Digital Forensics - Lab 11

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

Aadhitya Swarnesh

- 11 November 2021

Question 1 :

File Carving

Many test images are available for performing file carving. For this exercise. take two images from a site and perform file carving.

Include screenshots in your submission.

File carving is the process of reassembling computer files from fragments in the absence of file system metadata. All file systems contain some metadata that describes the actual file system. At a minimum, the following is stored: the hierarchy of folders and files, with names for each. For each file is also kept the physical address on the hard disk where the file is stored. A file might be scattered in fragments at different physical addresses.

File carving is the process of trying to recover files without the metadata. This is done by analysing the raw data and identifying what it is (text, executable, png, mp3, etc.). This can be done in different ways, but the simplest is to look for headers. For instance, every Java class file has as its first four bytes, the hexadecimal value CA FE BA BE. Some files such as pdfs contain footers as well, making it just as simple to identify the ending of the file.

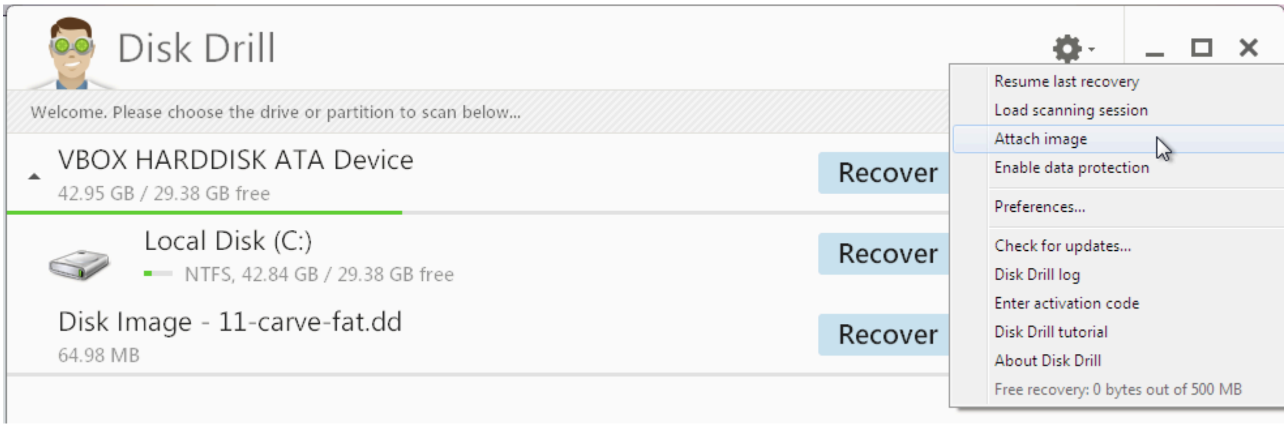
File carving can be used to recover data from a hard disk where the metadata is missing or damaged, especially by professional data recovery companies. When a file is deleted, only the entry in the file system metadata is removed, while the actual data is still on the disk. After a format and even a repartitioning it might be that most of raw data is untouched and can be recovered using file carving. Many carving schemes have been developed. File carving should be done on a disk image, rather than on the original disk. The majority of file carving programs will only recover files that are contiguous on the media (in other words files that are not fragmented).

For the purpose of this lab experiment, we will use the **Disk Drill** to perform file carving from a forensic image file of a suspect's disk. The forensic images can be obtained from this link : http://dftt.sourceforge.net/

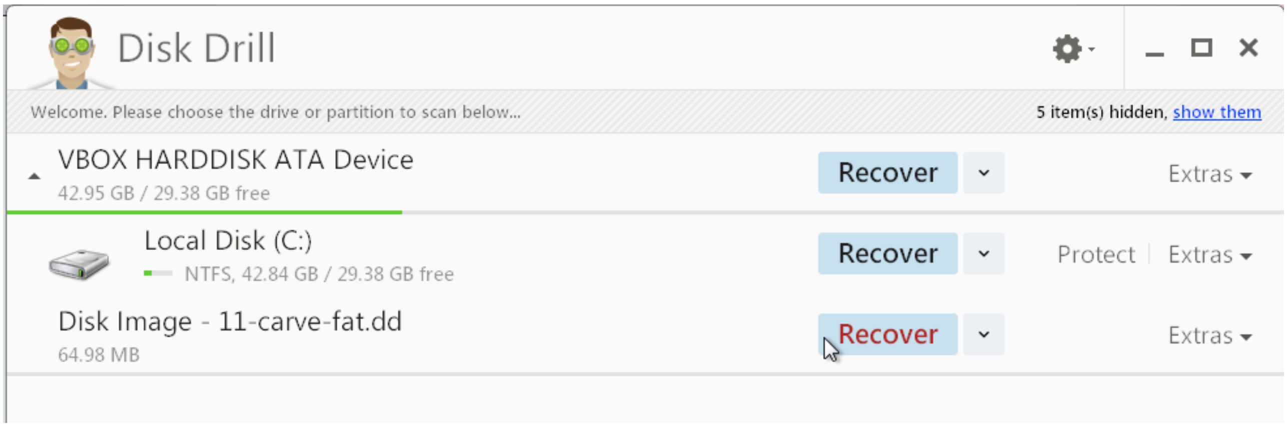
As stated in the question, we will perform the same procedure in two disk images obtained from the previous website. Download the image files which will be in a compressed version, and so extract and save them.

Let us proceed with **carving the first image file** :

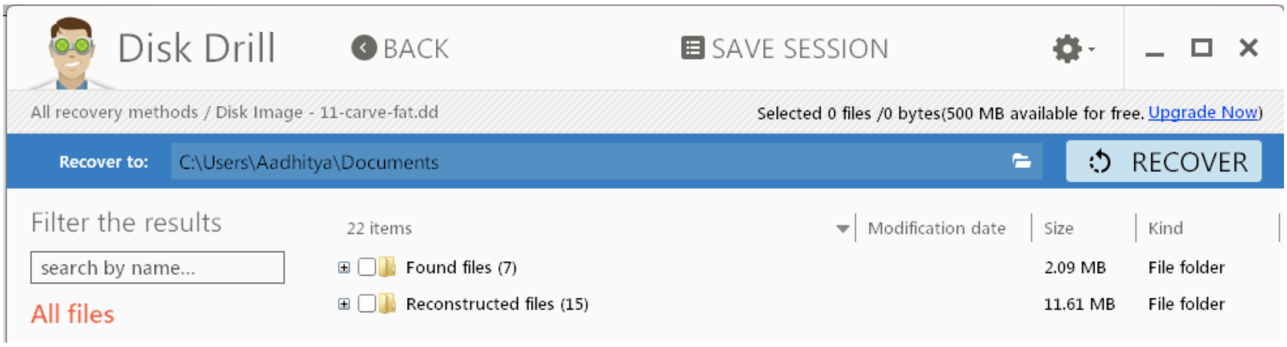
First open the Disk Drill software, and then add the disk image as a source to recover from. It can be done by the options shown as follows :



With this done, we now proceed with recovering the files from this forensic image, and in order to do this, we click on the "Recover" option next to the disk image we need to carve.


Disk Drill
Welcome. Please choose the drive or partition to scan below...
5 item(s) hidden, show them
VBOX HARDDISK ATA Device
42.95 GB / 29.38 GB free
Recover
Extras
Local Disk (C:)
NTFS, 42.84 GB / 29.38 GB free
Recover
Protect
Extras
Disk Image - 11-carve-fat.dd
64.98 MB
Recover
Extras

Once this is done, the application scans over the entire disk and then identifies the files based on the hexadecimal values of headers and footers and then shows these files listed by their file type. In our case, a list of recovered files looks as follows :



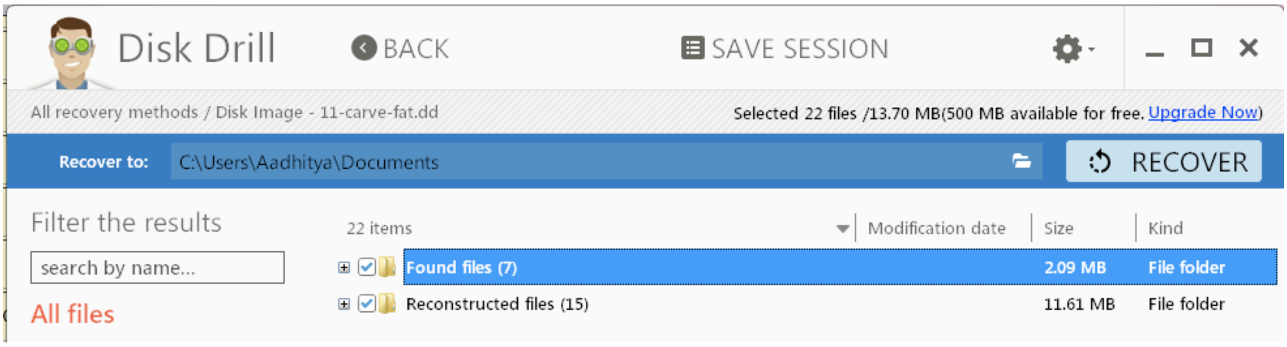
All recovery methods / Disk Image - 11-carve-fat.dd

Selected 0 files /0 bytes(500 MB available for free. Upgrade Now)

Recover to: C:\Users\Aadhitya\Documents

22 items	Modification date	Size	Kind
⊞ □ Found files (7)		2.09 MB	File folder
⊞ □ Reconstructed files (15)		11.61 MB	File folder

We will now click on all the files which need to be recovered and then click on the recover button found above after choosing the detonation where these recovered files need to be placed.



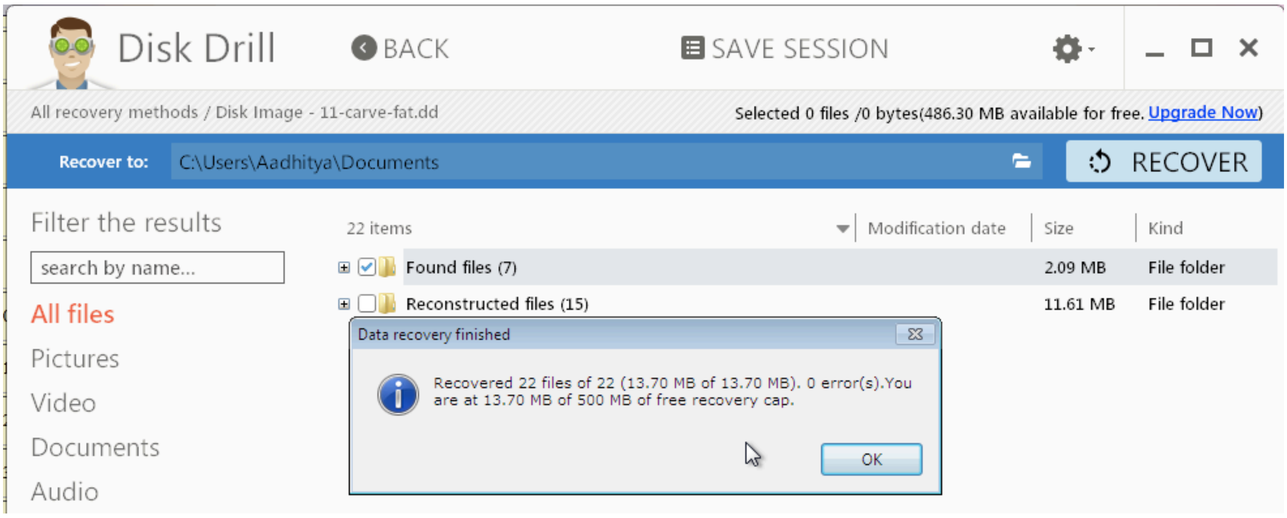
All recovery methods / Disk Image - 11-carve-fat.dd

Selected 22 files /13.70 MB(500 MB available for free. Upgrade Now)

Recover to: C:\Users\Aadhitya\Documents

22 items	Modification date	Size	Kind
⊞ ☑ Found files (7)		2.09 MB	File folder
⊞ ☑ Reconstructed files (15)		11.61 MB	File folder

On clicking this, the recovery process takes place, and the files are saved to the destination mentioned earlier.



All recovery methods / Disk Image - 11-carve-fat.dd

Selected 0 files /0 bytes(486.30 MB available for free. Upgrade Now)

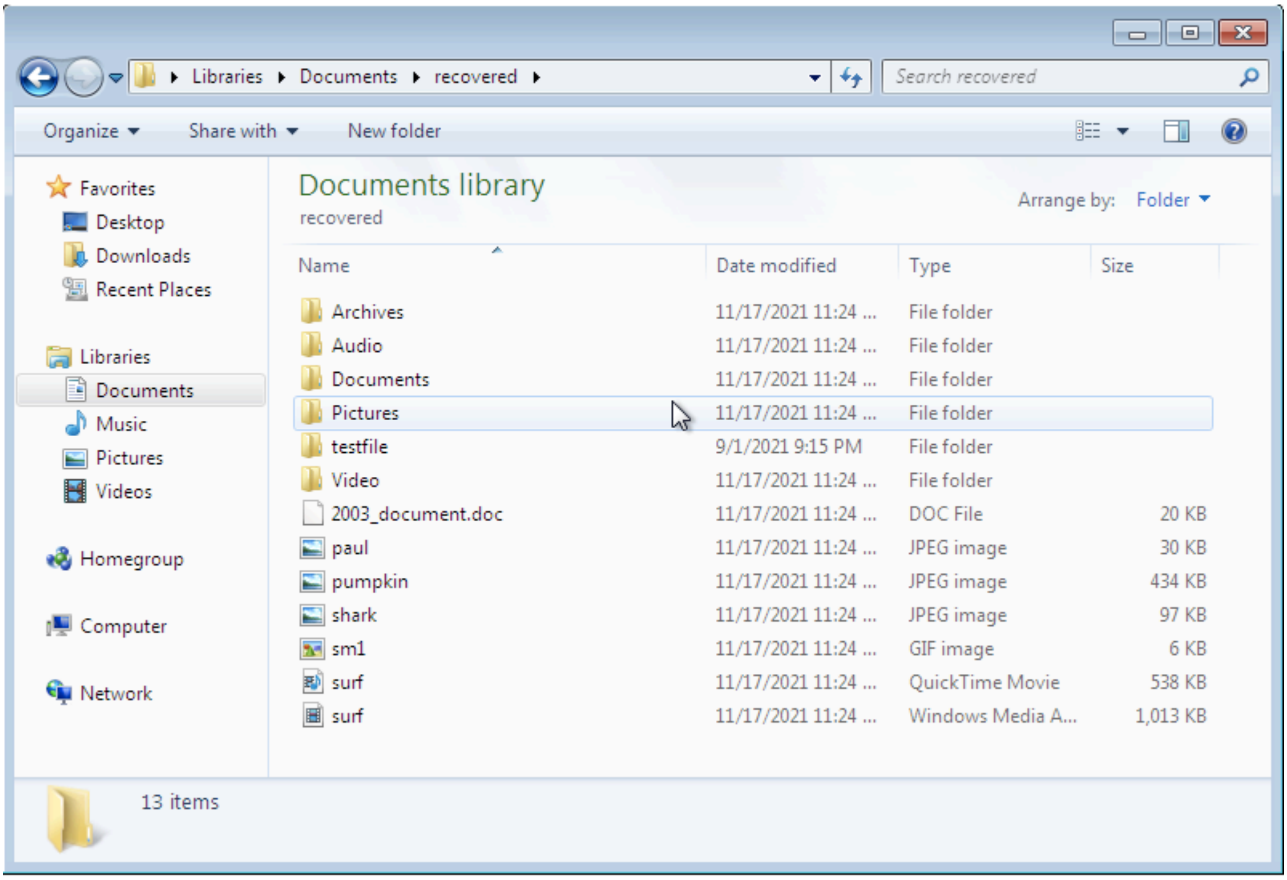
Recover to: C:\Users\Aadhitya\Documents

22 items	Modification date	Size	Kind
⊞ ☑ Found files (7)		2.09 MB	File folder
⊞ □ Reconstructed files (15)		11.61 MB	File folder

Data recovery finished

Recovered 22 files of 22 (13.70 MB of 13.70 MB). 0 error(s).You are at 13.70 MB of 500 MB of free recovery cap.

Now the recovery process is complete and the recovered files are now saved in the destination folder, we can now use the File Explorer to navigate to the destination folder to find the files fully recovered.



Documents library
recovered

Name	Date modified	Type	Size
Archives	11/17/2021 11:24 ...	File folder	
Audio	11/17/2021 11:24 ...	File folder	
Documents	11/17/2021 11:24 ...	File folder	
Pictures	11/17/2021 11:24 ...	File folder	
testfile	9/1/2021 9:15 PM	File folder	
Video	11/17/2021 11:24 ...	File folder	
2003_document.doc	11/17/2021 11:24 ...	DOC File	20 KB
paul	11/17/2021 11:24 ...	JPEG image	30 KB
pumpkin	11/17/2021 11:24 ...	JPEG image	434 KB
shark	11/17/2021 11:24 ...	JPEG image	97 KB
sm1	11/17/2021 11:24 ...	GIF image	6 KB
surf	11/17/2021 11:24 ...	QuickTime Movie	538 KB
surf	11/17/2021 11:24 ...	Windows Media A...	1,013 KB

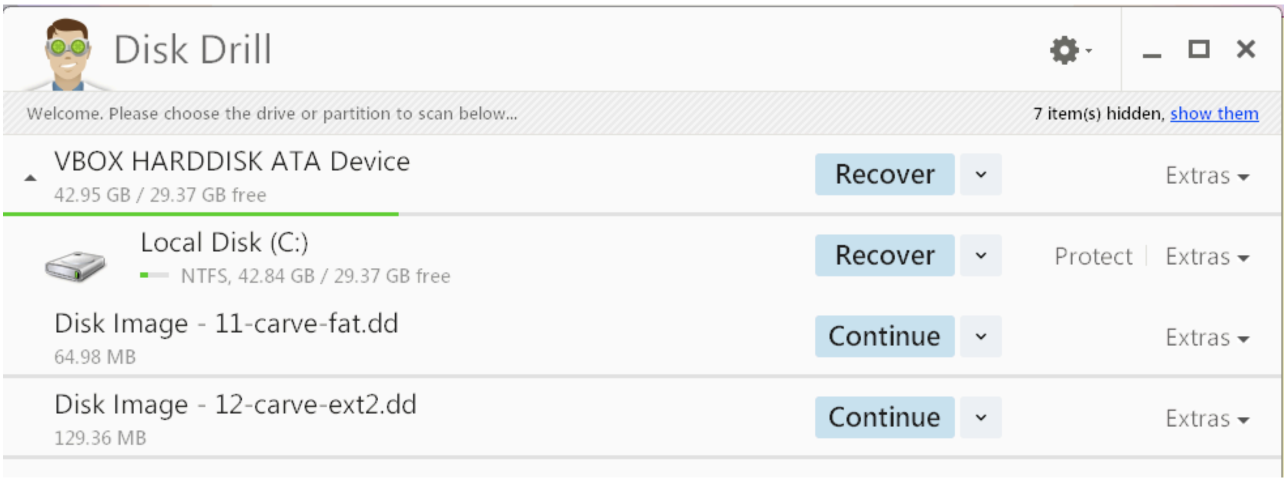
13 items

We can notice here that the files have been completely recovered and are placed in the folder by their file type. We can now open these files by their appropriate applications and view their content.

We have thus performed file carving on an disk image, we will now take up another disk image and perform the same procedure.

Let us proceed with **carving the second image file** :

First open the Disk Drill software, and then add the disk image as a source to recover from. It can be done by the options shown as follows :

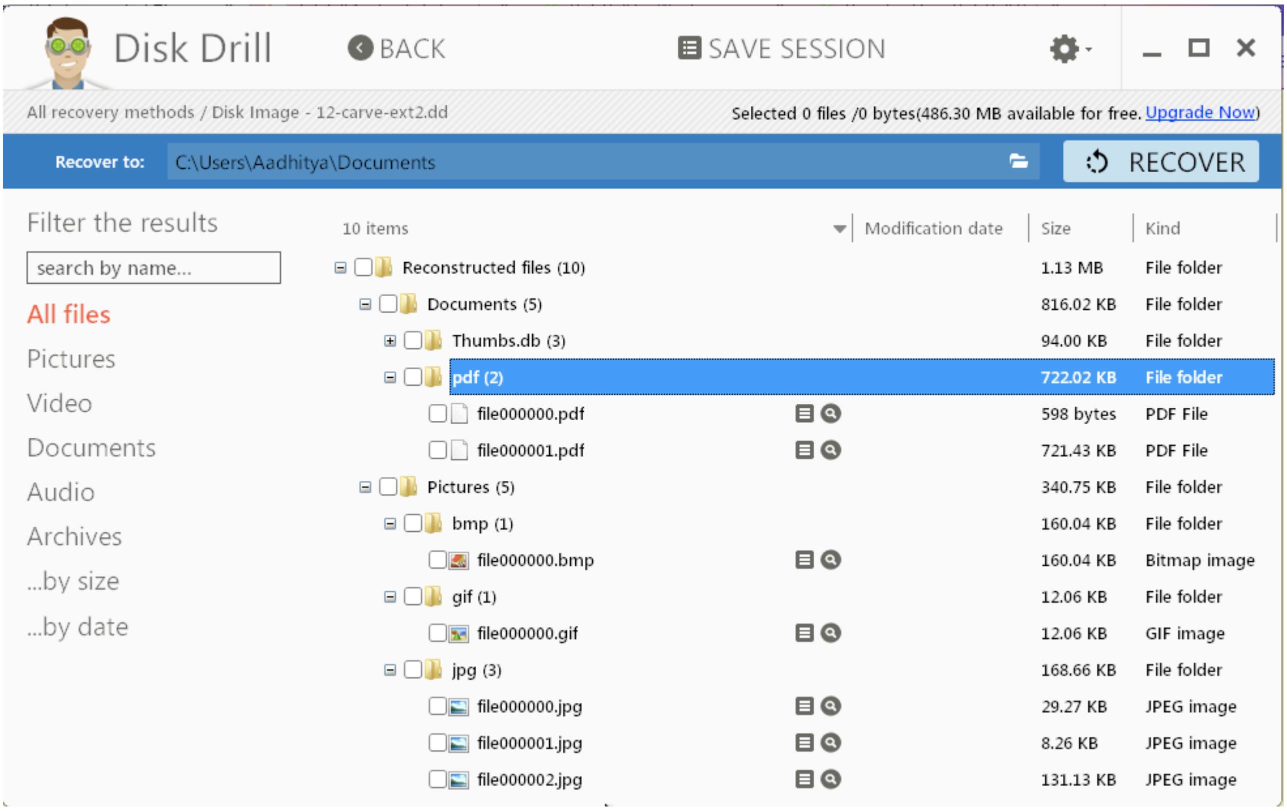


Welcome. Please choose the drive or partition to scan below... 7 item(s) hidden, show them

VBOX HARDDISK ATA Device 42.95 GB / 29.37 GB free	Recover	Extras
Local Disk (C:) NTFS, 42.84 GB / 29.37 GB free	Recover	Protect | Extras
Disk Image - 11-carve-fat.dd 64.98 MB	Continue	Extras
Disk Image - 12-carve-ext2.dd 129.36 MB	Continue	Extras

With this done, we now proceed with recovering the files from this forensic image, and in order to do this, we click on the “Recover” option next to the disk image we need to carve.

Once this is done, the application scans over the entire disk and then identifies the files based on the hexadecimal values of headers and footers and then shows these files listed by their file type. In our case, a list of recovered files looks as follows :



All recovery methods / Disk Image - 12-carve-ext2.dd

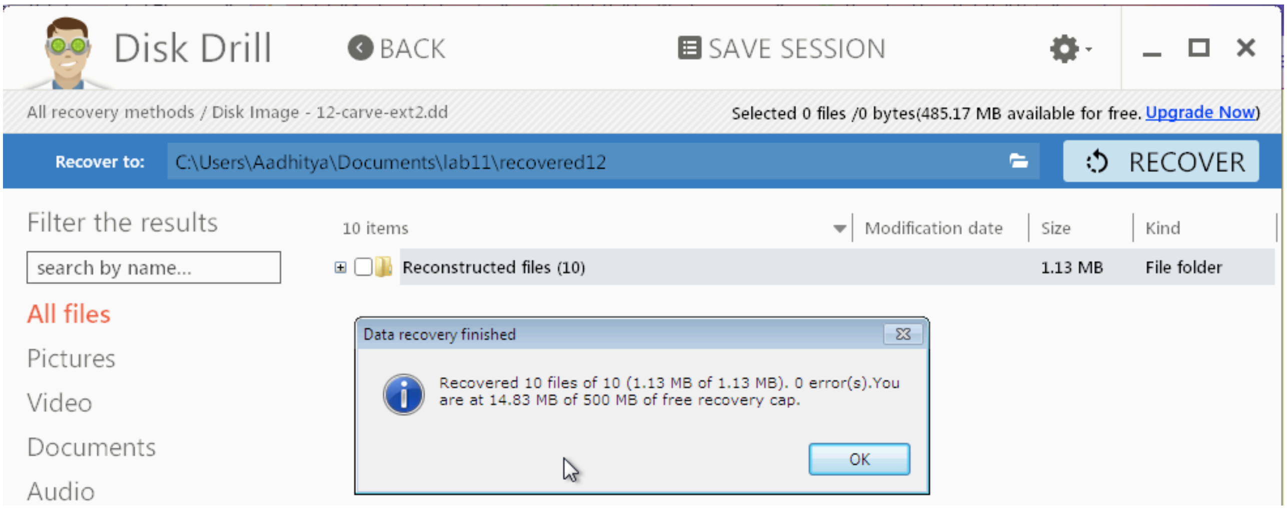
Selected 0 files /0 bytes(486.30 MB available for free. Upgrade Now)

Recover to: C:\Users\Aadhitya\Documents

10 items	Modification date	Size	Kind
⊟ □ Reconstructed files (10)		1.13 MB	File folder
⊟ □ Documents (5)		816.02 KB	File folder
⊞ □ Thumbs.db (3)		94.00 KB	File folder
⊟ □ pdf (2)		722.02 KB	File folder
□ file000000.pdf		598 bytes	PDF File
□ file000001.pdf		721.43 KB	PDF File
⊟ □ Pictures (5)		340.75 KB	File folder
⊟ □ bmp (1)		160.04 KB	File folder
□ file000000.bmp		160.04 KB	Bitmap image
⊟ □ gif (1)		12.06 KB	File folder
□ file000000.gif		12.06 KB	GIF image
⊟ □ jpg (3)		168.66 KB	File folder
□ file000000.jpg		29.27 KB	JPEG image
□ file000001.jpg		8.26 KB	JPEG image
□ file000002.jpg		131.13 KB	JPEG image

We will now click on all the files which need to be recovered and then click on the recover button found above after choosing the detonation where these recovered files need to be placed.

On clicking this, the recovery process takes place, and the files are saved to the destination mentioned earlier.



Selected 0 files /0 bytes(485.17 MB available for free.

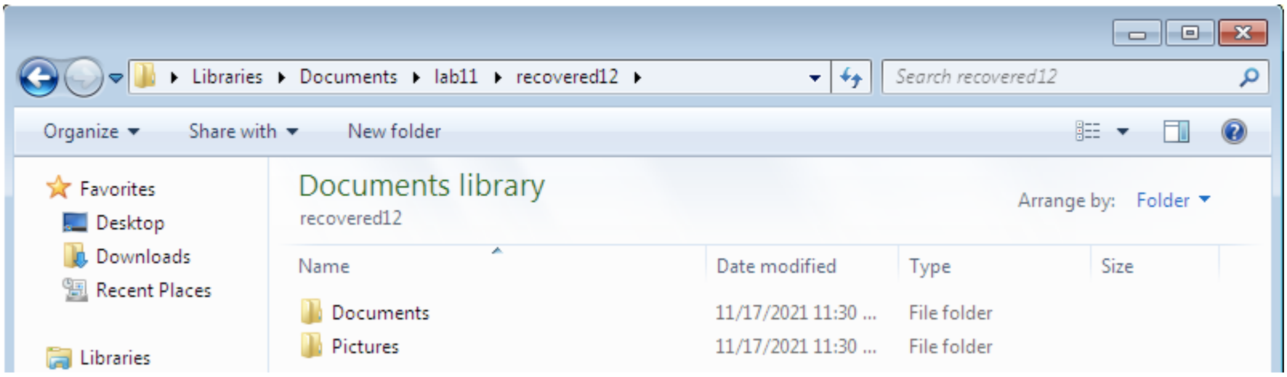
Recover to: C:\Users\Aadhitya\Documents\lab11\recovered12

10 items	Modification date	Size	Kind
Reconstructed files (10)		1.13 MB	File folder

Data recovery finished

Recovered 10 files of 10 (1.13 MB of 1.13 MB). 0 error(s).You are at 14.83 MB of 500 MB of free recovery cap.

Now the recovery process is complete and the recovered files are now saved in the destination folder, we can now use the File Explorer to navigate to the destination folder to find the files fully recovered.



Name	Date modified	Type	Size
Documents	11/17/2021 11:30 ...	File folder	
Pictures	11/17/2021 11:30 ...	File folder	

We can notice here that the files have been completely recovered and are placed in the folder by their file type. We can now open these files by their appropriate applications and view their content.

We have thus performed file carving on another disk image, we can thus use the same procedure to carve up any forensic disk image and extract the files from within.

Question 2 :

File Carving

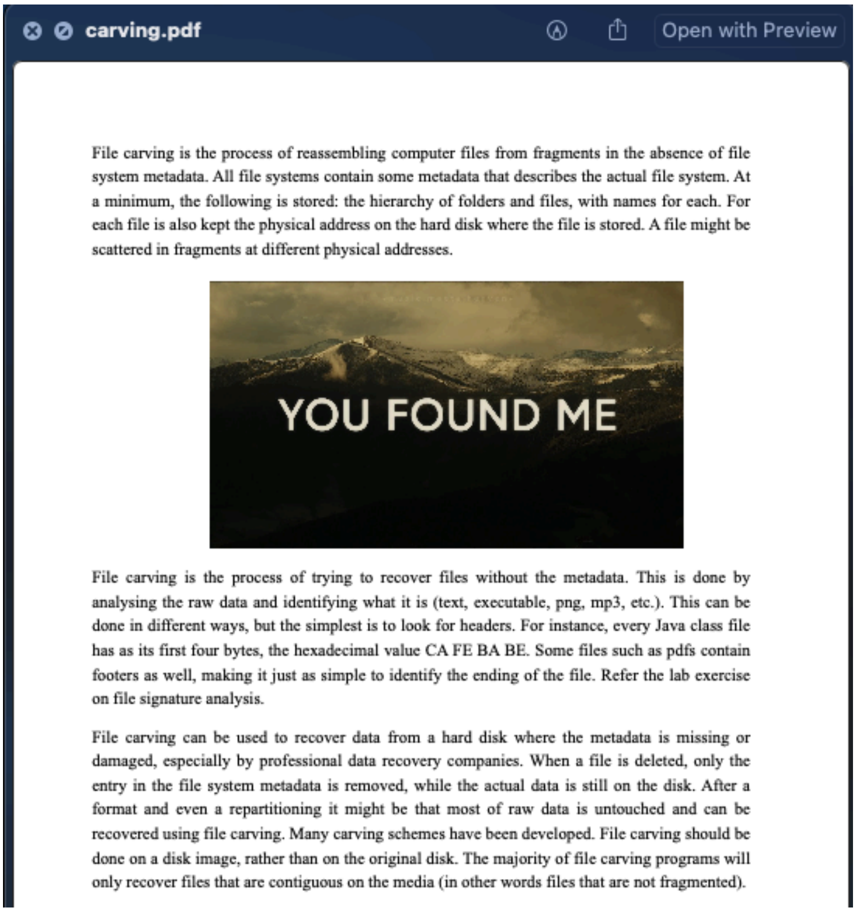
Create a document with text and images, and then perform file carving to extract and save the image without using any file carving tools.

Include screenshots in your submission.

File carving usually takes place by observing the header and the footer values of the individual files inside the image. This is because each file type have their own header and footer values. For example the file header of a jpeg image starts with **FFD8** and its footer ends with **FFD9**. With these values, we can parse through the hexadecimal version of the file to extract the region which coincides with this format, in order to extract essentially the file from within another file.

We will use the WinHex Hexadecimal editor in order to extract an image in jpeg format from within a text document in docx format.

We shall first prepare the document, with some text and the image. In our case the prepared document looks as follows :

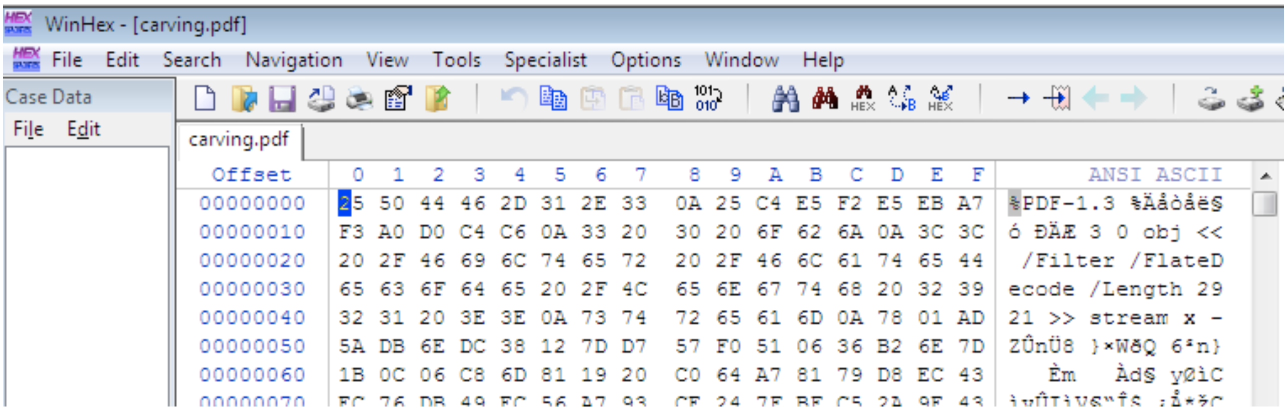


File carving is the process of reassembling computer files from fragments in the absence of file system metadata. All file systems contain some metadata that describes the actual file system. At a minimum, the following is stored: the hierarchy of folders and files, with names for each. For each file is also kept the physical address on the hard disk where the file is stored. A file might be scattered in fragments at different physical addresses.

File carving is the process of trying to recover files without the metadata. This is done by analysing the raw data and identifying what it is (text, executable, png, mp3, etc.). This can be done in different ways, but the simplest is to look for headers. For instance, every Java class file has as its first four bytes, the hexadecimal value CA FE BA BE. Some files such as pdfs contain footers as well, making it just as simple to identify the ending of the file. Refer the lab exercise on file signature analysis.

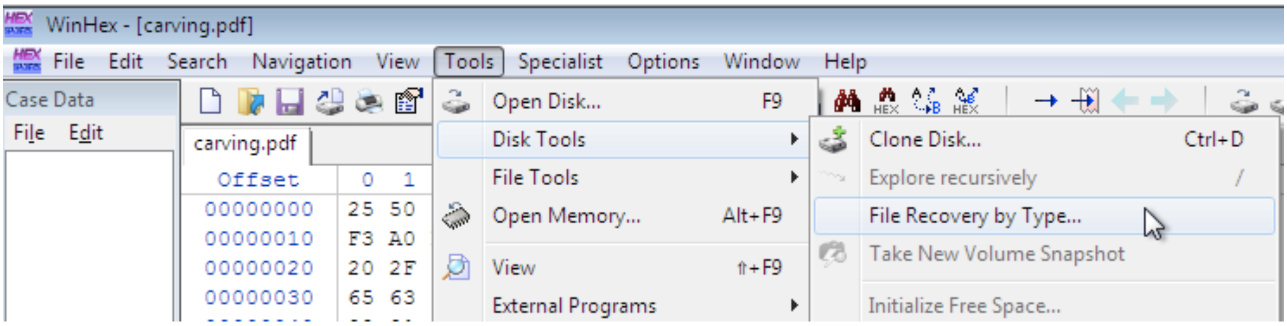
File carving can be used to recover data from a hard disk where the metadata is missing or damaged, especially by professional data recovery companies. When a file is deleted, only the entry in the file system metadata is removed, while the actual data is still on the disk. After a format and even a repartitioning it might be that most of raw data is untouched and can be recovered using file carving. Many carving schemes have been developed. File carving should be done on a disk image, rather than on the original disk. The majority of file carving programs will only recover files that are contiguous on the media (in other words files that are not fragmented).

With this done, we shall open this inside the WinHex editor and view the file in a hexadecimal format.

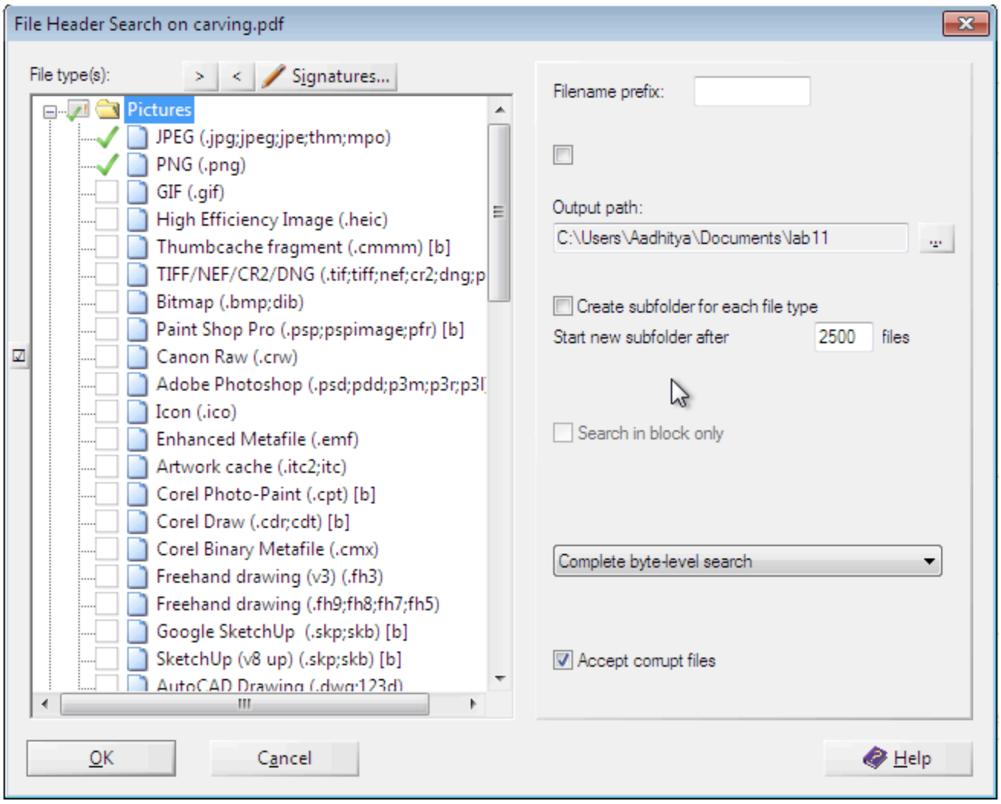

WinHex - [carving.pdf]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
carving.pdf

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F       ANSI ASCII
00000000   25 50 44 46 2D 31 2E 33  0A 25 C4 E5 F2 E5 EB A7   %PDF-1.3 %ÄåòåëS
00000010   F3 A0 D0 C4 C6 0A 33 20  30 20 6F 62 6A 0A 3C 3C   ó ÐÄÆ 3 0 obj <<
00000020   20 2F 46 69 6C 74 65 72  20 2F 46 6C 61 74 65 44    /Filter /FlateD
00000030   65 63 6F 64 65 20 2F 4C  65 6E 67 74 68 20 32 39   ecode /Length 29
00000040   32 31 20 3E 3E 0A 73 74  72 65 61 6D 0A 78 01 AD   21 >> stream x -
00000050   5A DB 6E DC 38 12 7D D7  57 F0 51 06 36 B2 6E 7D   ZÛnÜ8 }×WðQ 6²n}
00000060   1B 0C 06 C8 6D 81 19 20  C0 64 A7 81 79 D8 EC 43     Èm   Àd§ yØìC
00000070   FC 76 DB 49 FC 56 A7 93  CF 24 7F BF C5 2A 9F 43
```

We will now head over to the tools and then to the option which lets us to recover files by the file type. The option is shown as follows :



In the next step, we will mention the type of files we suspect to be inside the document, so that the editor searches only for those patterns. We also mention the output folder where the carved files needs to be placed.



File Header Search on carving.pdf

File type(s):

- ☑ Pictures
  - ✓ JPEG (.jpg;jpeg;jpe;thm;mpo)
  - ✓ PNG (.png)
  - □ GIF (.gif)
  - □ High Efficiency Image (.heic)
  - □ Thumbcache fragment (.cmmm) [b]
  - □ TIFF/NEF/CR2/DNG (.tif;tiff;nef;cr2;dng;p
  - □ Bitmap (.bmp;dib)
  - □ Paint Shop Pro (.psp;pspimage;pfr) [b]
  - □ Canon Raw (.crw)
  - □ Adobe Photoshop (.psd;pdd;p3m;p3r;p3l
  - □ Icon (.ico)
  - □ Enhanced Metafile (.emf)
  - □ Artwork cache (.itc2;itc)
  - □ Corel Photo-Paint (.cpt) [b]
  - □ Corel Draw (.cdr;cdt) [b]
  - □ Corel Binary Metafile (.cmx)
  - □ Freehand drawing (v3) (.fh3)
  - □ Freehand drawing (.fh9;fh8;fh7;fh5)
  - □ Google SketchUp (.skp;skb) [b]
  - □ SketchUp (v8 up) (.skp;skb) [b]
  - □ AutoCAD Drawing (.dwg;123d)

Filename prefix:

□

Output path: C:\Users\Aadhitya\Documents\lab11

□ Create subfolder for each file type

Start new subfolder after 2500 files

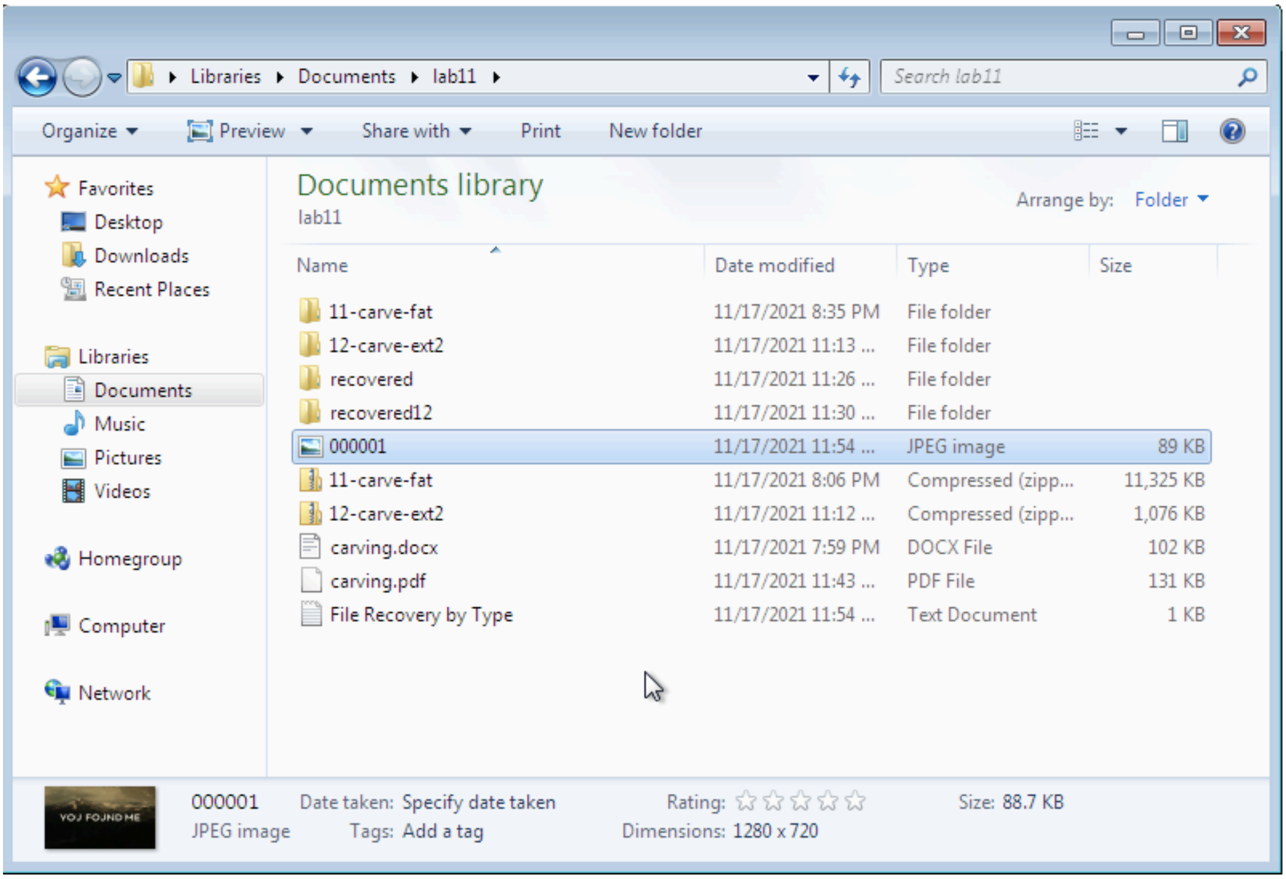
□ Search in block only

Complete byte-level search

☑ Accept corrupt files

With these specified, we proceed to carve these files. We click on the OK button, and then the file carving proceeds and finds our image from within the file, extracts it and then saved it in the destination we specified earlier. We can now use the File explorer to navigate to the destination folder and view the file.

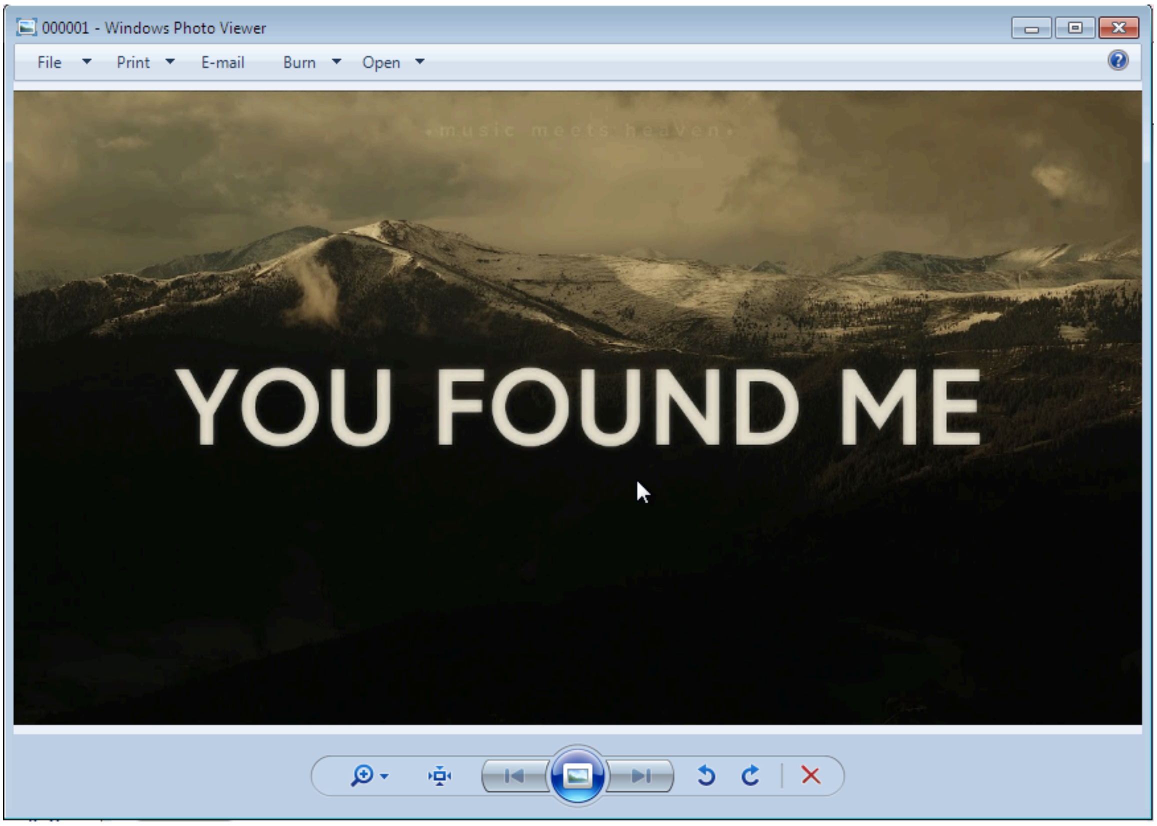
In our current case the image file can be viewed using the file explorer as follows :



Name	Date modified	Type	Size
11-carve-fat	11/17/2021 8:35 PM	File folder	
12-carve-ext2	11/17/2021 11:13 ...	File folder	
recovered	11/17/2021 11:26 ...	File folder	
recovered12	11/17/2021 11:30 ...	File folder	
000001	11/17/2021 11:54 ...	JPEG image	89 KB
11-carve-fat	11/17/2021 8:06 PM	Compressed (zipp...	11,325 KB
12-carve-ext2	11/17/2021 11:12 ...	Compressed (zipp...	1,076 KB
carving.docx	11/17/2021 7:59 PM	DOCX File	102 KB
carving.pdf	11/17/2021 11:43 ...	PDF File	131 KB
File Recovery by Type	11/17/2021 11:54 ...	Text Document	1 KB

000001 JPEG image
Date taken: Specify date taken
Tags: Add a tag
Rating: ☆☆☆☆☆
Dimensions: 1280 x 720
Size: 88.7 KB

We can now open this file using any image viewer to open and view this file. If we open this image, it looks as follows :



We have thus performed a file carving process without using any file carving tools, but relying on just a hexadecimal tool. This can be used in cases we do not have access to any file carving tools readily.

CONCLUSION

In this set of lab experiments, we have dealt with file and data carving to recover hidden files from within other files, or to recover files from partitions or disk images 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 data and also to retrieve this said data from such regions which might alter the course of many criminal or civil investigative measures.