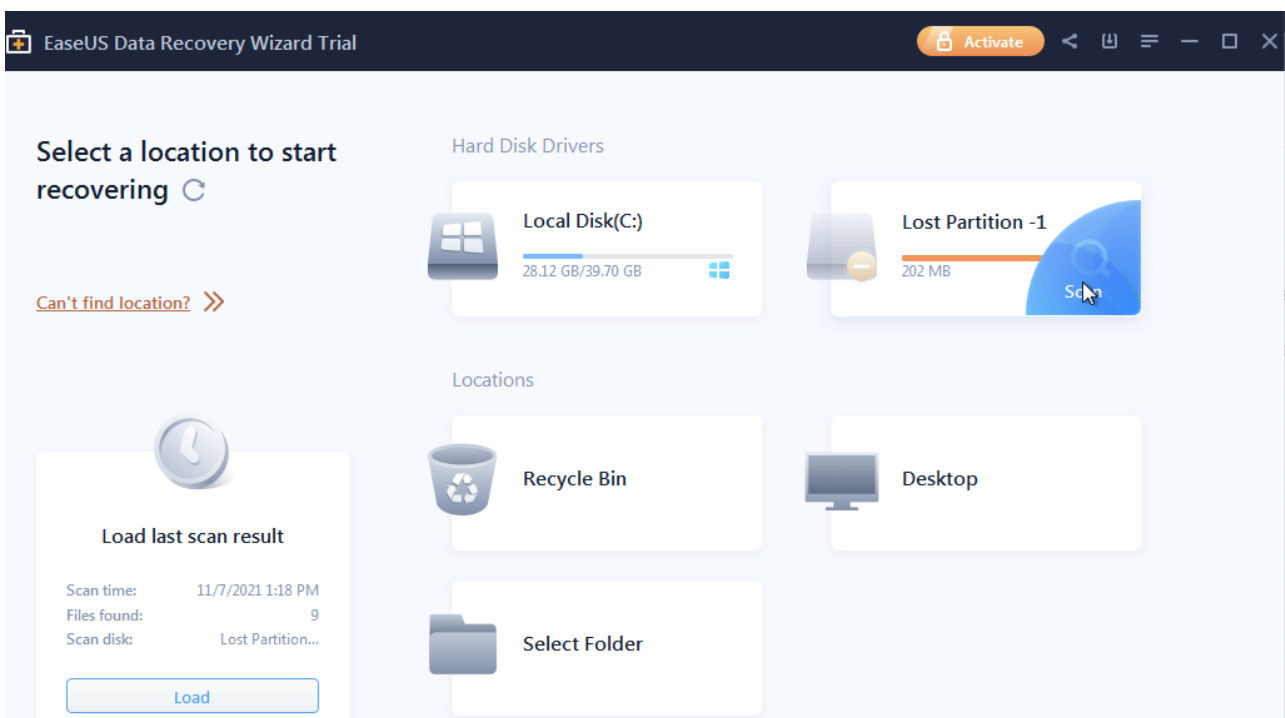
Recovering Files and Folders from Deleted Partitions

Download a trial version of EaseUS partition recovery software to restore files from lost or deleted hard drive partitions in Windows 10/8/7.

In this portion, we will restore the files from the deleted hard disk partition and then access the files which have been retrieved and copied to any location of our choice. For the setup process, we use the same deleted 200MB partition which was created and deleted in the previous portion of the lab.

At the end of this portion, we plan to restore the required files and folders from the deleted partition. For this, we will use the EaseUS partition recovery software. As a setup procedure for this portion, we download and install this software application.

We first ensure that the partition we want to restore has been deleted, we can do this by opening the disk management tool. After this, we open the EaseUs tool. After opening, it automatically scans the hard disk drive and recognizes all the invalid partitions i.e the ones which are corrupted or deleted.

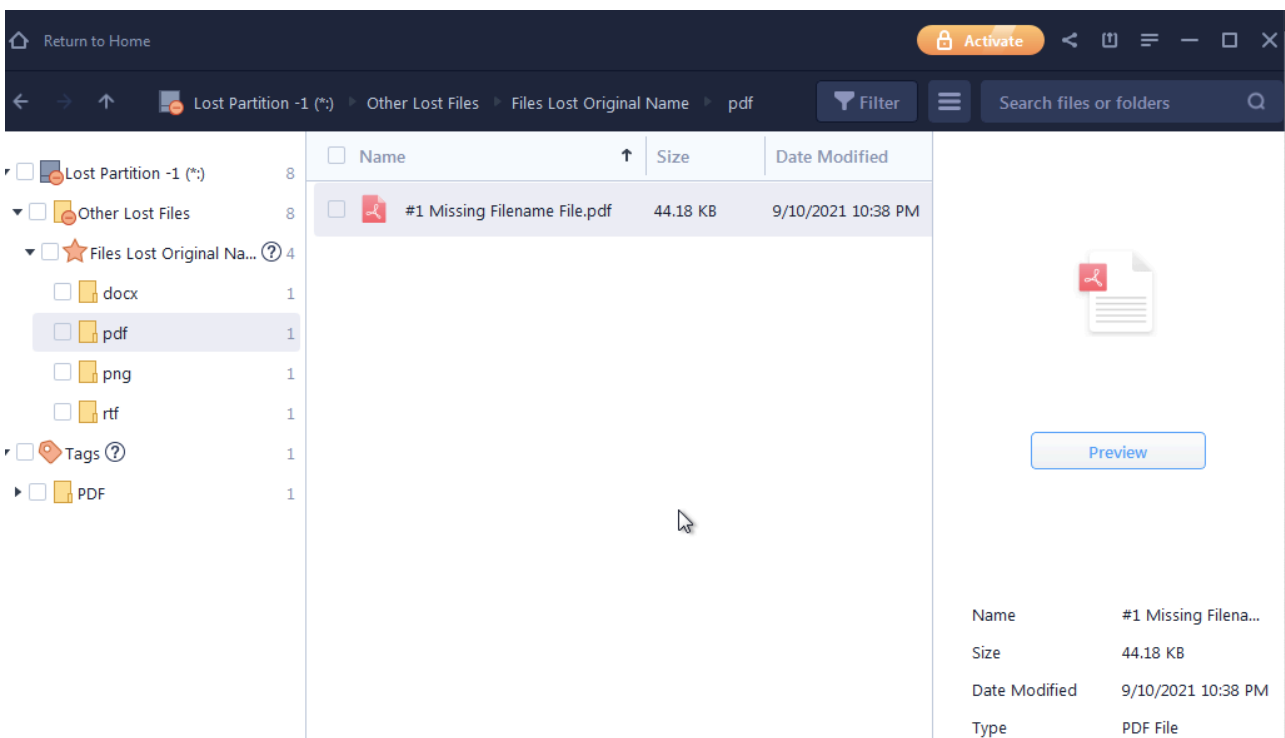


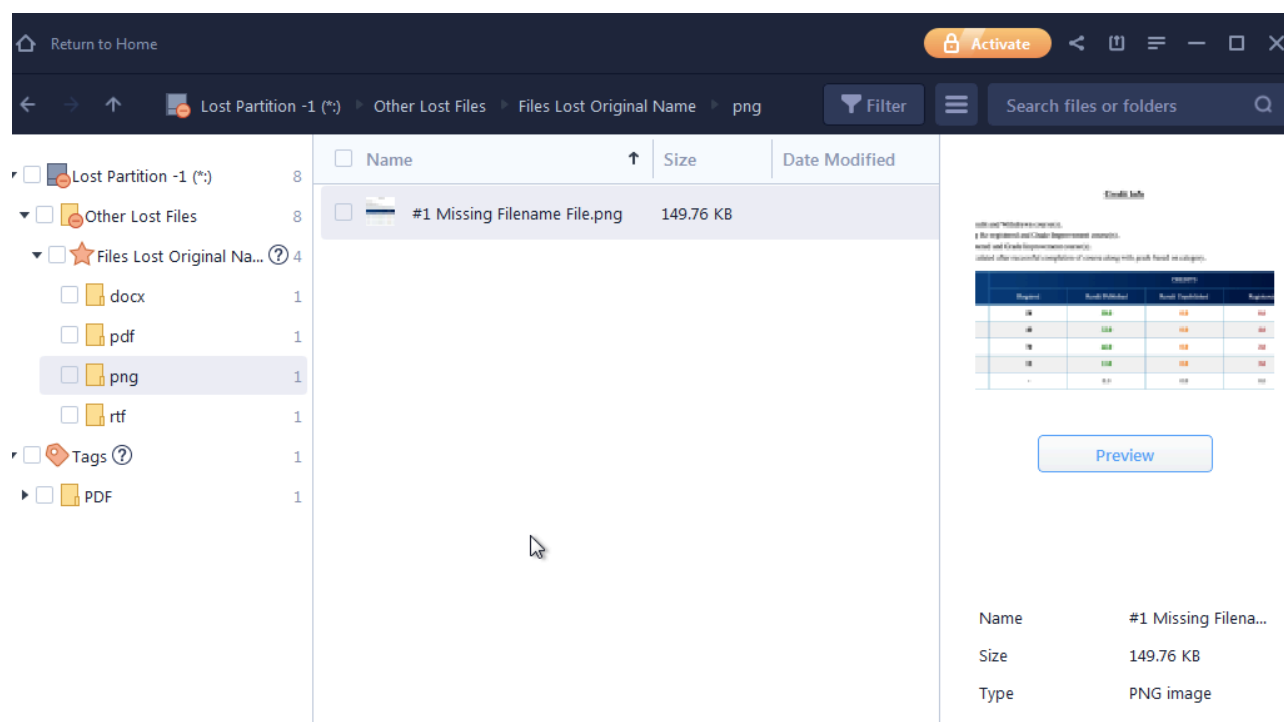
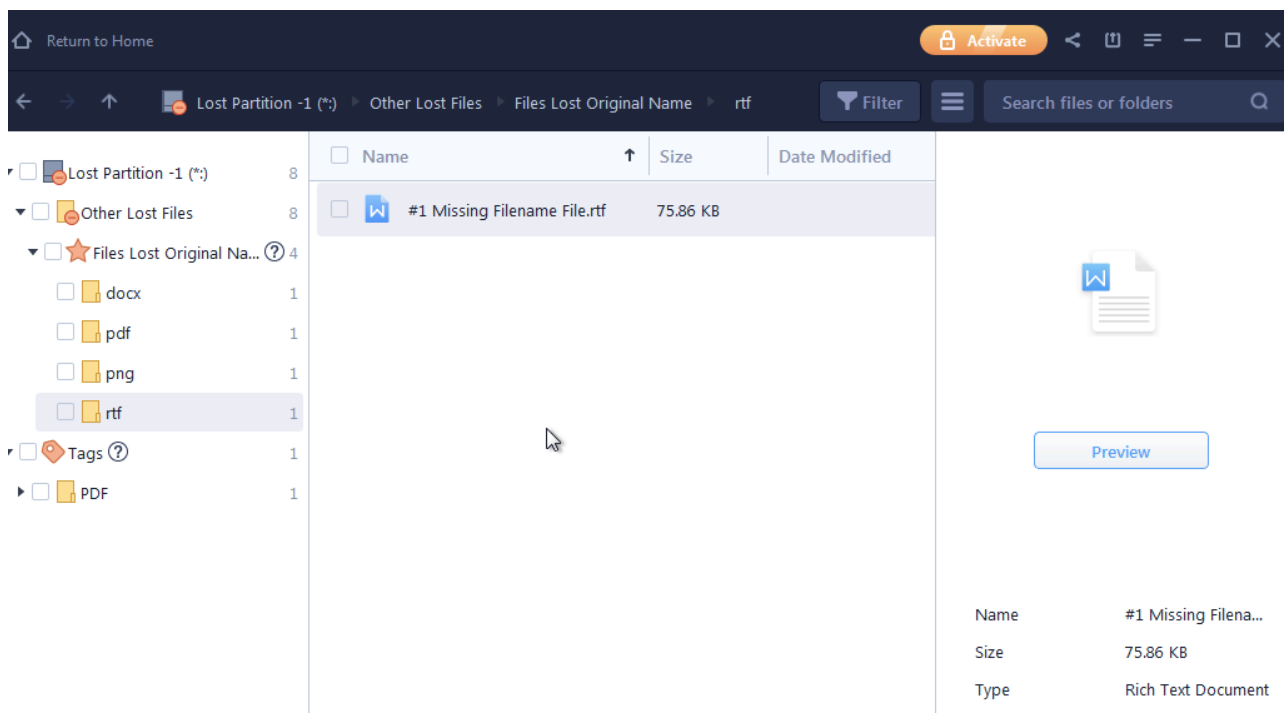
We then click on the scan option on the deleted or lost partition, which scans the partition for files or folders inside and then returns a list of all the files based on the file formats, and groups them on the same basis. It is not able to retrieve the names of such files, but is able to retrieve the files.

The below diagrams show a few files which it has listed down by the file format.

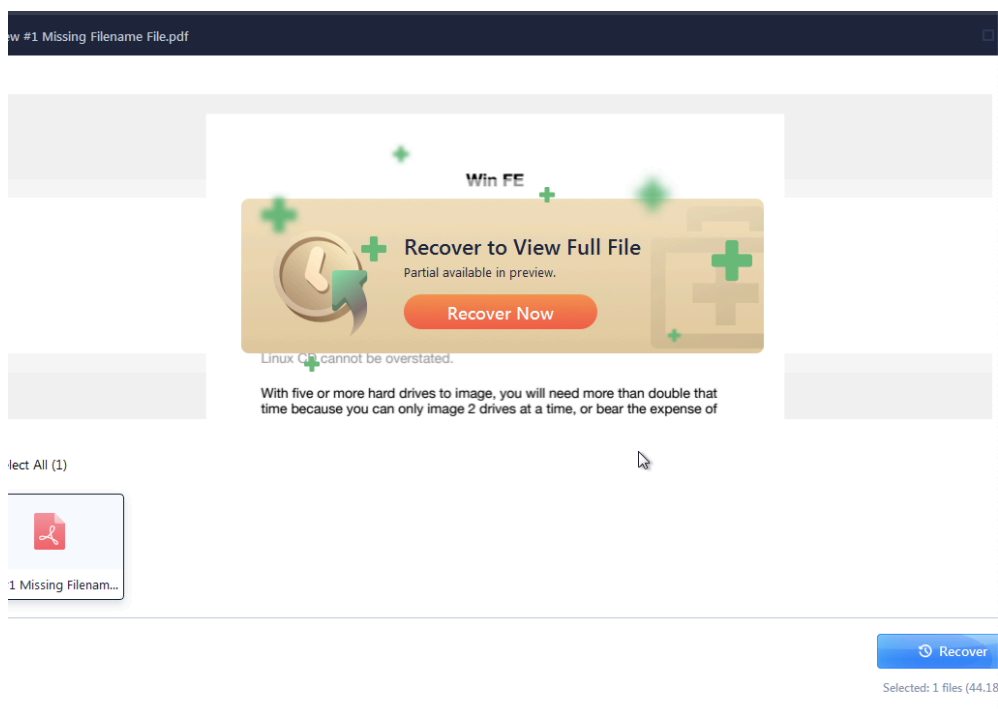
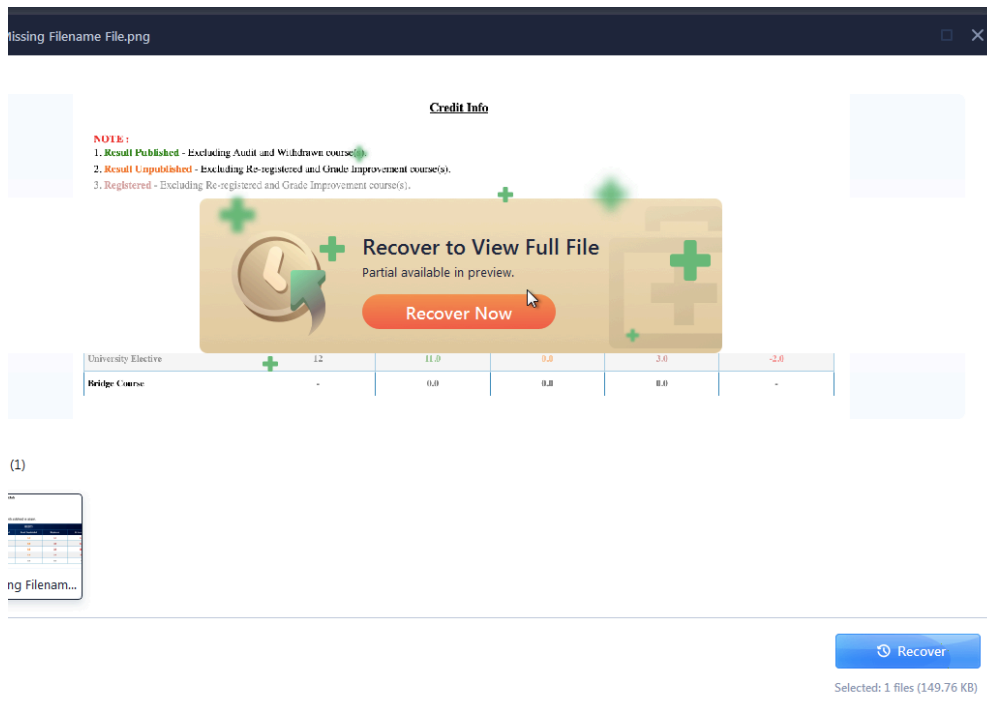


On going through each folder, we can see all the files of that format listed, a few such instances are shown as follows :





We have now seen that the software is able to list out and display all the files, now say we want to retrieve any such file. If we want to do so, we click on the retrieve option after opening these files. This option is better showcased in the pictures below :



Thus the EaseUS software is incredibly useful in retrieving files and folders from deleted partitions which has many applications in Digital forensics in going through the suspect's computers.

Question 3 :

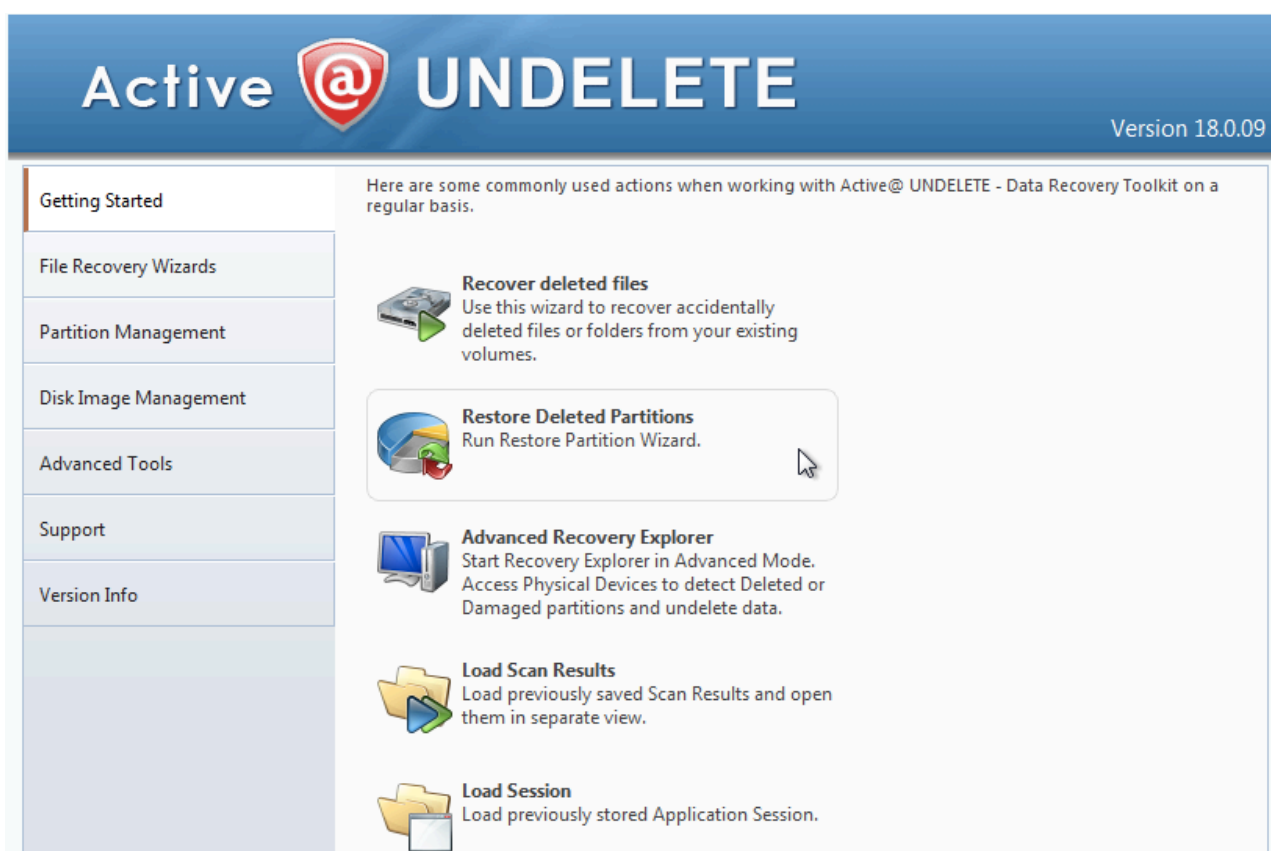
Restoring Lost or Deleted Hard Disk Drive Partition

Download the UnDelete Software application and use it to restore the deleted partition completely.

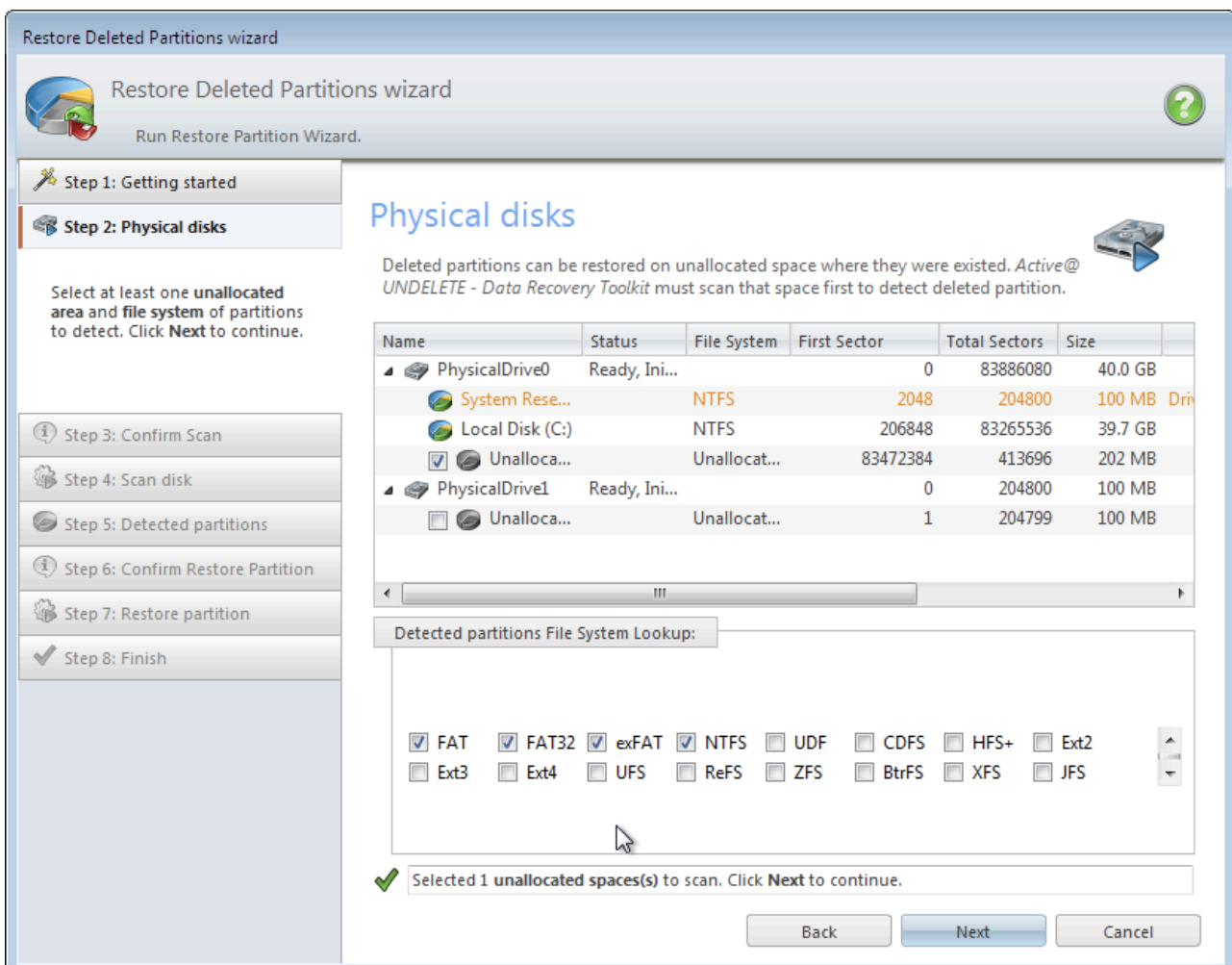
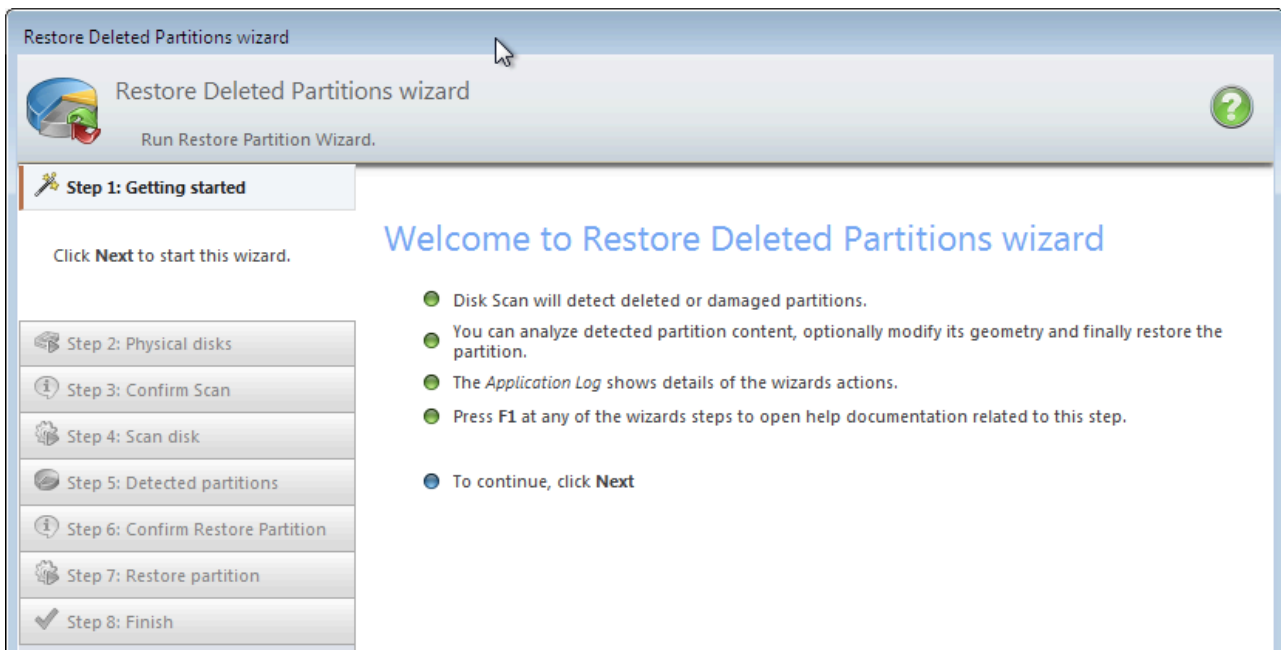
In this portion, we will restore the deleted hard disk partition completely and then access the files from inside this deleted partition just as if the partition was never deleted. For the setup process, we use the same deleted 200MB partition which was created and deleted in the previous portion of the lab.

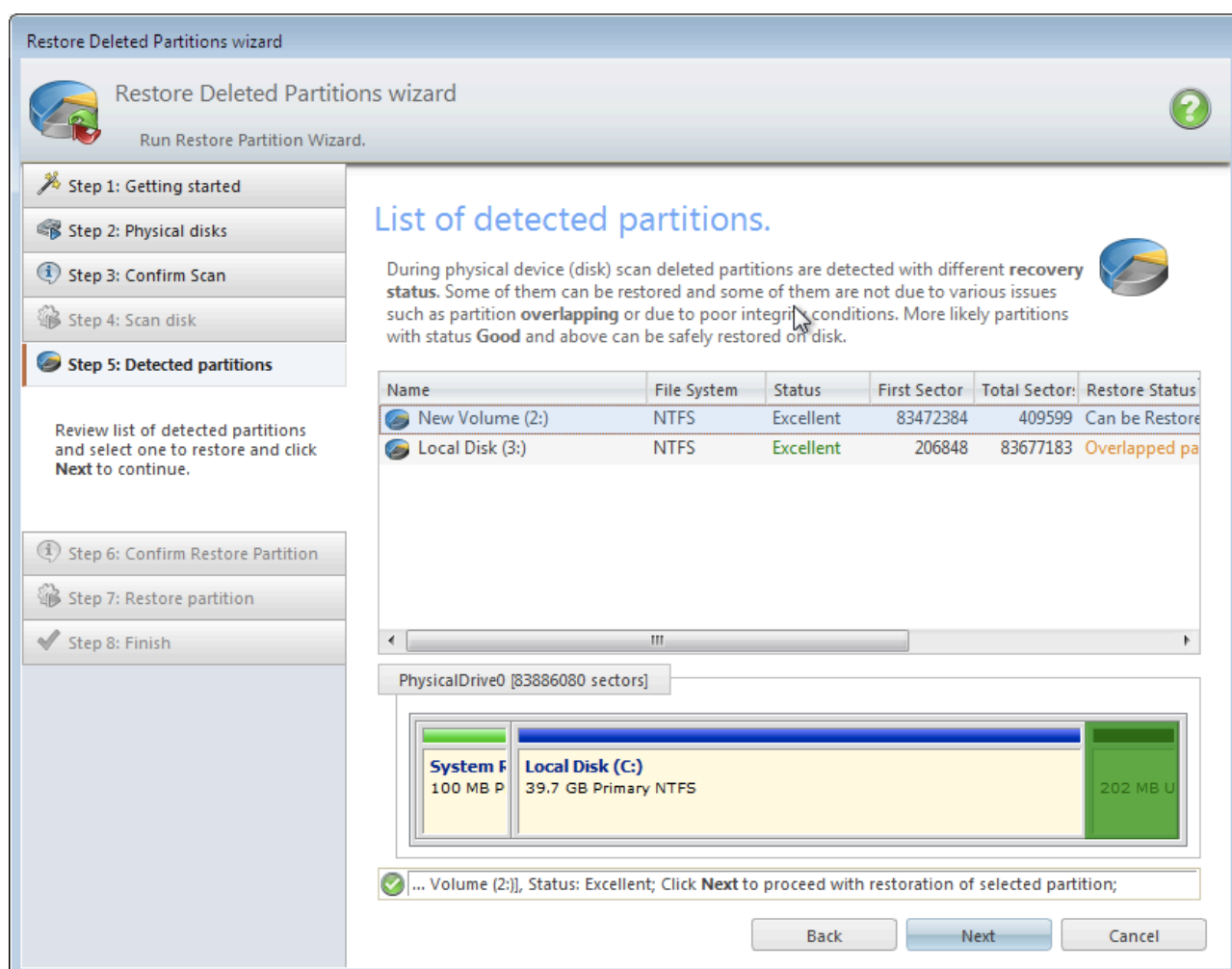
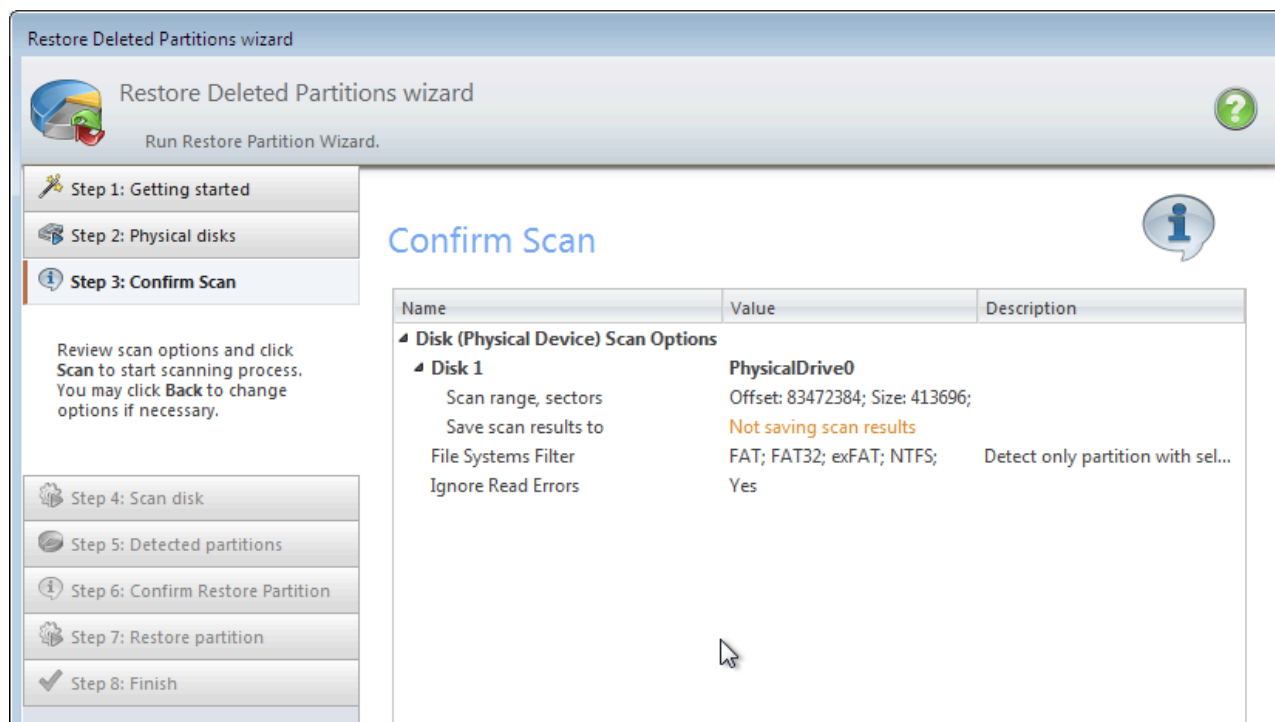
At the end of this portion, we plan to completely restore the deleted partition. For this, we will use the UnDelete partition recovery software. As a setup procedure for this portion, we download and install this software application.

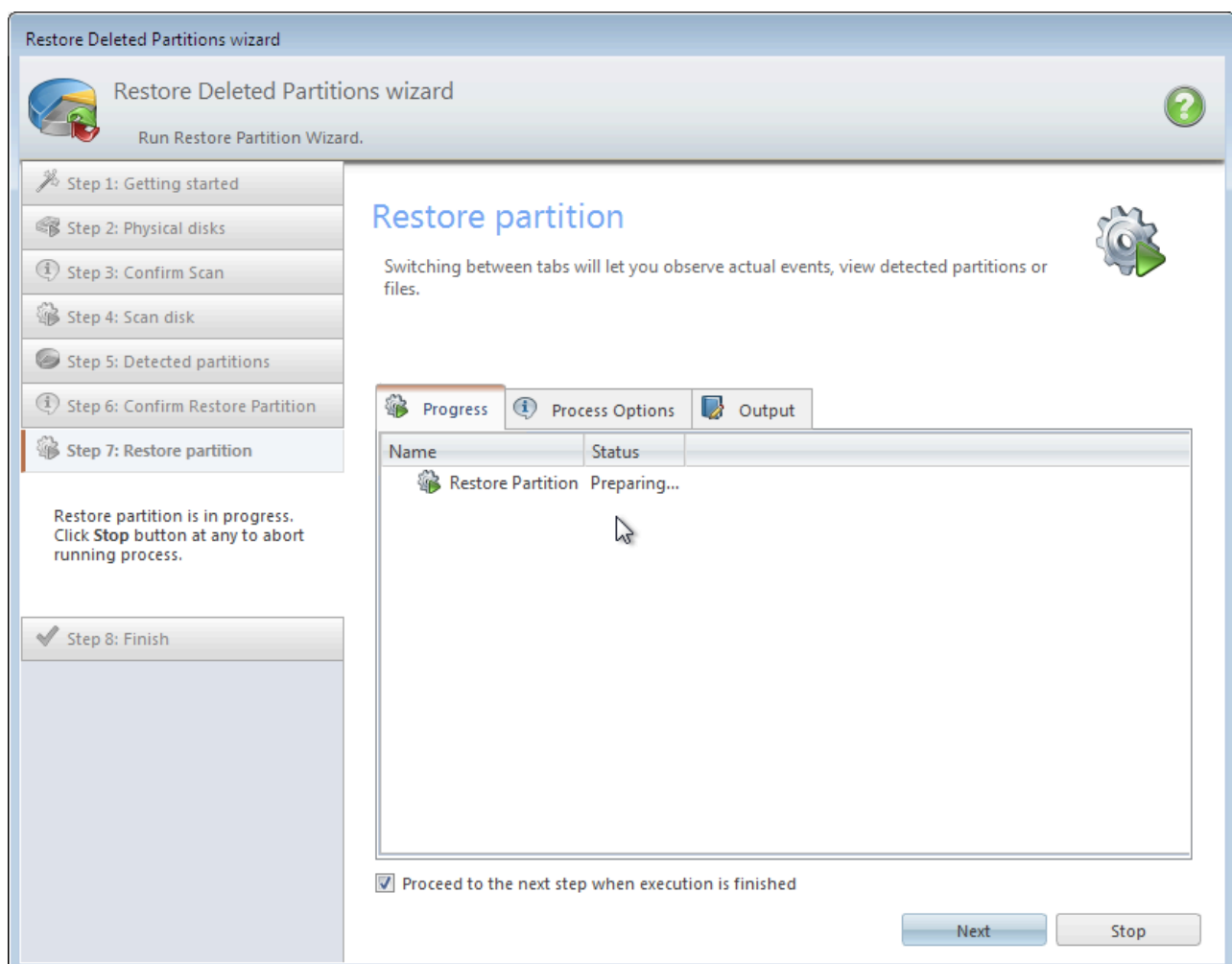
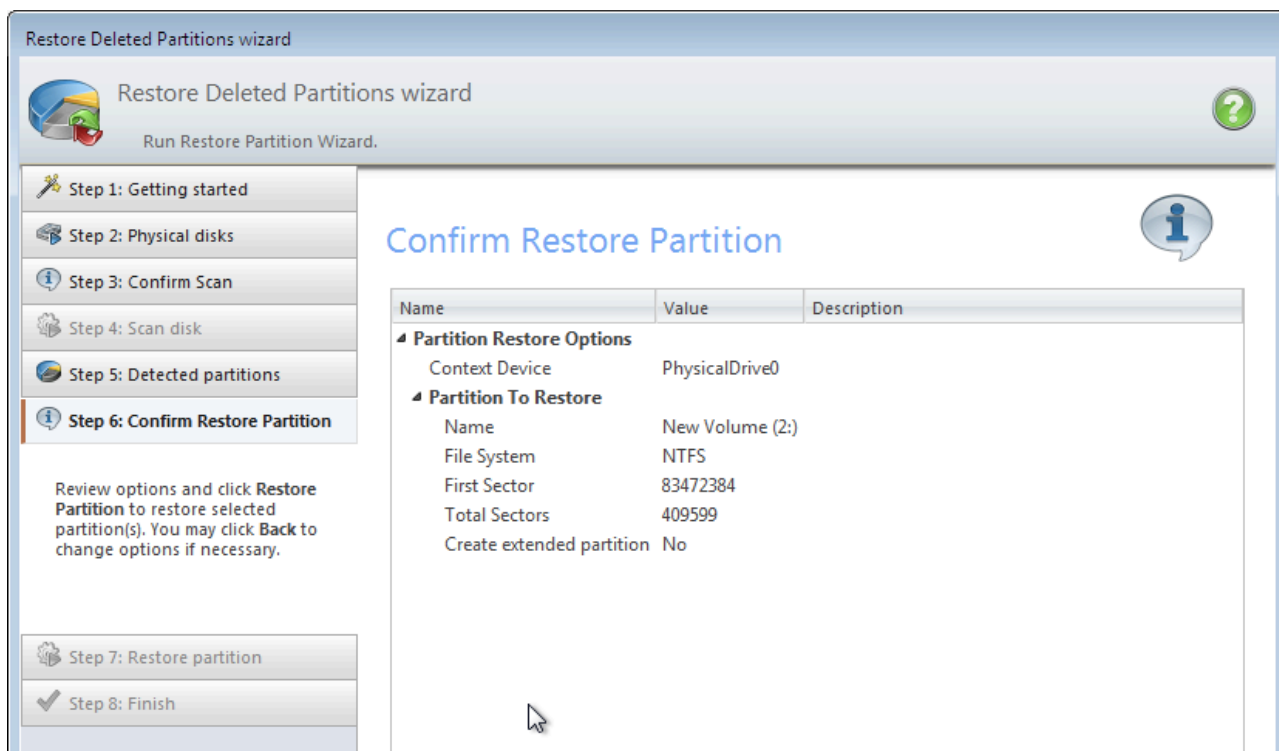
We first ensure that the partition we want to restore has been deleted, we can do this by opening the disk management tool. After this, we open the UnDelete tool, as here our aim is to recover a deleted partition, we choose the “Restore Deleted Partition” option from the home page.



We then go through the wizard, follow the steps in the wizard like choosing the appropriate disks, etc. The steps in the wizard are shown as follows :

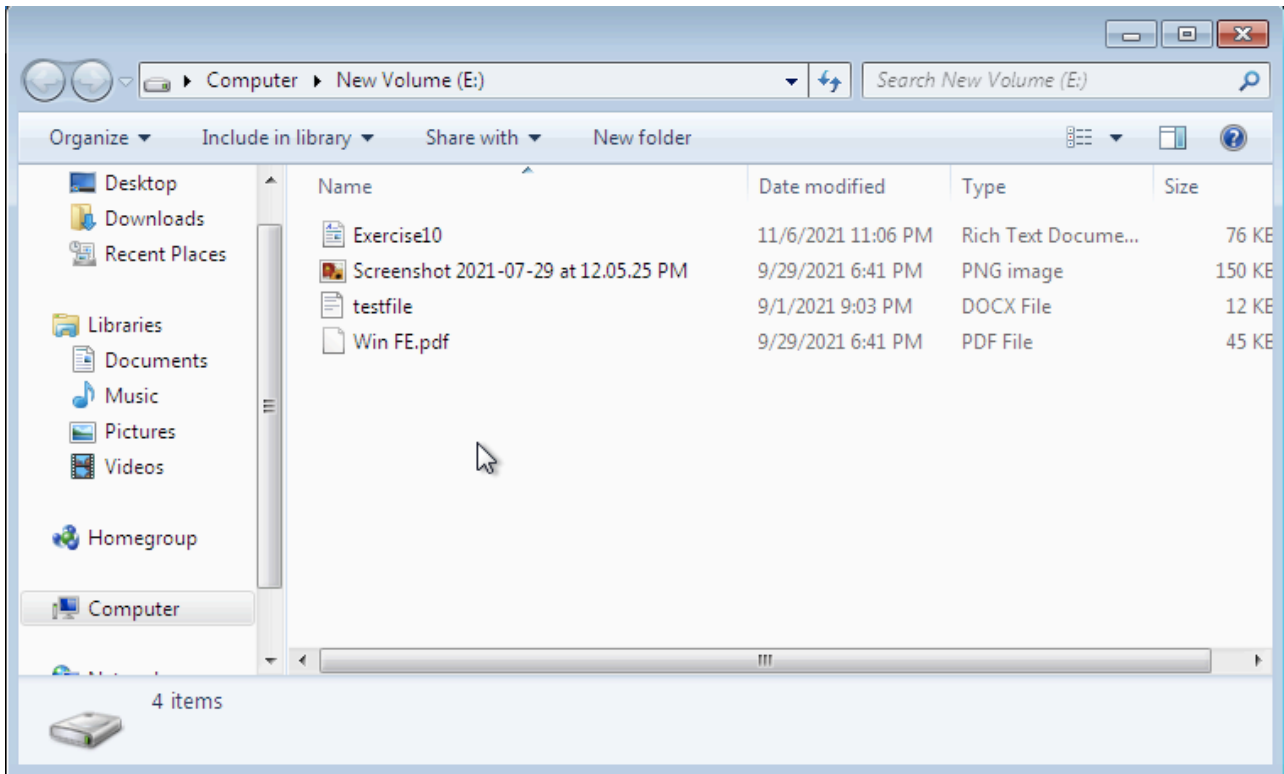






After the completion of the wizard, we can notice that the partition is completely restored with all the identical files and folder structures. It appears just as if we never had deleted the partition earlier.

In our case after the restoration of the partition, we can open it using the file explorer and it looks just identical, and it looks as below :



Thus this UnDelete tool is a major benefit and a useful tool for any digital forensic tool, as it can completely bring a vanished partition back to life with all the files just as if they had not been deleted. It can be used to restore suspects deleted partition where they might try to save hidden data, or even from unallocated space in the middle of the drives which might be bad partitions.

CONCLUSION

In this set of lab experiments, we have dealt with recovering and restoring files from deleted partitions of a hard disk drive and also from partitions which are invisible in standard disk management tools, or are visible as unallocated region due to various reasons ranging from it being corrupted to a suspect hiding confidential data in such regions. Thus these tools serve an important part in the field of digital forensics and help the digital forensic investigators to gain access to hidden regions of the drives and also to retrieve data from such regions which might alter the course of many criminal or civil investigative measures.