
Digital Forensics - Lab 13

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

Aadhitya Swarnesh

- 25 November 2021

Question 1 :

Hiding entire partitions

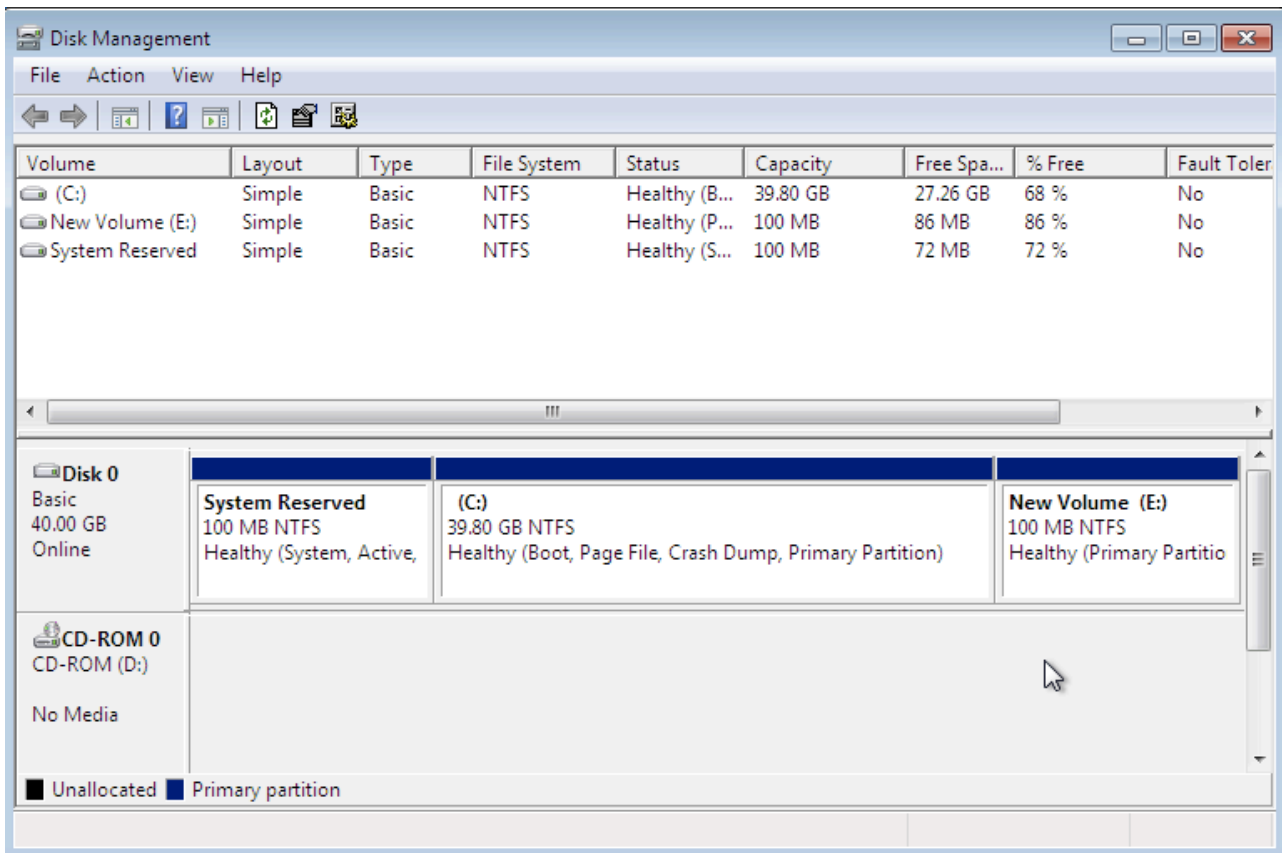
Hide an entire partition in windows, and elaborate on how we can find such partitions.

By using the Windows **diskpart** remove letter command you can un-assign the partition's letter, which hides it from view in File Explorer. To unhide, use the diskpart assign letter command. Some tools such as Partition Magic, Partition Master, and Linux Grand Unified Bootloader (GRUB) are also useful for hiding or revealing partitions. To detect whether a partition has been hidden :

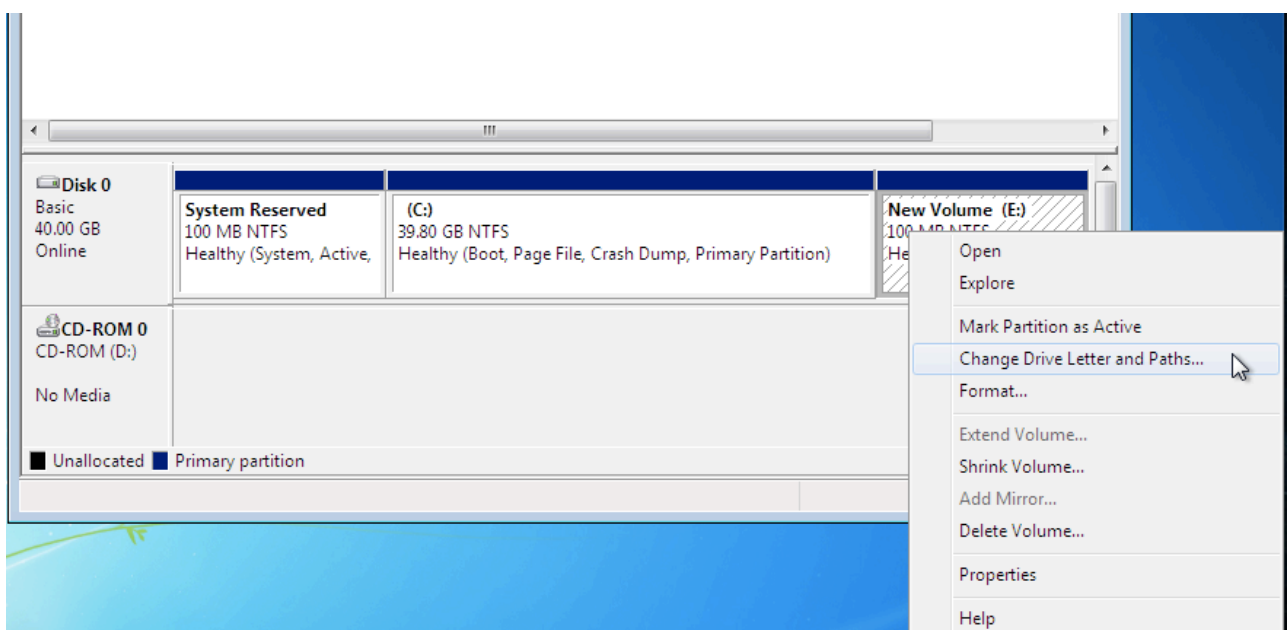
- account for all disk space when examining an evidence drive
- analyze any disk areas containing space you can't account for.

Let us now proceed with creating a new partition and then un-assigning its letter, so as to effectively make it disappear from the Explorer. For this implementation, we will be using a Windows 7 Professional version. The complete hard disk has a total space of 40 GB.

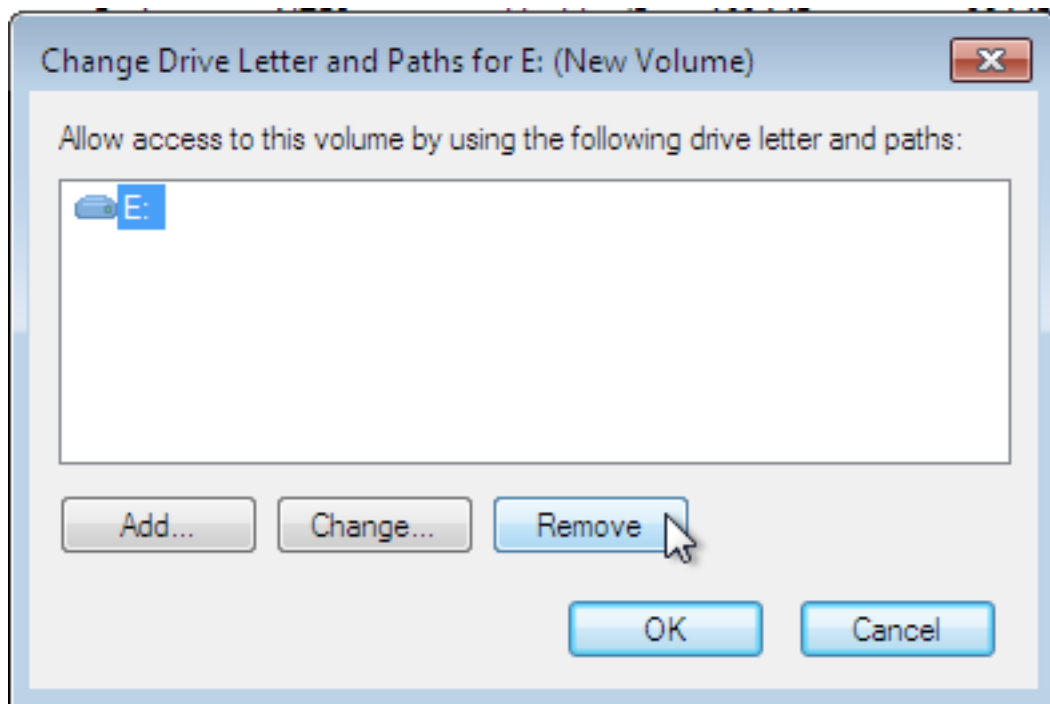
As a first step, we will create a new partition of say 100MB and assign the letter E, to it, so as to have it as a separate partition. This newly created partition can be viewed below :



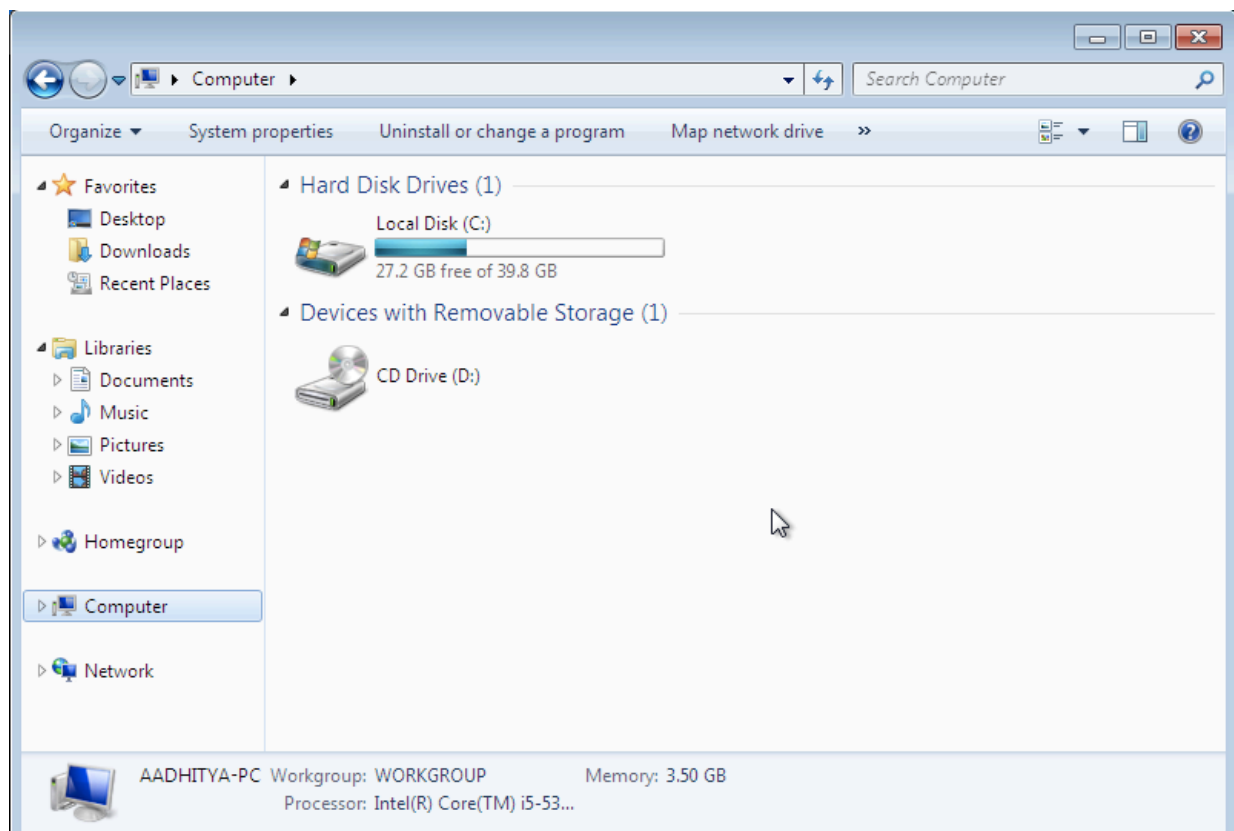
With this partition created and it is visible now, and can be used in a normal manner. Let us now remove the assigned letter in this E - drive. In order to do this, we right click on this partition and select the "Change Drive Letter and path".



On selecting this option, we get a new dialog box, and here we select the assigned drive letter and click on remove. This step is shown in the following image :



With this done, the partition has been un-assigned with the letter, and is now invisible in the Windows Explorer. We can see from the below image that the E-drive is not visible to the windows explorer.



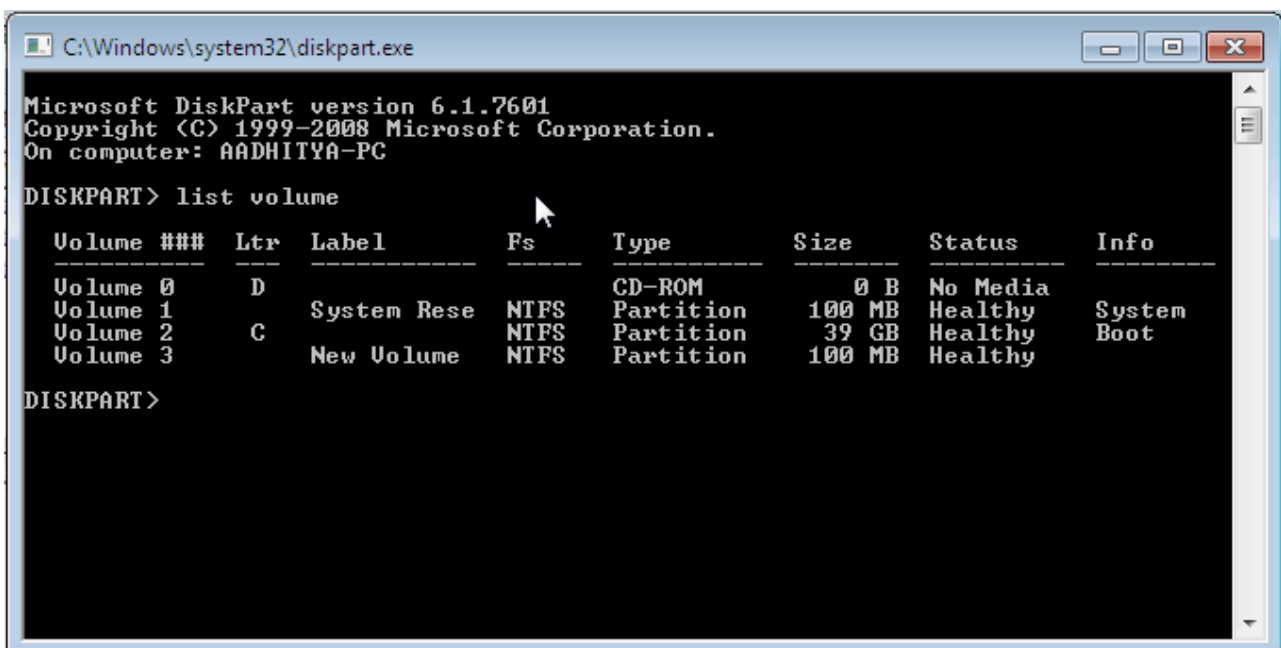
But you can yet notice that the size of the other partition is still missing the 100 MB which we had allocated to the other partition which is now not visible. It is thus this way that data is hidden in partitions which are invisible to the file managers. In order to detect such aspects, we can add up the total space of all the partitions and then compare this value with the total size of the physical hard disk drive. Any inconsistencies in these values will denote the existence of any such partitions.

These petitions will be visible in the Windows disk manager however, and we can assign any letter to these partitions and thereby mount it and open it using the Explorer. We can also detect such partitions using the “diskpart” tool in windows.

In order to use this cli tool, open command prompt and type “diskpart” to open the tool. Then type this command there to view all the partitions and volumes in the disk :

>> list volume

We can view the same in the following image, that there is a partition with the assigned space of 100MB but with no assigned letter.



```
C:\Windows\system32\diskpart.exe
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: AADHITYA-PC

DISKPART> list volume

  Volume ###  Ltr  Label          Fs      Type          Size      Status       Info
  -----
  Volume 0                D             CD-ROM          0 B      No Media
  Volume 1                System Rese    NTFS    Partition     100 MB    Healthy      System
  Volume 2                C             New Volume     NTFS    Partition     39 GB      Healthy      Boot
  Volume 3

DISKPART>
```

Thus we can use this strategy to detect any hidden partitions in the suspect’s disk and drives in case we find any inconsistencies in the amount of occupied space in the disk, as this is a common way in which suspects hide data in their computers.

Question 2 :

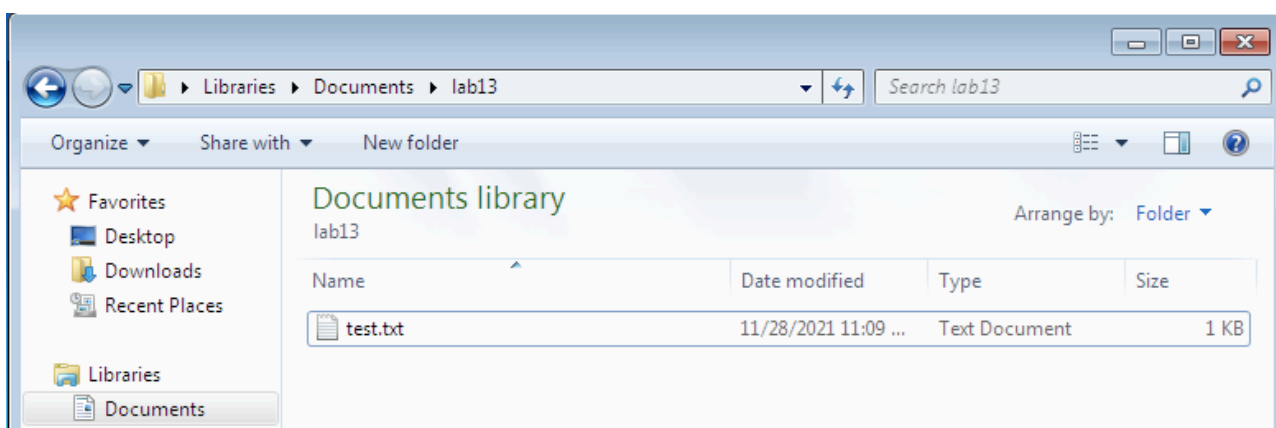
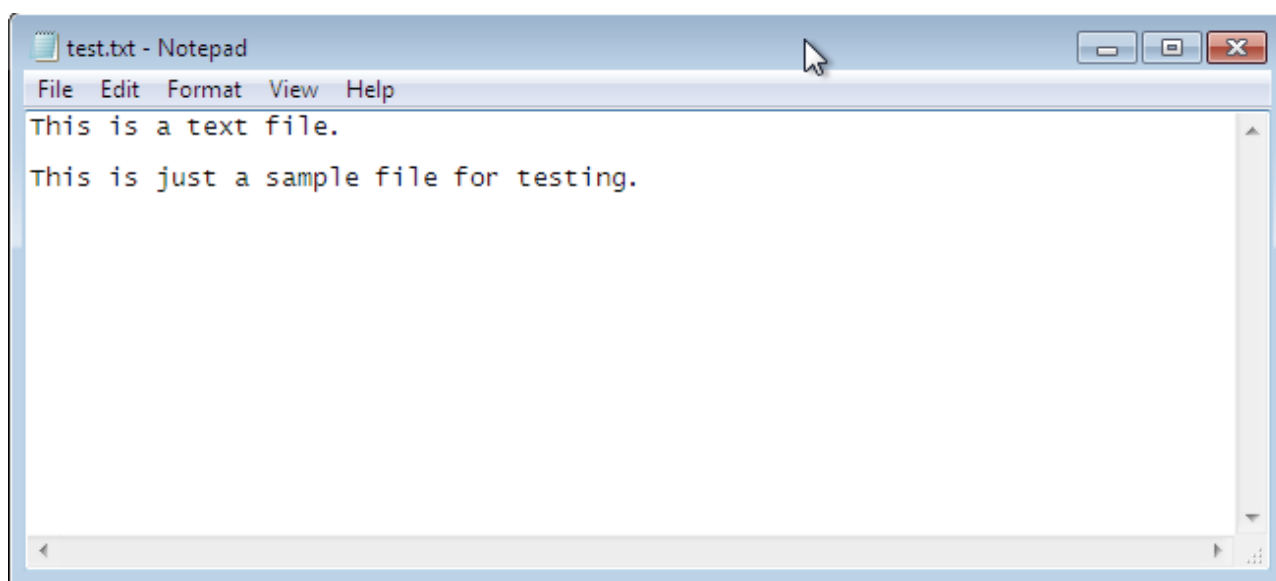
Changing file extensions

Elaborate on how we can hide data by changing the extension of the files.

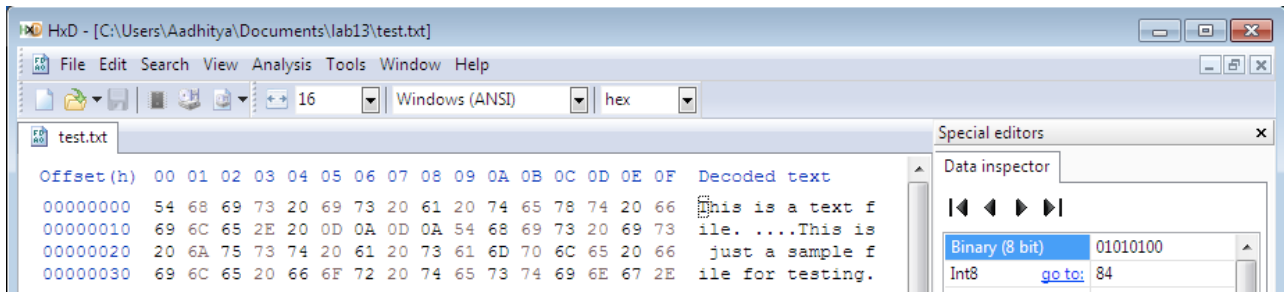
It is one of the first techniques to hide data. Advanced digital forensics tools check file headers. They compare the file extension to verify that it's correct. If there's a discrepancy, the tool flags the file as a possible altered file.

In order to demonstrate an example where changing the name of the file can effectively prevent the operating system from choosing the right application to open the file with thereby making the file unreadable. We will be using a Windows 7 operating system for this demonstration.

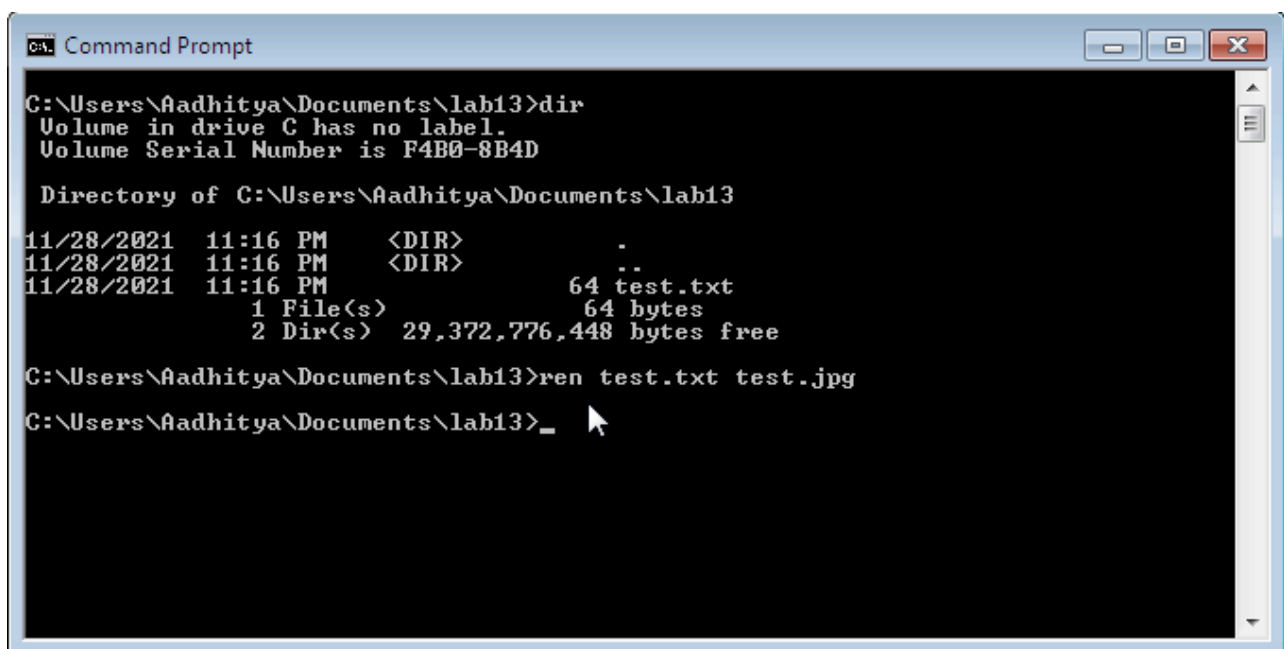
Here we will create a simple text file with say two lines of text. The file is shown below, and so is it visible in the file explorer as a text file.



We can further improve our notion that this is a text file by opening this file with any hexadecimal editor. Here, we will use the HxD editor for opening this file. On opening the file with this application, notice the file header and footer, and this is the same as the header and footer commonly associated with text files. It is by this, that we can verify that this file is indeed of txt format.

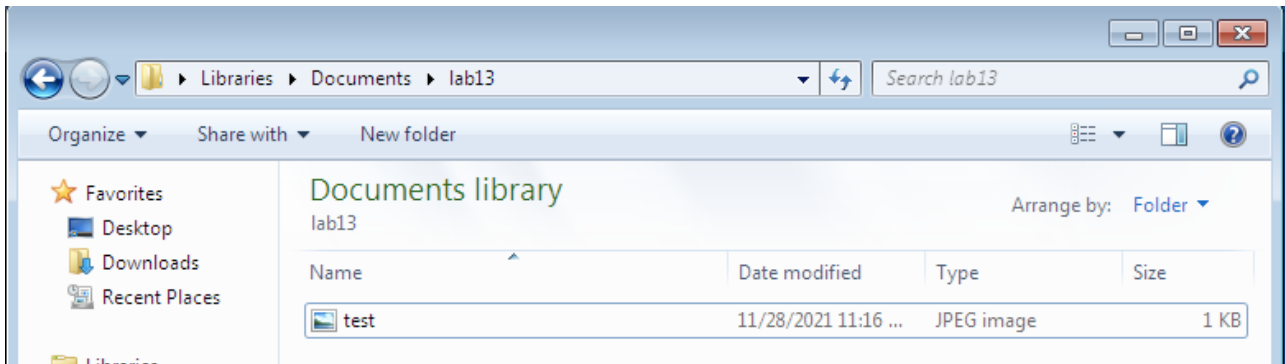


Now to make this data un-readable, we will change the file extension of the file. For this we use the **ren** command in Windows through its command prompt. The re-naming process is shown as follows :

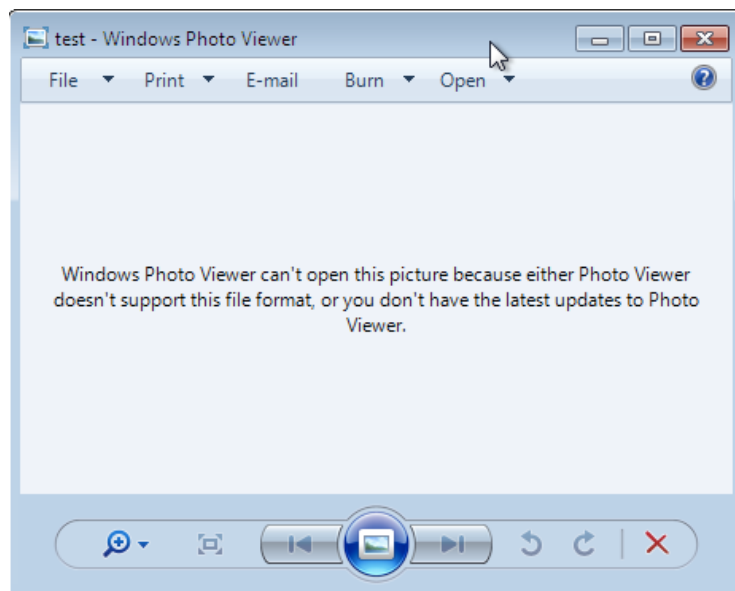


With this file re-named, we will now not be able to open it and view its contents. This is because the Explorer detects files based on their extension and when we changed that, we effectively told explorer that this file was an image. So it will try to open the file by using the application which is default for opening image files.

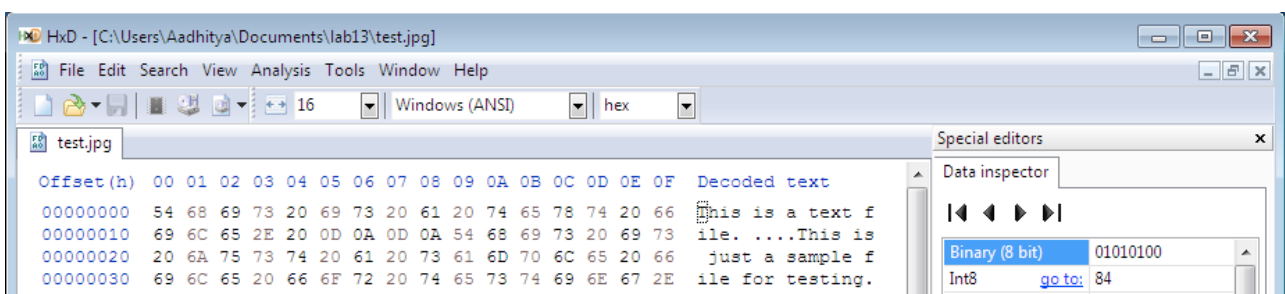
After renaming the file, it looks as follows when viewed from an explorer window :



When we try to open this, it opens the Windows Photo Viewer application which is unable to read the file appropriately.



If we try to open the file again using a hexadecimal editor, we can notice that there is no change in the header and footer.



Thus this can be used as an effective measure in detecting files with modified extension formats. The headers and footers are unique for a particular file format and can thus be used to identify the file format easily.

Question 3 :

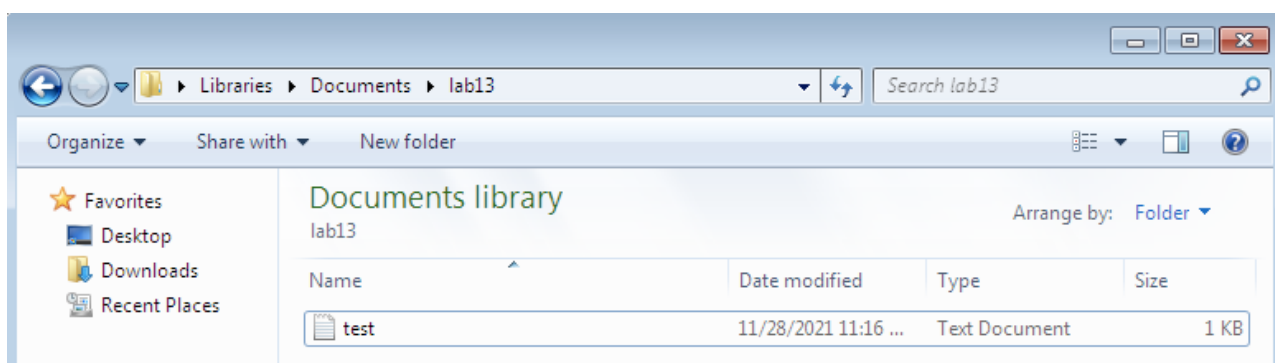
Setting file attributes to hidden

Hide files by using the Windows Explorer tool.

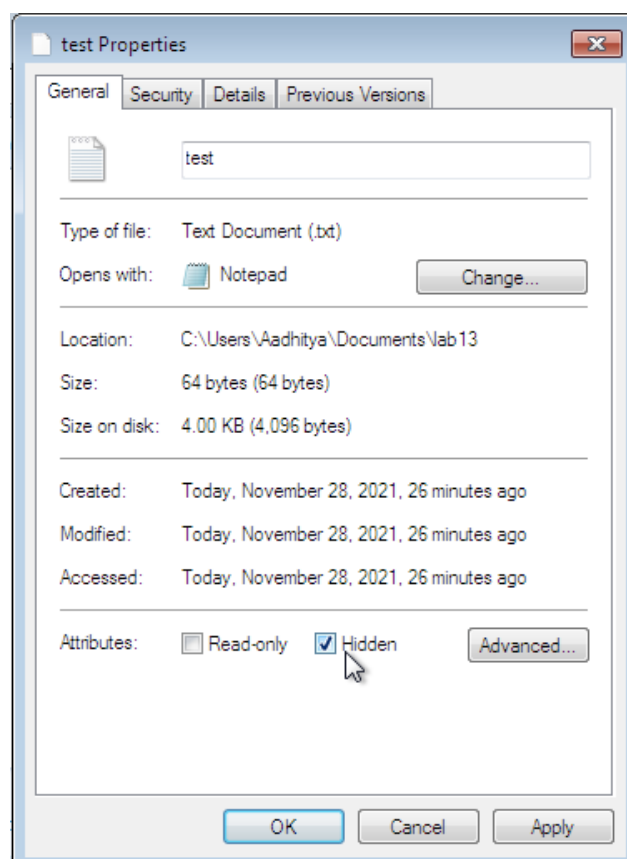
This is done by selecting the Hidden attribute in a file's Properties dialog box in Windows or any such measure in other operating systems.

We shall now demonstrate this with a simple text file. For this demonstration, we will be using a Windows 7 Environment.

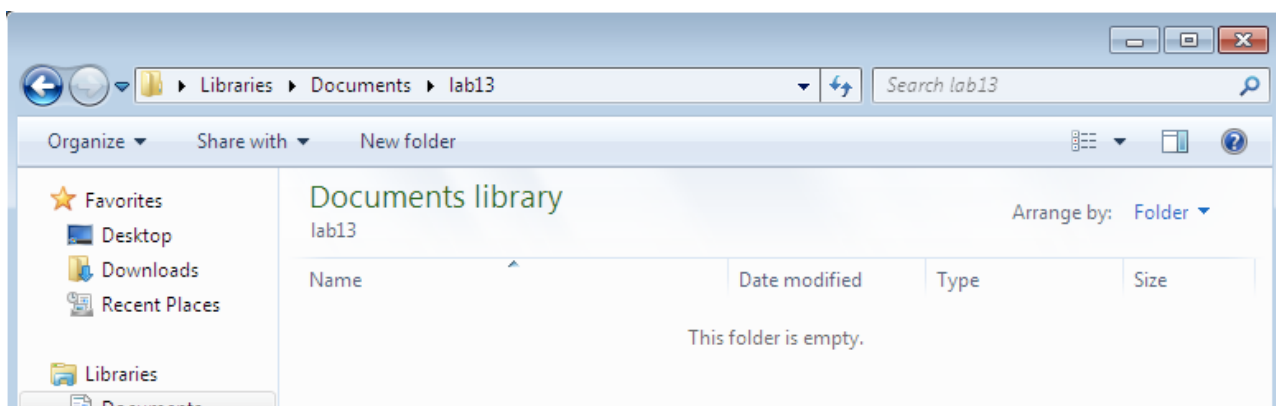
We will first create a new text file and fill it with some content. The following image shows this file created :



We will then go to its file properties and click on the attribute — **Hidden**, in order to hide this file. This process is shown the the following image :

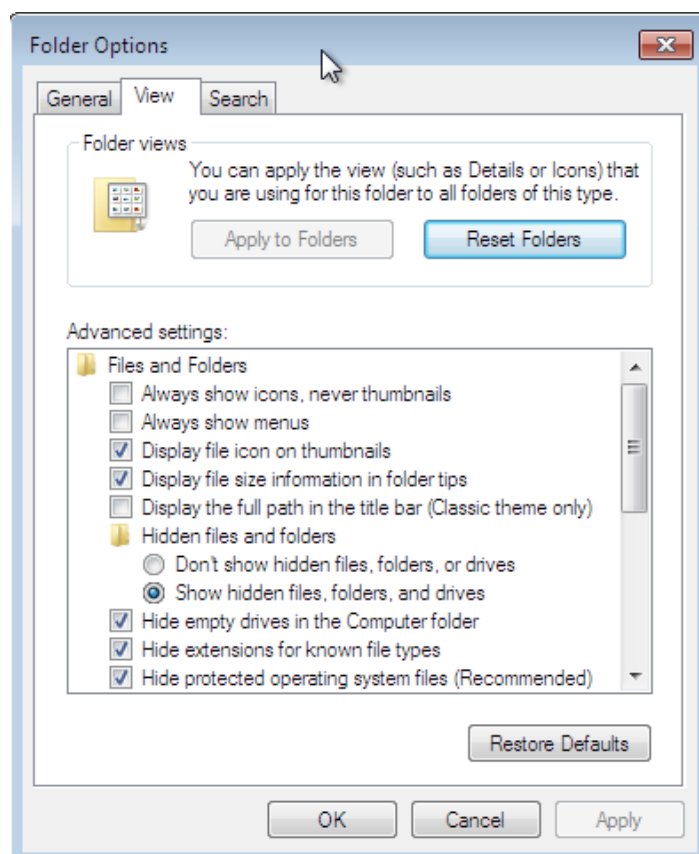


With this done and the changes applied the file is now hidden from the file explorer, say in our case after making this change the file is not listed in the explorer window :



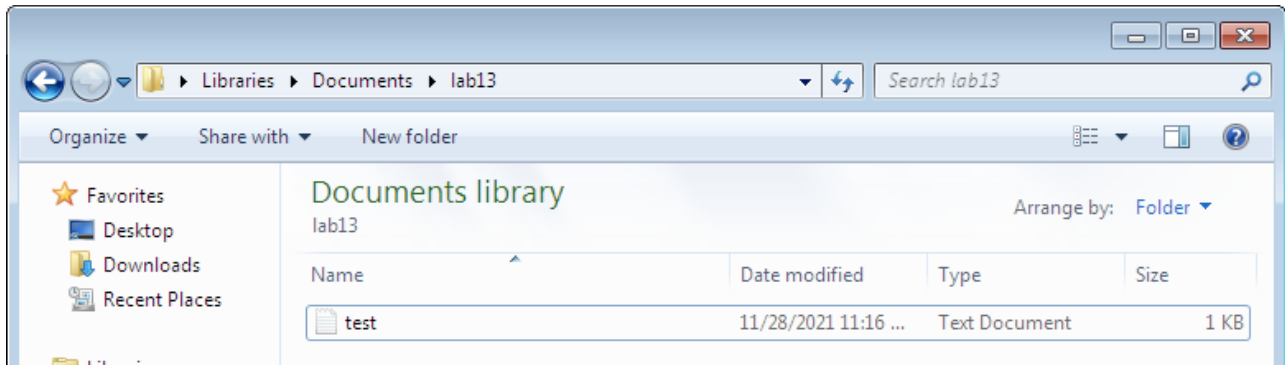
This is thus an effective way to hide data in files and make it invisible to file managers. This is too easy to perform data hiding, and we will also see how this can be reversed and effectively find hidden files in folders.

We head over to the control panel and then into Folder Options, there we will have a radio button for enabling the show hidden files, we select this option and then the hidden files will appear in the file manager.



In order to differentiate between the hidden and the non - hidden files, the explorer will show the hidden files in a blurred format. This can be used to distinguish between the two.

In our case, the hidden file is now visible as sated above in the file explorer as shown the following image :



This is thus a very easy method for hiding sensitive data and can be used by anyone as it does not involve any complicated procedure to hide the files. Thus this is a preferred by criminals who are not tech savvy, and thus a forensic investigator should always keep this in mind to set the option in the control panel and thereby view any files hidden in the suspect's computer.

Question 4 :

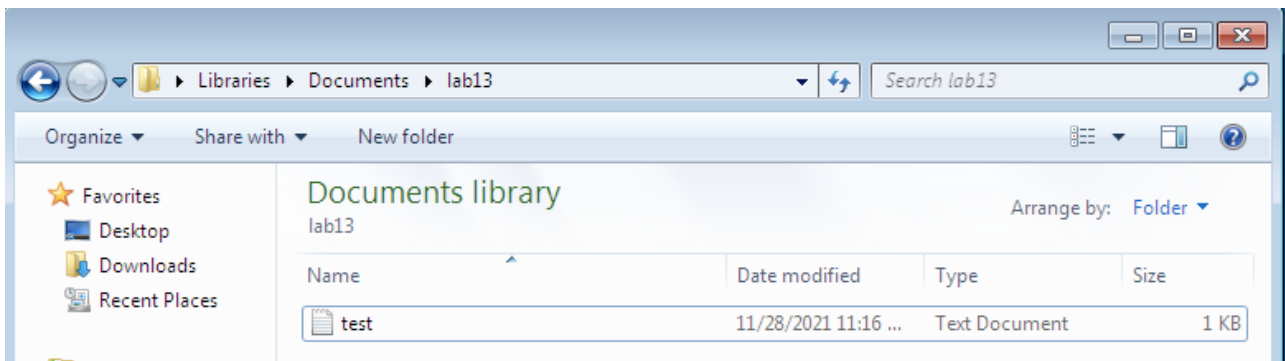
Bit-shifting

Encrypt a file' by using just bit shifting of its contents.

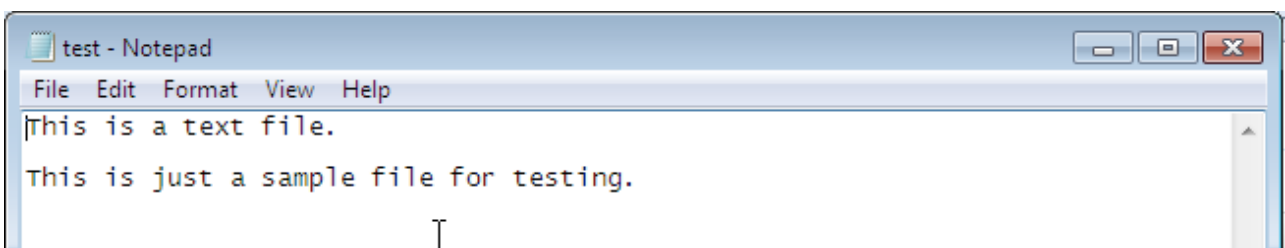
Bit shifting changes data from readable code to data that looks like binary executable code. WinHex includes a feature for shifting bits.

We shall now demonstrate this with a simple text file. For this demonstration, we will be using a Windows 7 Environment. We will be using the **Hex Workshop** Hexadecimal editor to make the necessary changes and to edit the files.

We will first create a new text file and fill it with some content. The following image shows this file created :

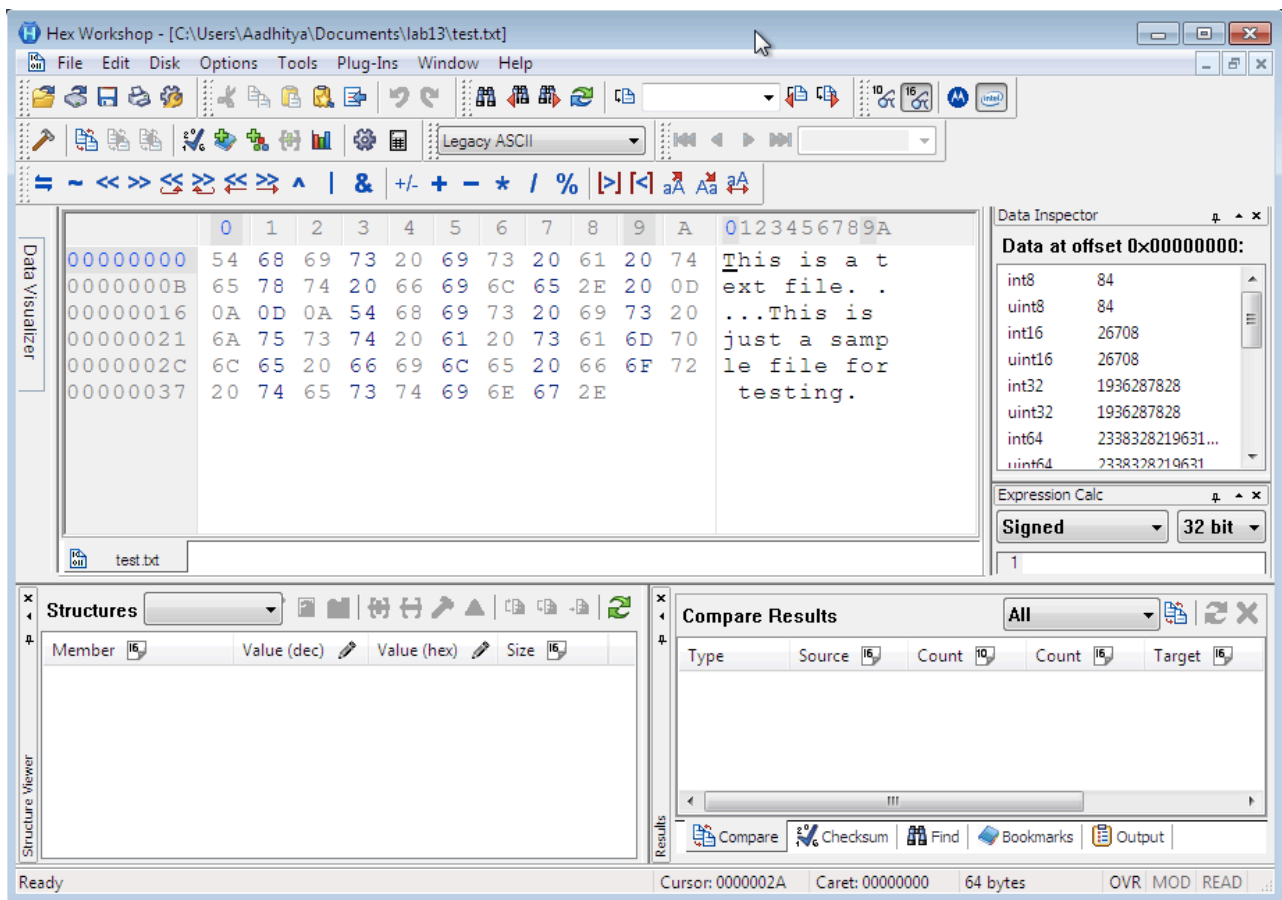


Let us then open this file and type in some content as a sample text for viewing purposes. The following image denotes the text typed into the file created :

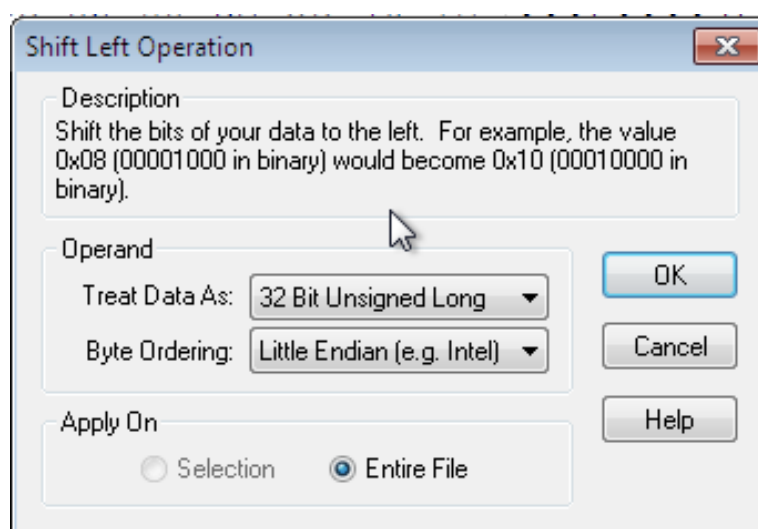


The next steps to shift the bits of this text by using any hexadecimal editor, in order to do this, reopen the file in a hexadecimal editor with functionalities for editing and modifying the source file. Some editors which allow this are WinHex, **Hex Workshop**, etc. Here we will be using the latter tool for this demonstration.

We will first open the file inside the **Hex Workshop**, tool, and the file when opened is as follows :

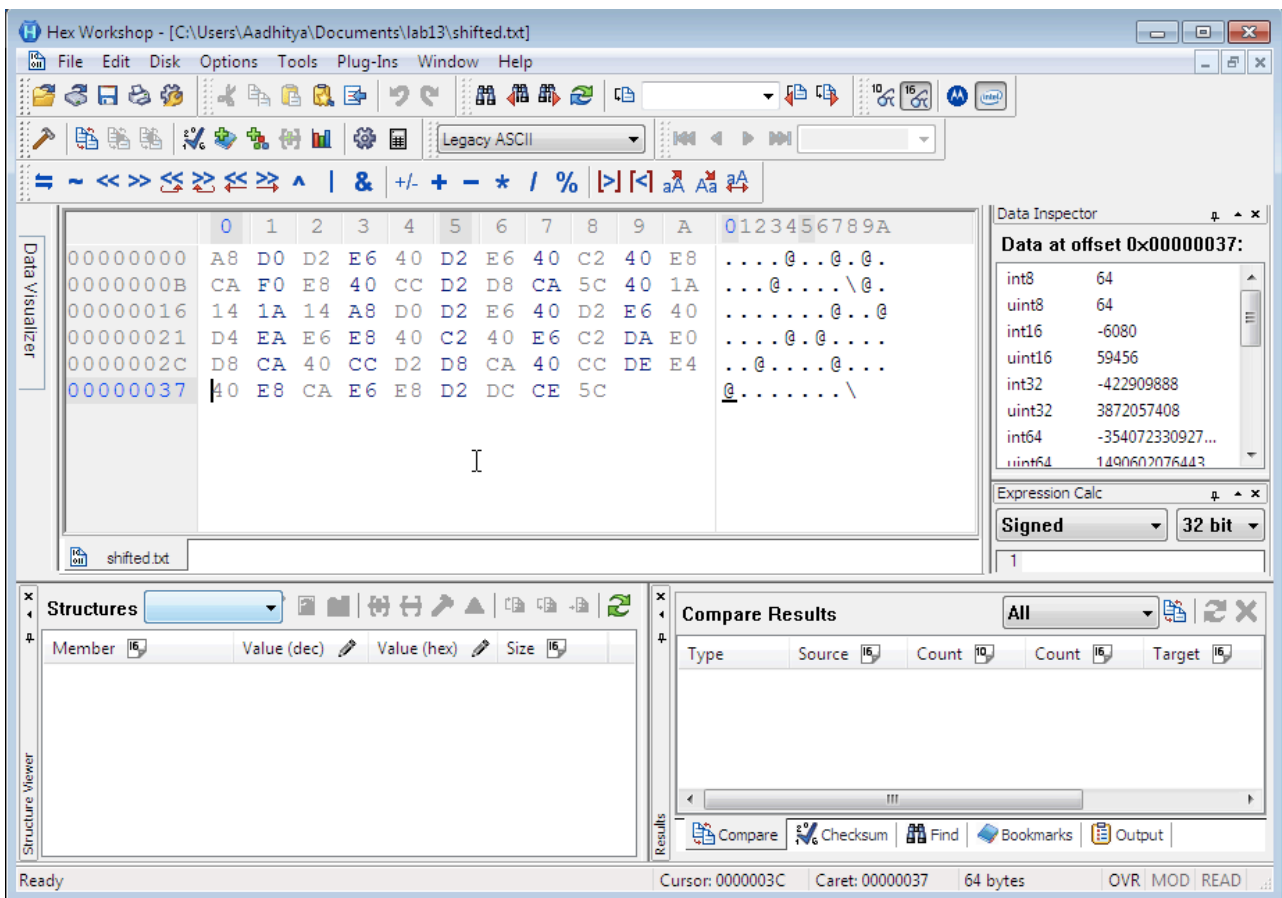


In this software, we will use the editing toolbar to make the bit shifting operations. We will then select the shift left option in the toolbar, and then make the following settings for the operation :

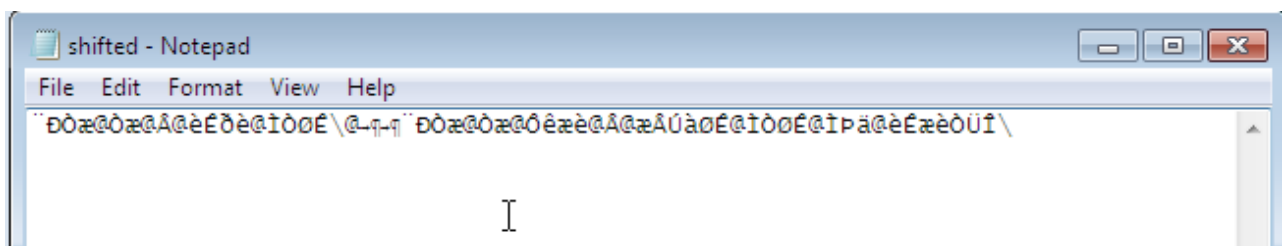


Here the operation applied is a bitwise left shift for the complete file.

After applying this operation, the file is modified and in this case shifted bitwise left by one position, and the modified file looks as follows :



We can notice that operation is complete, we can also verify this by opening the file using the notepad application which is shown below :



We can notice here that the complete text is now just pieces of symbols which make no sense when looked with our eye. Thus we have managed to use bit shift to hide the data. In this case, we can reverse this by just performing bitwise right shift operation on this text.

This is thus an effective method for hiding data as when looks upon is like random symbols or a corrupted file, but the forensic investigator should be cautious to apply the right set of shifting operations in order to get the original data which would make sense.

Question 5 :

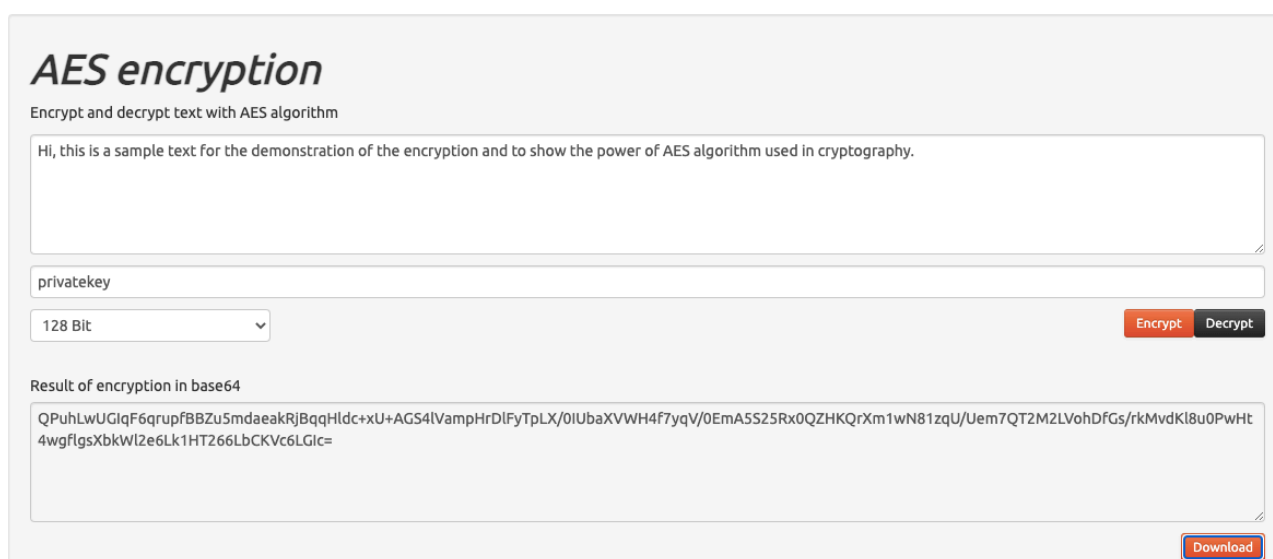
Encryption

Elaborate on how files or file contents can be encrypted using popular algorithms like AES, RSA, etc.

Also mention if entire hard disks can be encrypted, and if so elaborate on how this is achieved.

It is possible to encrypt data using encryption algorithms such as AES and RSA. Many online encryption/decryption tools are available. For example, <https://aesencryption.net>

In this demonstration, we will be encrypting a piece of text, using a randomly selected key text. We will use the aforementioned website for the encryption process. Here we can see that we have entered the text and the key and also the mode of encryption. The text box over the bottom of the image shows the encrypted form of text.



AES encryption
Encrypt and decrypt text with AES algorithm

Hi, this is a sample text for the demonstration of the encryption and to show the power of AES algorithm used in cryptography.

privatekey

128 Bit

Encrypt Decrypt

Result of encryption in base64

QPuhLwUGIqF6qrupfBBZu5mdaeakRJBqqHldc+xU+AGS4IVampHrDIFyTpLX/0IUbaXVWH4f7yqV/0EmA5S25Rx0QZHKQrXm1wN81zqU/Uem7QT2M2LVohDFGs/rkMvdKI8u0PwHt4wgflgsXbkWlze6Lk1HT266LbCKVc6LGlc=

Download

Encryption is thus an excellent form of data hiding, as it ensures that the data is not readable, and further getting the plain text from this cipher text is very complicated and nearly impossible with our current advances in the compute power. Thus it is safe to say that the data encrypted is safe and cannot be accessed by anyone easily. At the same time this also poses as a hurdle in forensic investigations, as the encrypted text cannot be decrypted, and thus the investigators are forced to either lose hope of decrypting the evidence or to come up with enhanced and innovative techniques to make the suspect give away the decryption keys.

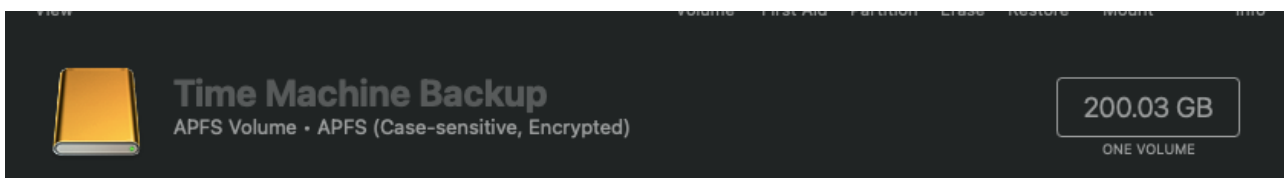
It is possible to encrypt a hard drive with Bitlocker in Windows 10, Refer to :

<https://www.securicy.com/blog/how-to-encrypt-a-hard-drive-with-bitlocker-in-windows-10>

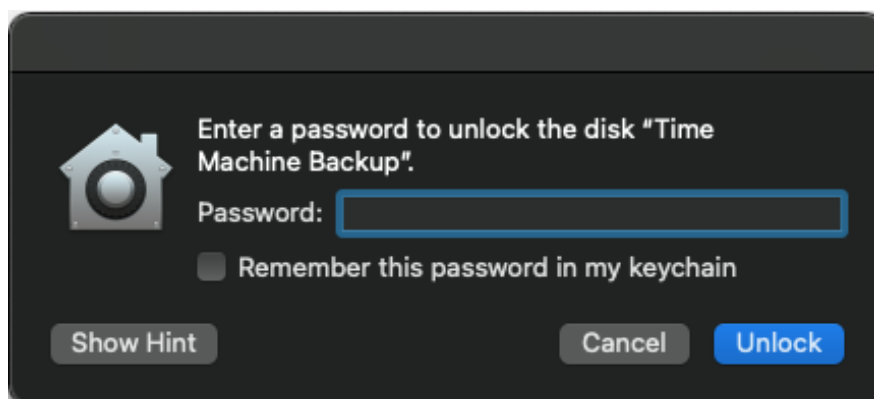
We will in this demonstration, show the same procedure but in a different environment. We will be using the Mac OS-X operating system and the Disk Utility tool available in it to encrypt the disk.

The process to do this is relatively simple, we just click on erase and format, choose a format of encryption with the word “Encrypted”, and then click on format, which will make the disk protected with a password that we set.

After this process is over, the partition that we just put under lock and key looks as follows when viewed under the disk utility tool. Note the word “Encrypted” which denotes that the partition is password protected.



When we try to mount the disk or in this case the partition, it requires us to provide a password, only after which we can access the contents of the disk.



This is thus another relatively easier way to secure the contents in the entire hard disk and have it encrypted so that it cannot be accessed without proper password for authentication. At the same time this also poses as a hurdle in forensic investigations, as the encrypted disks cannot be accessed, and thus the investigators are forced to either lose hope of decrypting the evidence or to come up with enhanced and innovative techniques to make the suspect give away the decryption keys and passwords.

Question 6 :

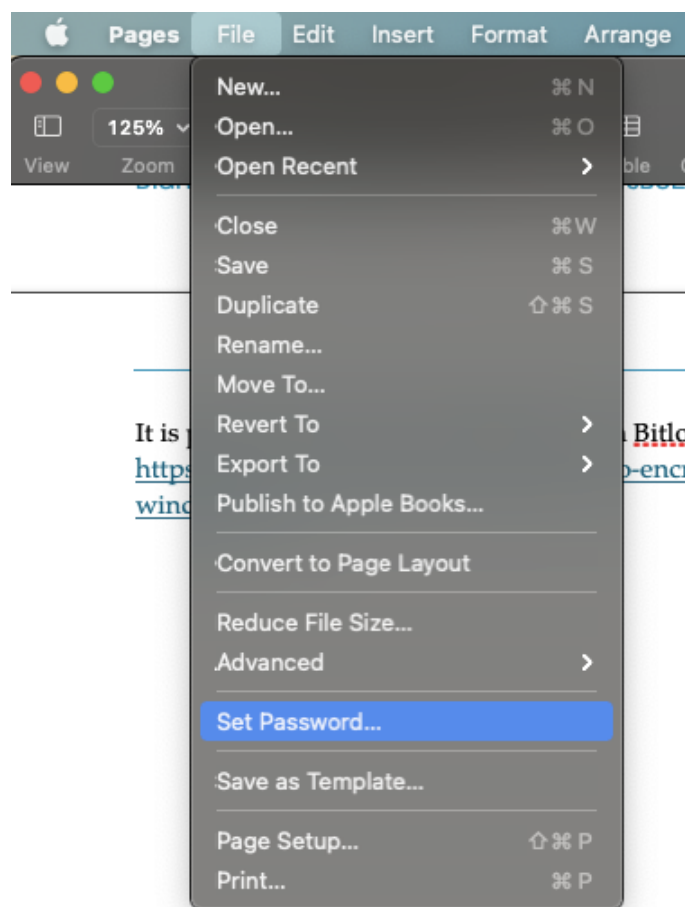
Setting up password protection

Mention how we can password protect important files and thereby limit access to the contents of such files.

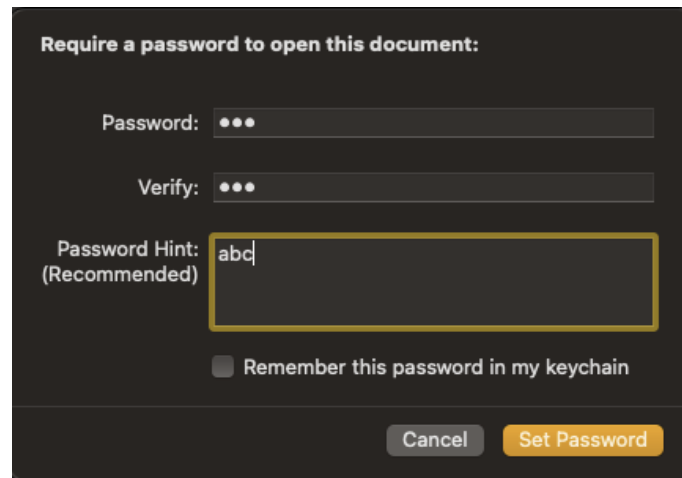
Enabling password-protection for your document can be a measure that any user can apply instantaneously for their individual documents. You can activate password protection for Word, PowerPoint or Excel documents. This will limit the ability to open the file by requiring a password to be entered. The process may differ slightly depending on the version of Microsoft Office, or any other document processing tools that you may use.

In this demonstration, we will show the same procedure of locking files in a Mac OS environment with using the Pages application which is a word processing tool similar to Microsoft Word in the Office 365 suite.

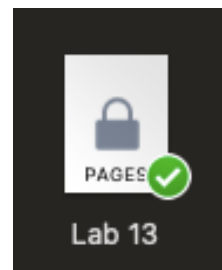
We will first open the file using the pages application, and then proceed to set a password. This process of setting the password is available from the top menu bar and is shown below :



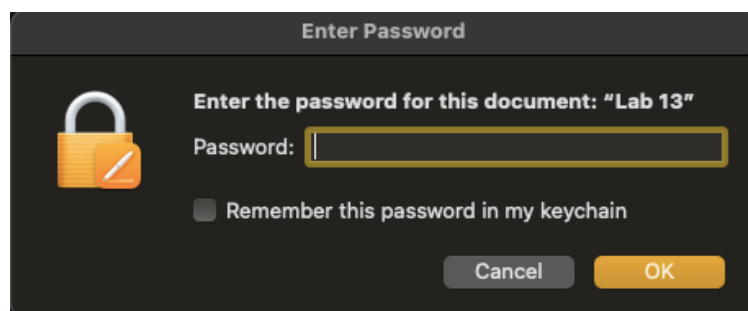
This then triggers a dialog box which prompts us to set a password and also a hint in case we forget the password. We now set these and then submit. This password entering process is shown as follows :



Once this is done, the file is locked with the password and the icon changes denoting that the file is password protected and locked. In case of Mac OS-X, the symbol looks like this :



Thus when we click on this or open the file, we are prompted with a window to enter the password only after which we can enter the file, and view its contents.



Thus saving files with sensitive content with passwords is an effective way to maintain access control over the data in those files, and to prevent any unauthorized access to the data. But in the case of forensic investigations, it is the place where the suspect might have hidden the information which might be vital to the case. Thus it is of utmost importance for investigators to come up with innovative ways to crack the password and thereby view its contents.

CONCLUSION

In this lab experiments, we have dealt with and seen the possible methods for hiding data, and also discussed on how such hidden data can be identified and even retrieved for that matter. We have also shown these with appropriate evidence in execution. Thus Data Hiding and its appropriate data retrieval can provide useful functionalities for the ease of forensic analysis.