Worcester Polytechnic Institute
Department of Computer Science

Module 3: Timestomping

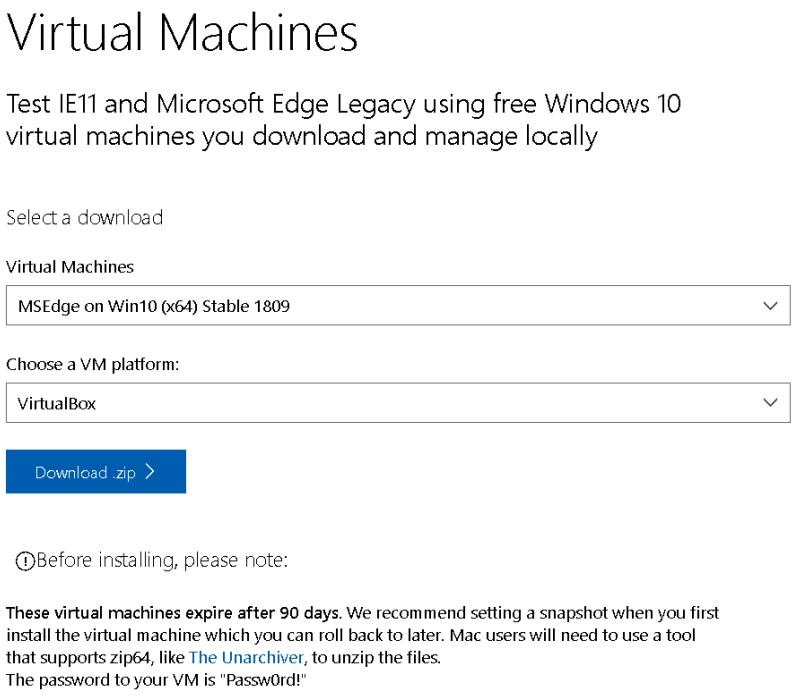
Objectives

- Learn how to manipulate timestamps by changing a file's creation, modification, and access time using Windows PowerShell
- Learn how to detect timestomping by checking the Master File Table (MFT) in the NTFS system using WinHex

Tasks

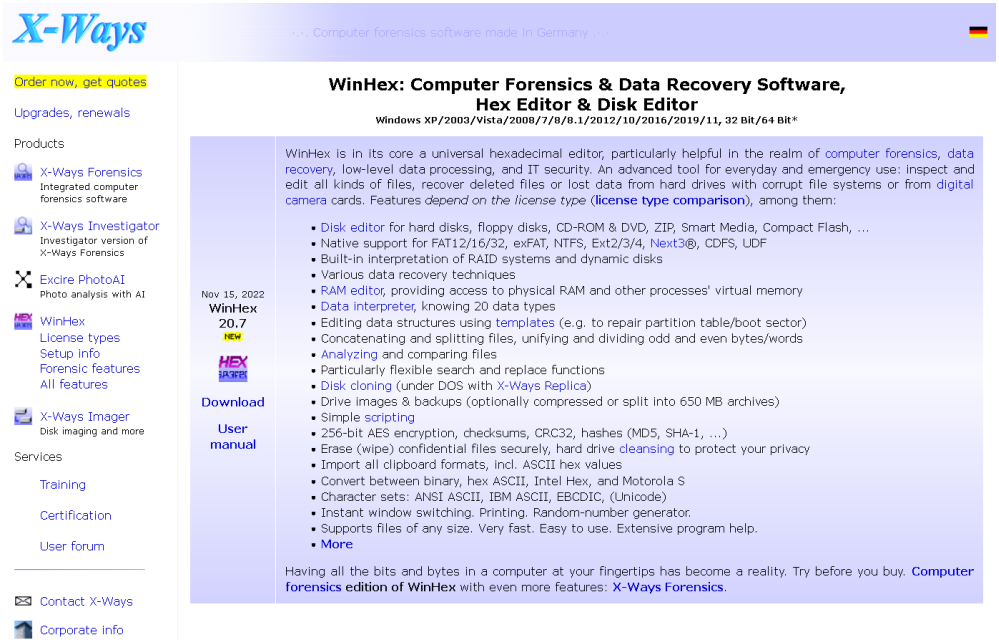
Task 0. Set up the environment.

1. (Recommended) Prepare a Windows 10 virtual machine
   You can download a free premade Windows 10 virtual machine at
   https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
   The virtual machine will expire after 90 days. The password is Passw0rd!
   You can choose whichever VM platform you would like.

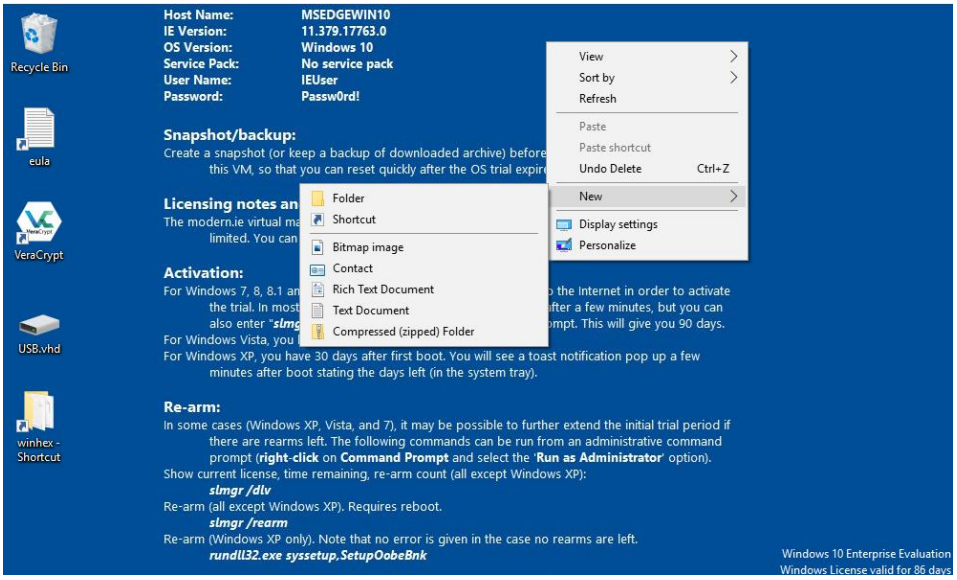


Task 1. Install WinHex

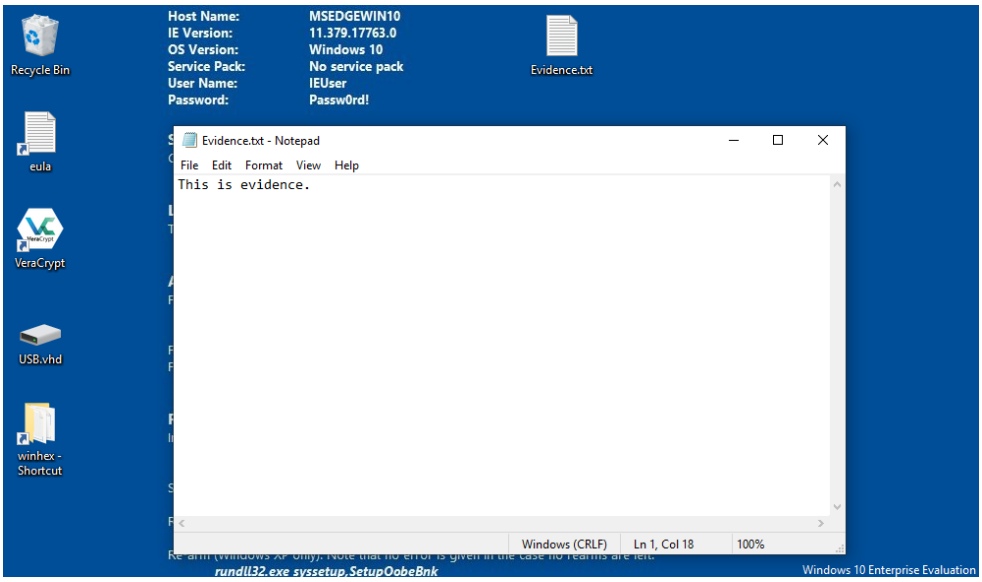
1. **Install WinHex at** https://www.x-ways.net/winhex/



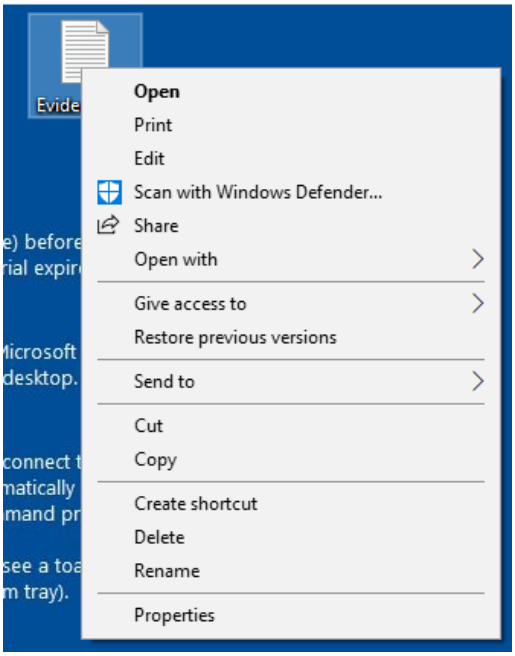
Task 2. Create a text file



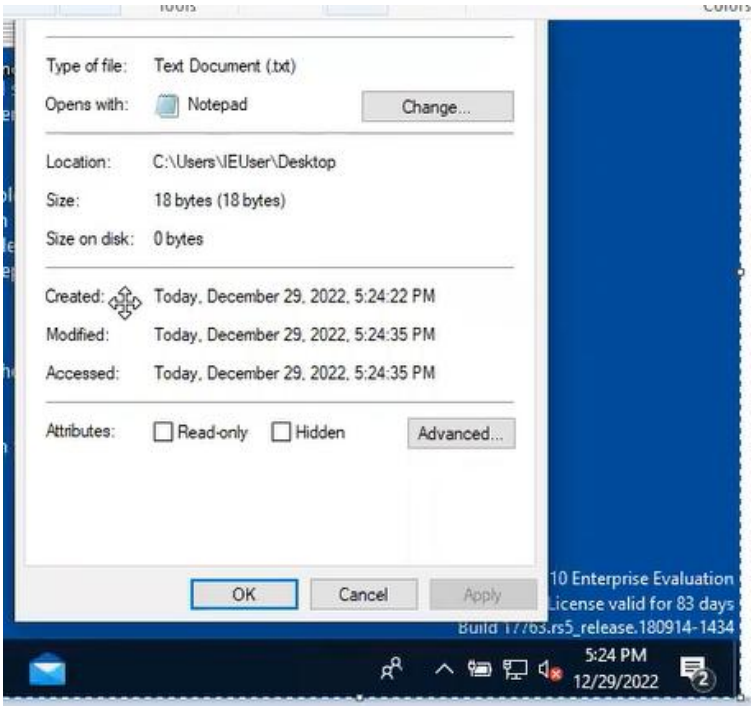
1. Right click where you would like to create a text file and navigate to New > “Text Document”



2. Name your file “Evidence.txt” and open it. Then type something in your file and save it.

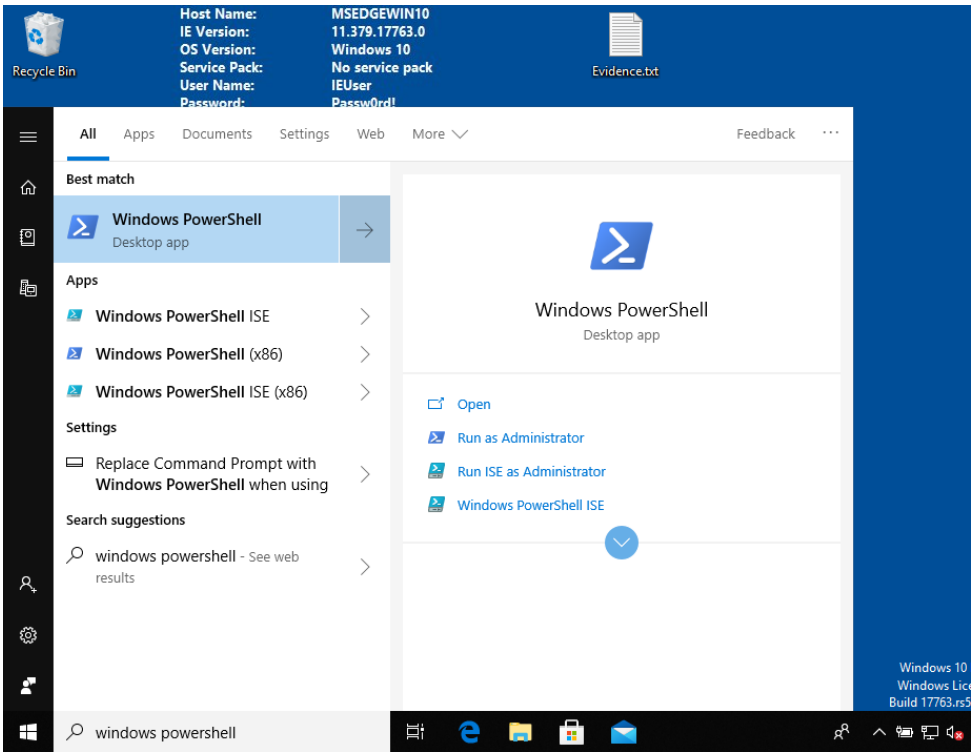


3. Right click your file and click “Properties”.



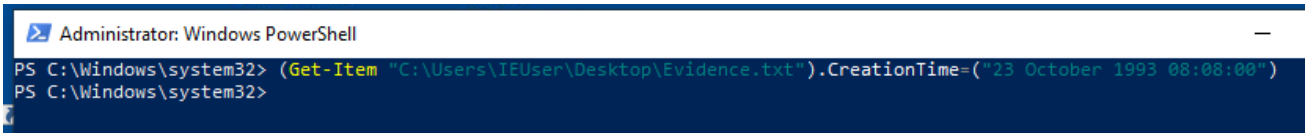
4. You should be able to see the file's location, created time, modified time, and accessed time. Take a screenshot of this (as well as the time you took the screenshot) or record this information somewhere.

Task 3. Timestomp a file using Windows PowerShell



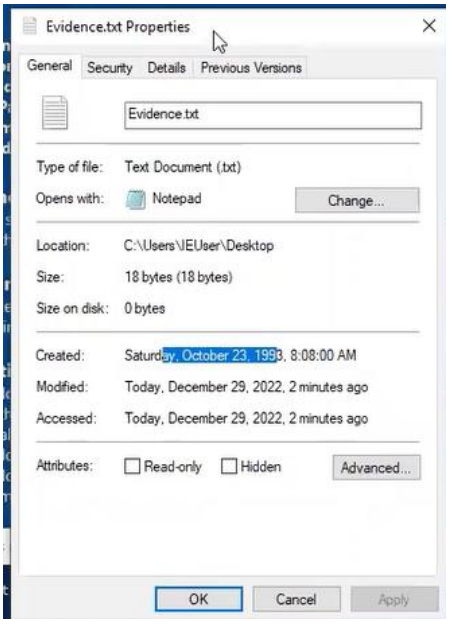
1. Click the windows button on the bottom left of the screen and type "Powershell".
2. Click "Run as administrator" on the right

3. If you receive this pop up, click “Yes”.

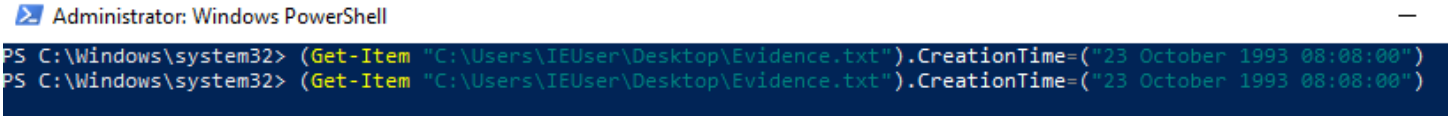


4. The command to change the creation time uses this format:
   (Get-Item "[LOCATION]\[FILE NAME]").CreationTime=("DAY MONTH YEAR TIME")

   Example command used in the image:
   (Get-Item "C:\Users\IEUser\Desktop\Evidence.txt").CreationTime=("23 October 1993 08:08:00")



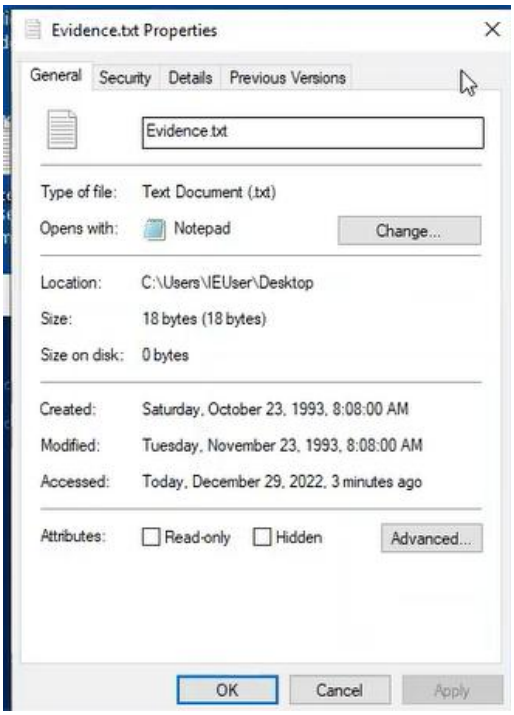
5. Examine the properties of your file again. You should see the new created time now.



6. Press the up arrow to get a copy of the last command.

7. Use the arrow keys to move the cursor to where it says “CreationTime” and replace it with “LastWriteTime”
8. Now you can change the modified time to whatever time you would like and then hit Enter.

   Example command used in the image:
   (Get-Item "C:\Users\IEUser\Desktop\Evidence.txt").LastWriteTime=("23 November 1993 08:08:00")



9. Your new modified time should reflect in the file’s properties.

```
PS C:\Windows\system32> (Get-Item "C:\Users\IEUser\Desktop\Evidence.txt").LastAccessTime=("23 December
>> 1993 08:08:00")
PS C:\Windows\system32>
```

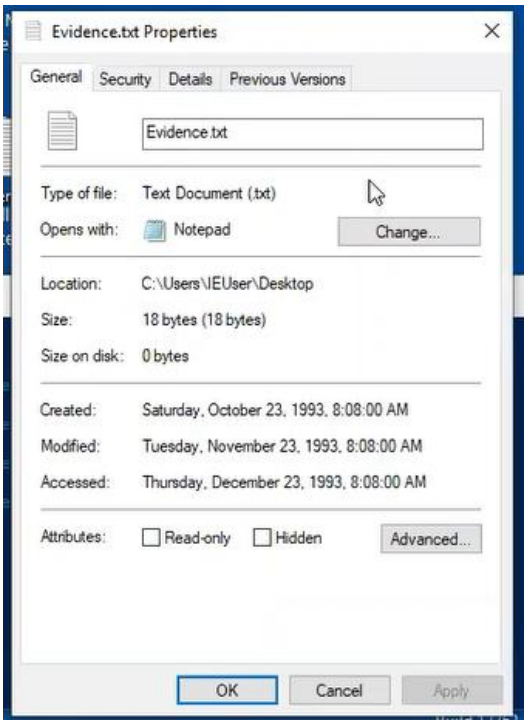
10. Once again, press up to get a copy of the last command and replace “LastWriteTime” with “LastAccessTime”
11. Now you can change the accessed time to whatever time you would like and then hit Enter.

    Example command used in the image:
    (Get-Item "C:\Users\IEUser\Desktop\Evidence.txt").LastAccessTime=("23 December 1993 08:08:00")

    NOTE: Some devices have LastAccessTime disabled by default, if your access time does not update with the command, type this command:
    fsutil behavior set disablelastaccess 1

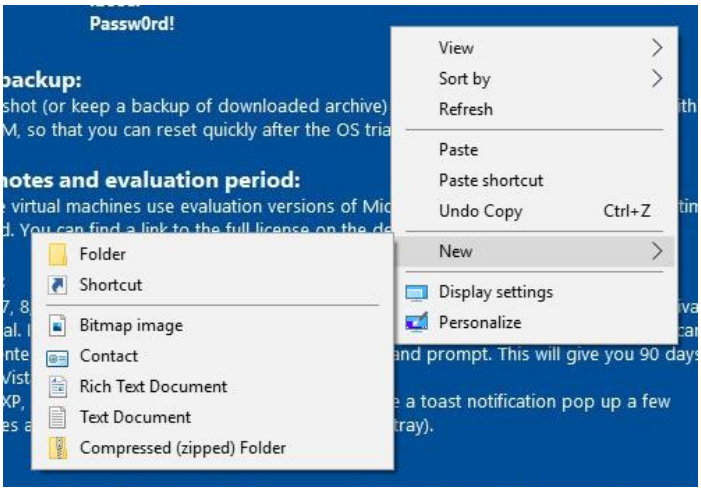
```
PS C:\Windows\system32> fsutil behavior set disablelastaccess 1
DisableLastAccess = 1  (User Managed, Enabled)
PS C:\Windows\system32>
```

    Once it says (User Managed, Enabled), you can try the LastAccessTime command again.

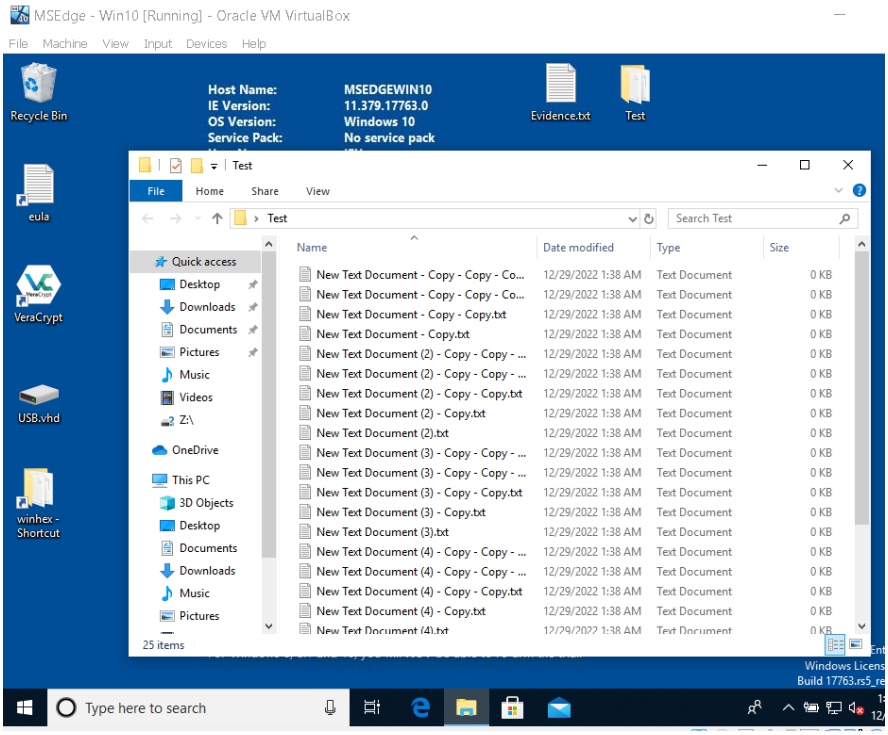


12. Now we can see that all the times have been changed.

Task 4. Create a directory with many files in it

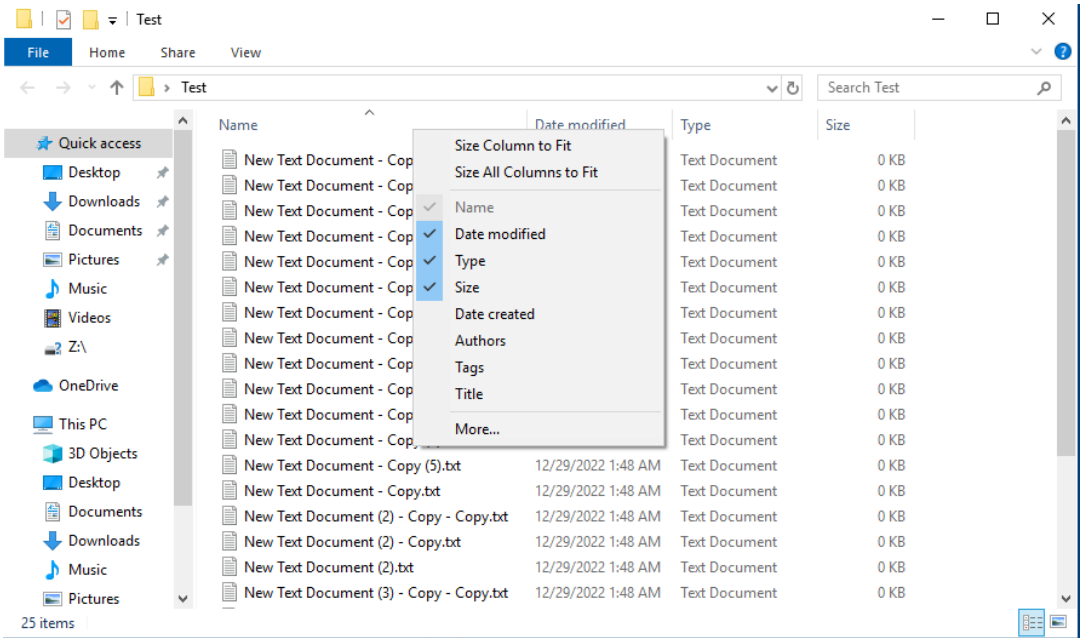


1. Right click where you would like to create a directory and navigate to New > Folder

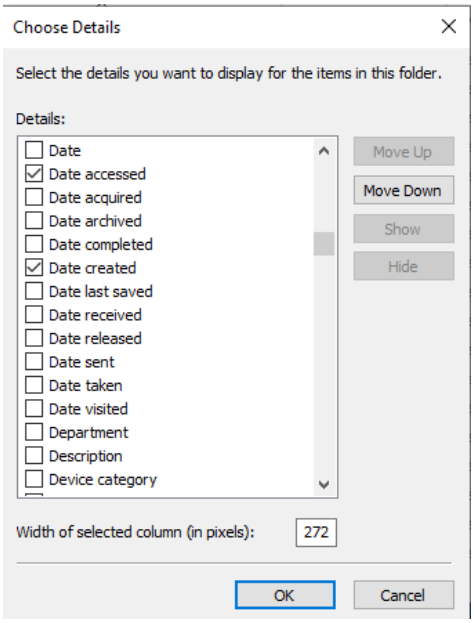


2. Name your folder and create many text files inside of it.

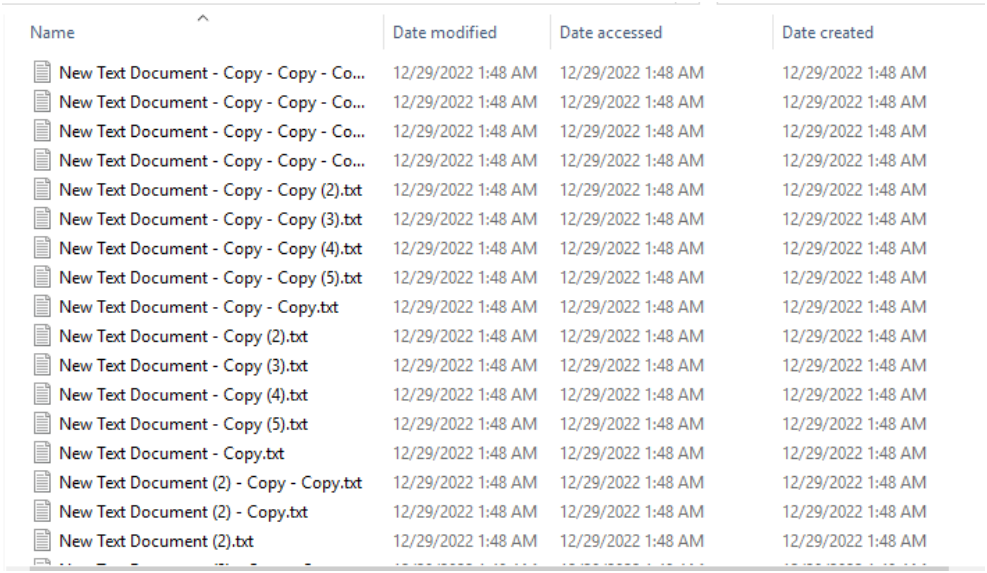
Task 5. Timestomp an entire directory using Windows Powershell



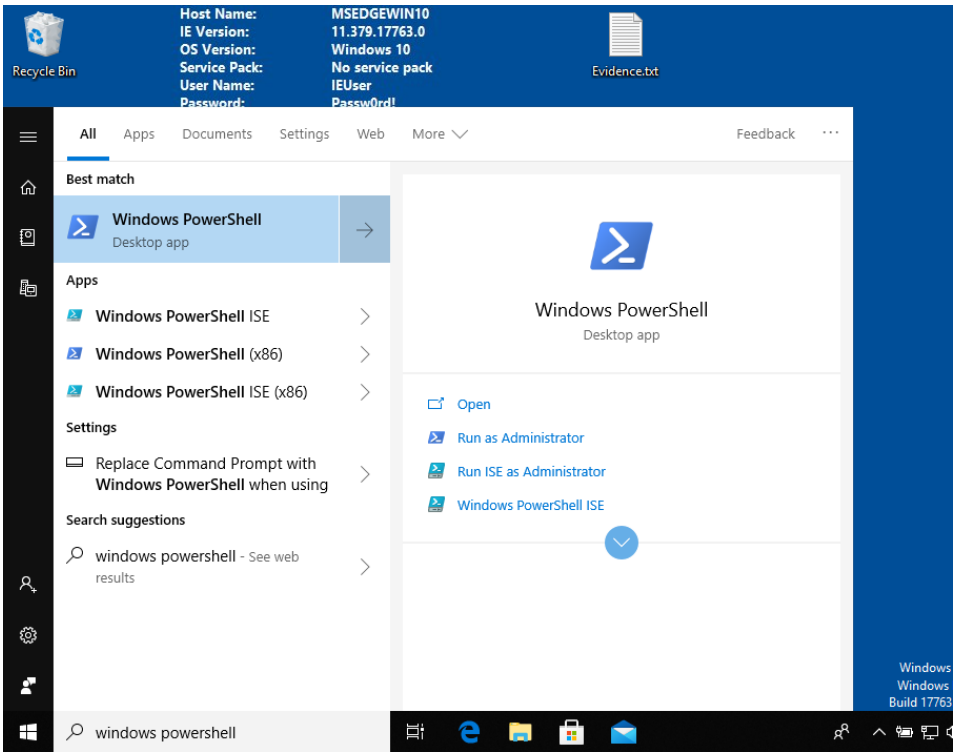
1. Right click the headers of the directory you just created and click “More…”



2. Uncheck “Size” and “Type” if they are already checked. Make sure “Name”, “Date modified”, “Date accessed”, and “Date created” are checked. Then click “OK”



3. You should now be able to see all of the modified, accessed, and created times for all of the files in the directory.

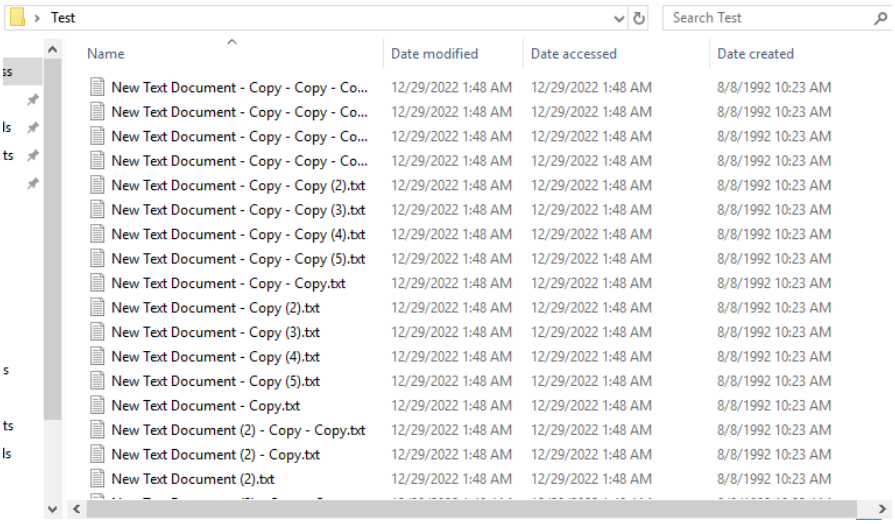


4. Once again, open Windows PowerShell as an administrator.

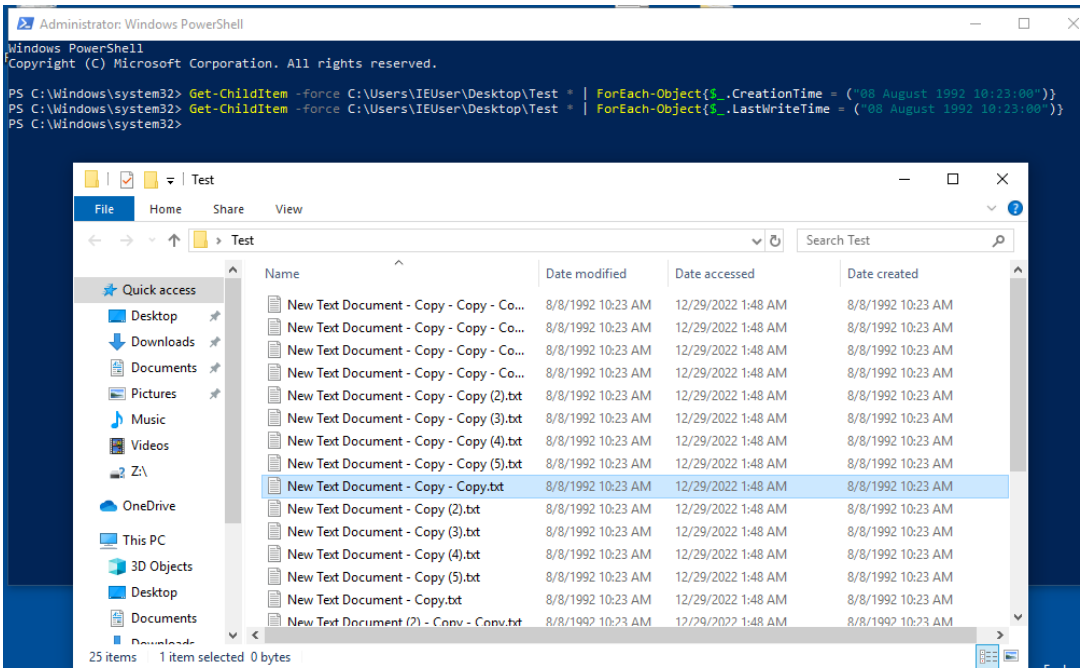
```
PS C:\Windows\system32> Get-ChildItem -force C:\Users\IEUser\Desktop\Test * | ForEach-Object{$_.CreationTime = ("08 August 1992 10:23:00")}
PS C:\Windows\system32>
```

5. The command to change the creation time for a directory uses this format:
   Get-ChildItem -force [LOCATION]\[DIRECTORY NAME] * | ForEach-Object{$_.CreationTime = ("DAY MONTH YEAR TIME")}

   Example command used in the image:
   Get-ChildItem -force C:\Users\IEUser\Desktop\Test * | ForEach-Object{$_.CreationTime = ("08 August 1992 10:23:00")}

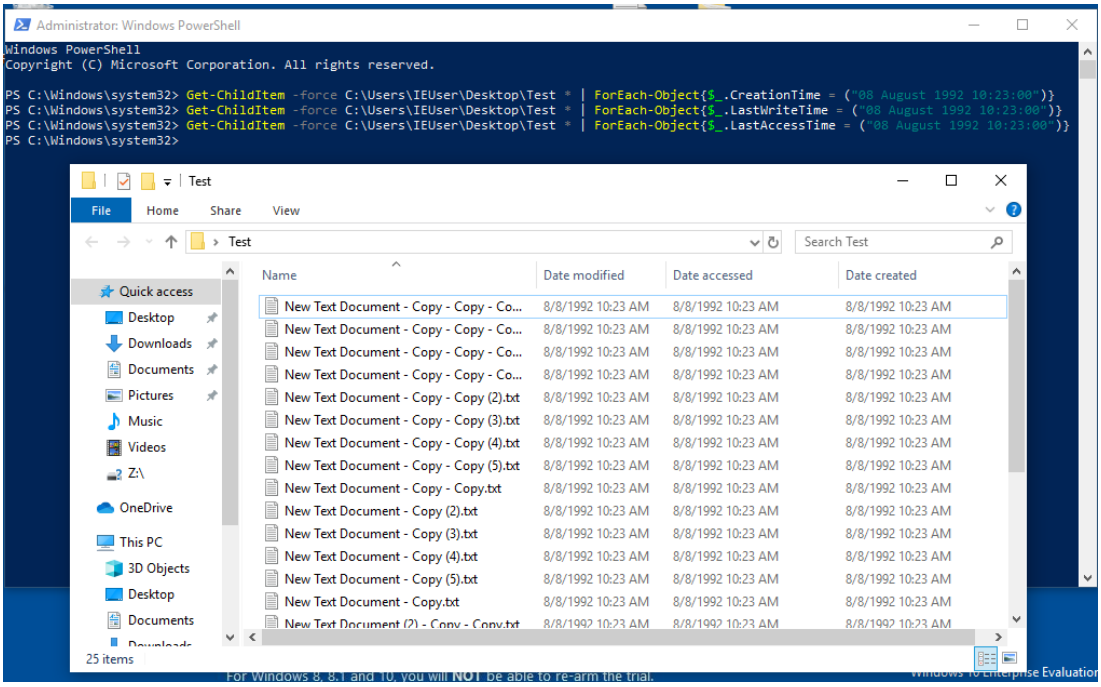


6. Open the directory again and you should see the “Date created” column has updated for all of the files.
7. Similar to task 3, change the modified and accessed time by replacing “CreationTime” with “LastWriteTime” and “LastAccessTime”



Example command used in the image:

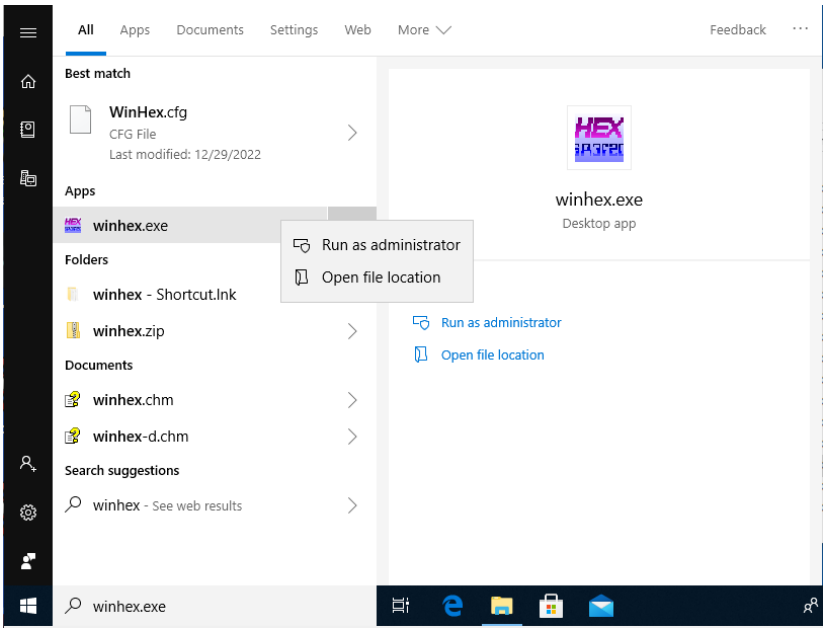
Get-ChildItem -force C:\Users\IEUser\Desktop\Test * | ForEach-Object{$_.LastWriteTime = ("08 August 1992 10:23:00")}



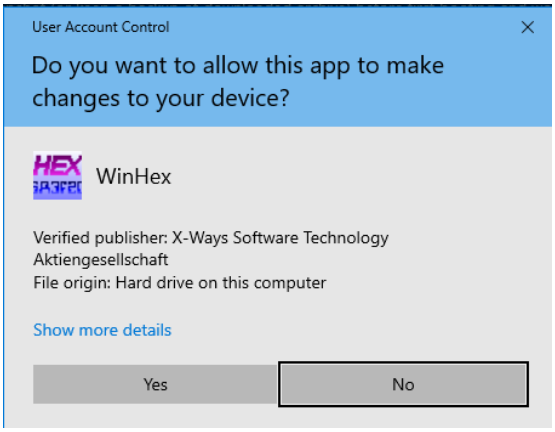
Example command used in the image:

Get-ChildItem -force C:\Users\IEUser\Desktop\Test * | ForEach-Object{$_.LastAccessTime = ("08 August 1992 10:23:00")}

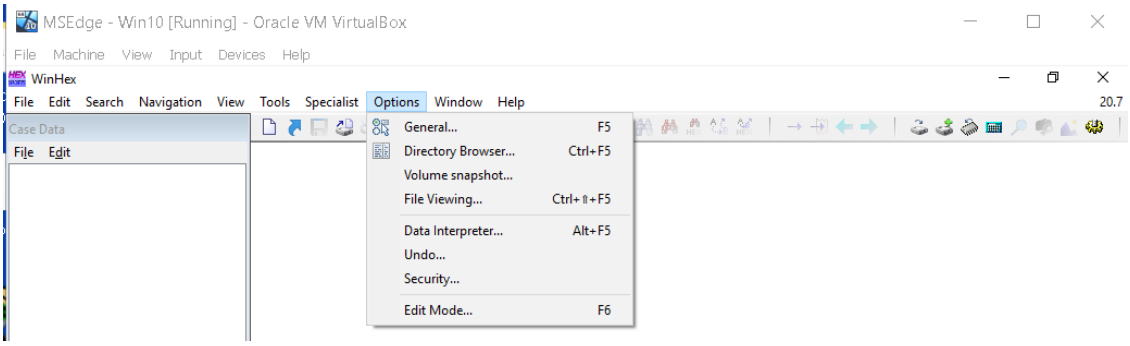
Task 6. Detect the timestomping using WinHex



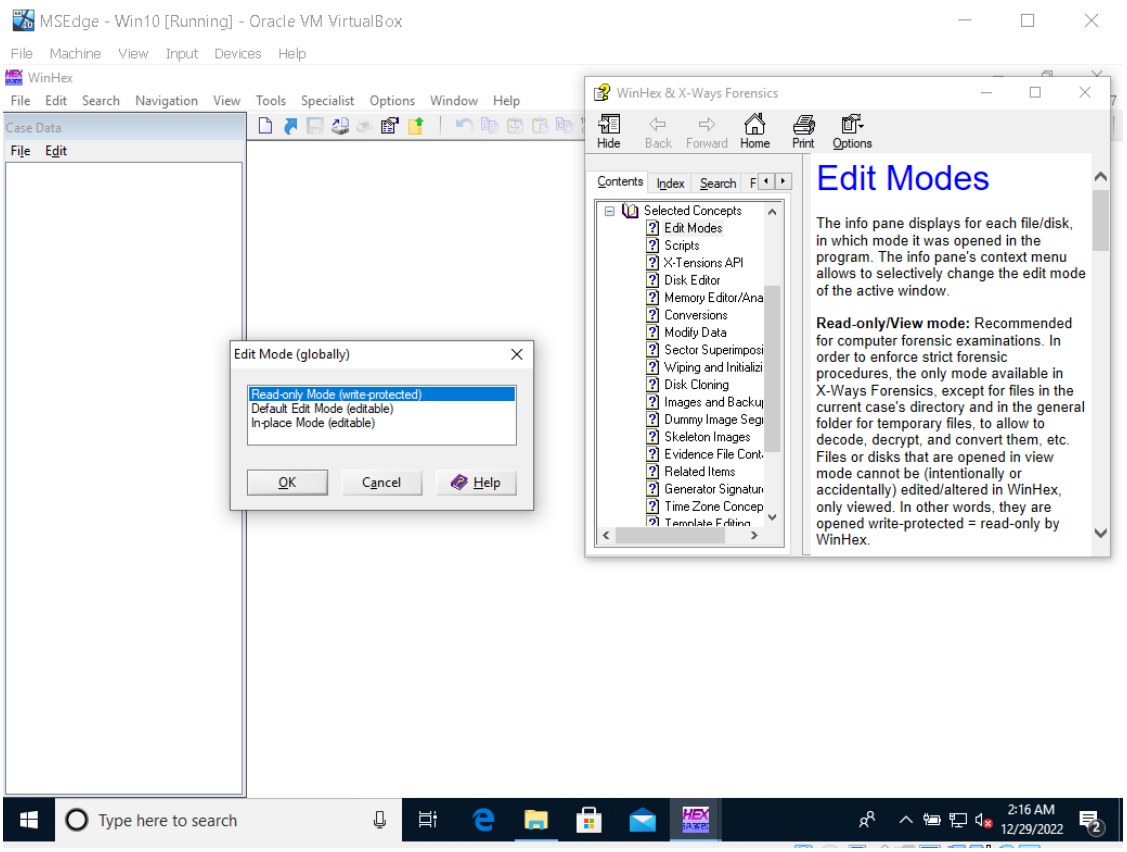
1. Run WinHex as an administrator



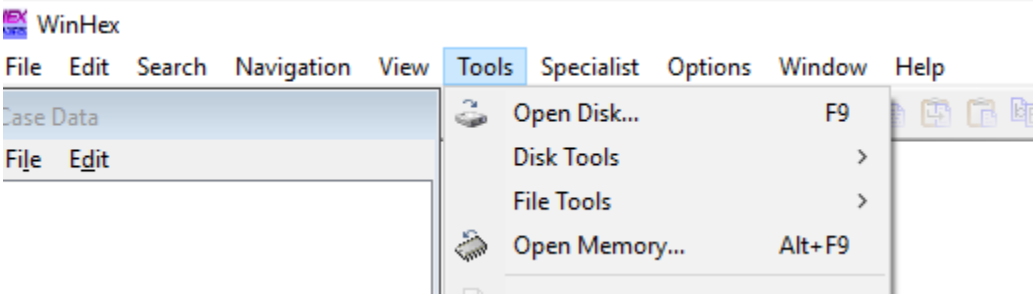
2. Click “Yes”



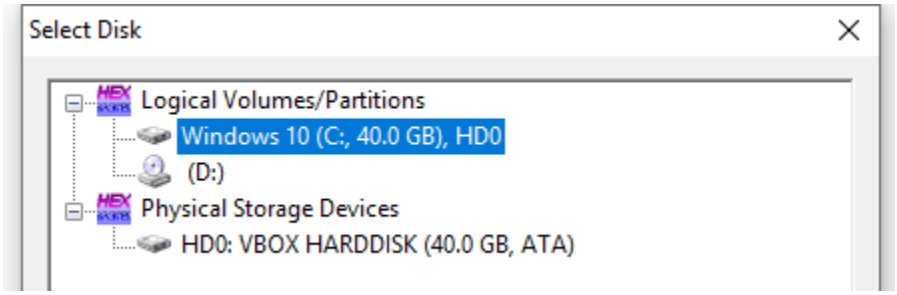
3. Navigate to Options > Edit Mode…



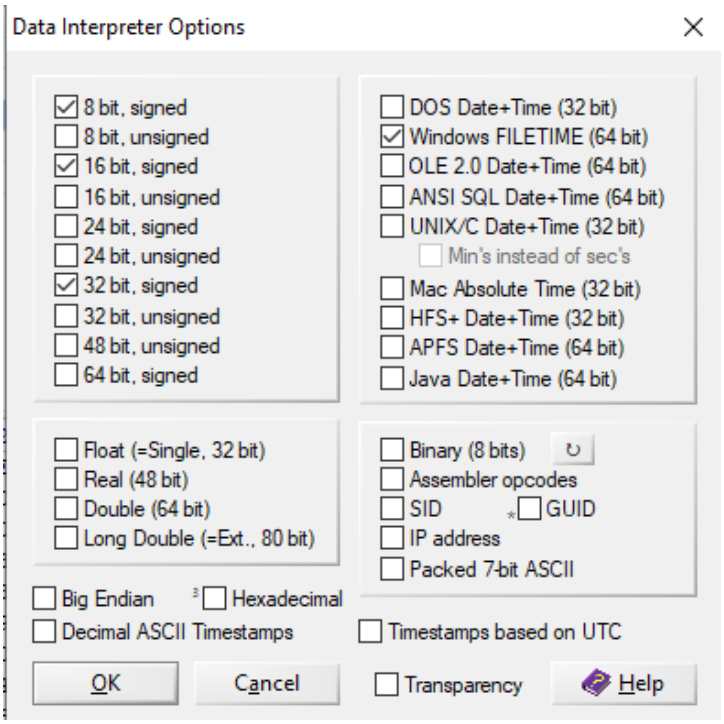
4. In the Select Mode dialog box, click **Read-Only Mode** (=**write protected**), as shown in Figure 2, and then click **OK**.



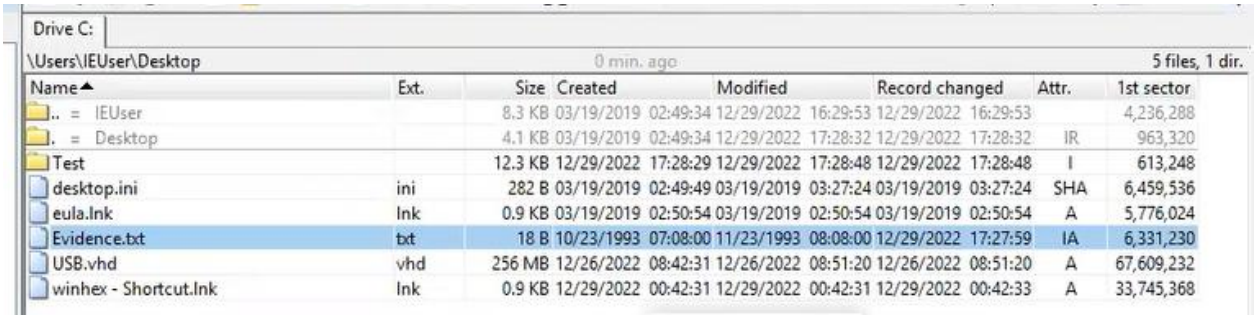
5. Click Tools, Open Disk from the menu



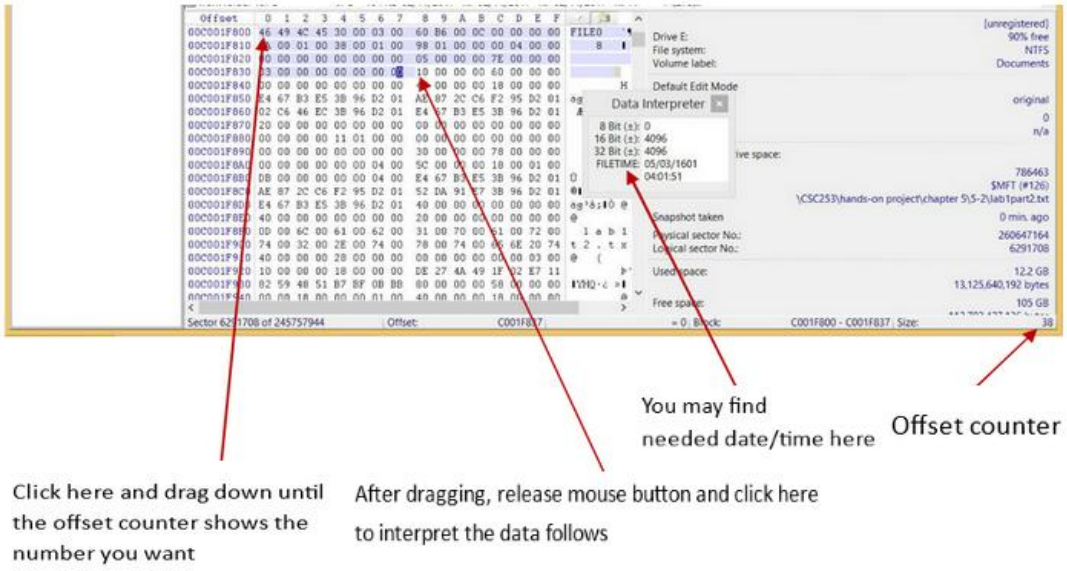
6. In the View Disk dialog box, click the drive where you saved the “Evidence.txt” text file from Task 1, and then click OK. If you’re prompted to take a new snapshot, click Take a new one. Depending on the size and quantity of data on your disk, it might take several minutes for WinHex to traverse all the files and paths on your disk drive.

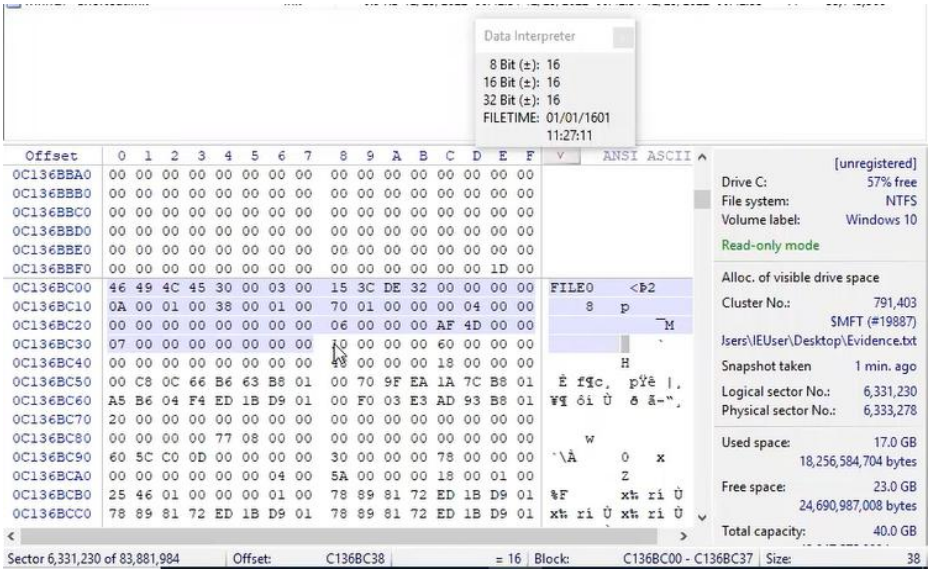


7. Click **Options**, **Data Interpreter** from the menu. In **the Data Interpreter Options** dialog box, click the **Win32 FILETIME (64 bit)** check box, shown in Figure 3, and then click **OK**. The Data Interpreter should then have FILETIME as an additional display item now.

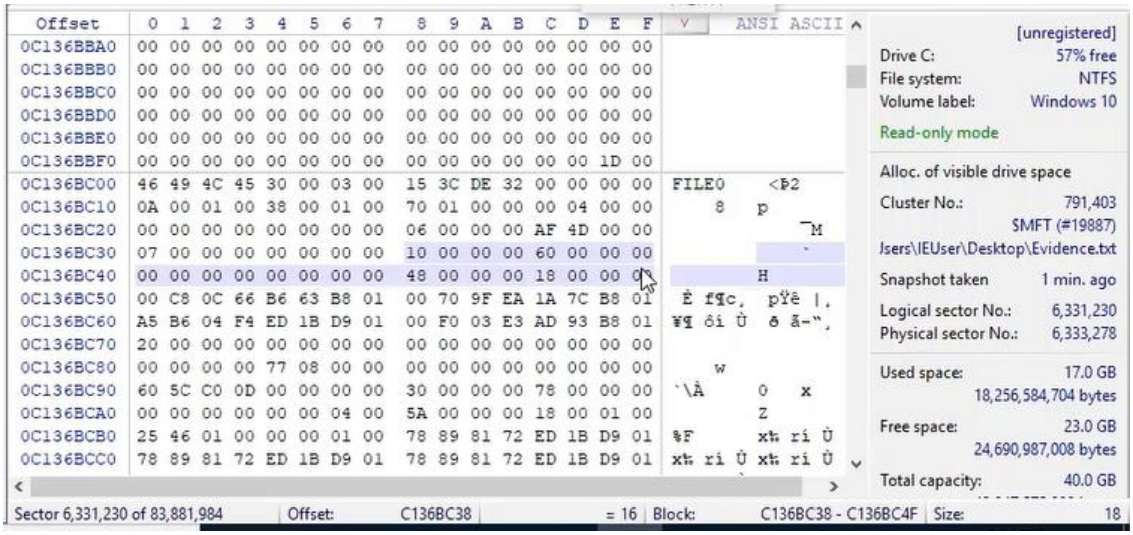


8. Now you need to navigate to your work folder where you saved your Evidence.txt in WinHex. In the upper-right pane of WinHex, scroll down until you see your work folder. Double-click each folder in the path and then click the Evidence.txt file.
9. Click at the beginning of the record, on the letter F in FILE, and then drag down and to the right while you monitor the hexadecimal counter in the lower-right corner. For example, the start of attribute 0x10 is at offset 0x38 from the beginning of the MFT record. To find the start of attribute 0x10, drag the cursor until the counter reaches 38. When the counter reaches 38, release the mouse button.

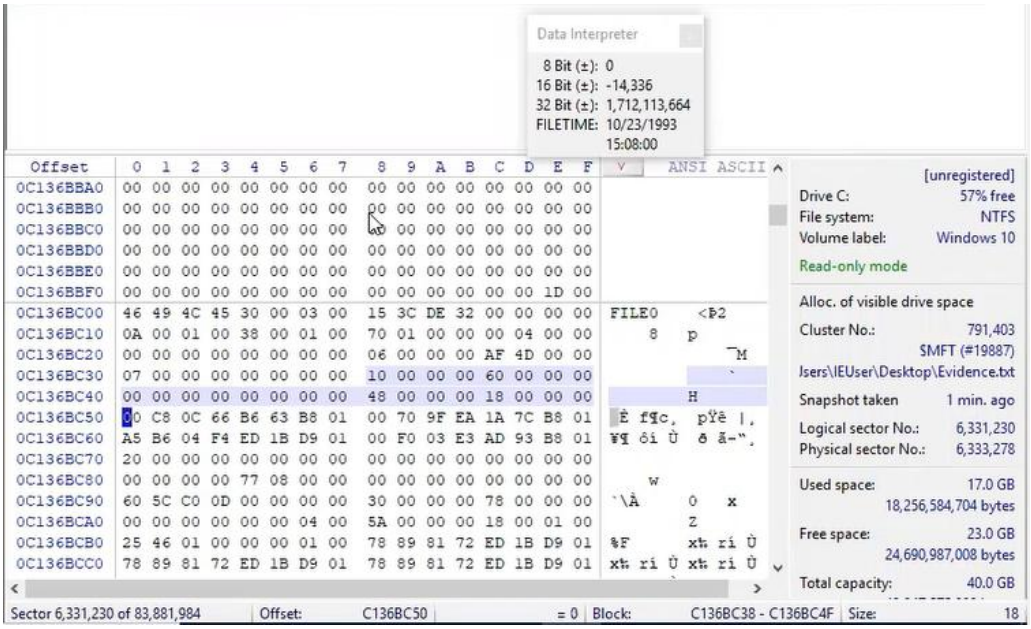




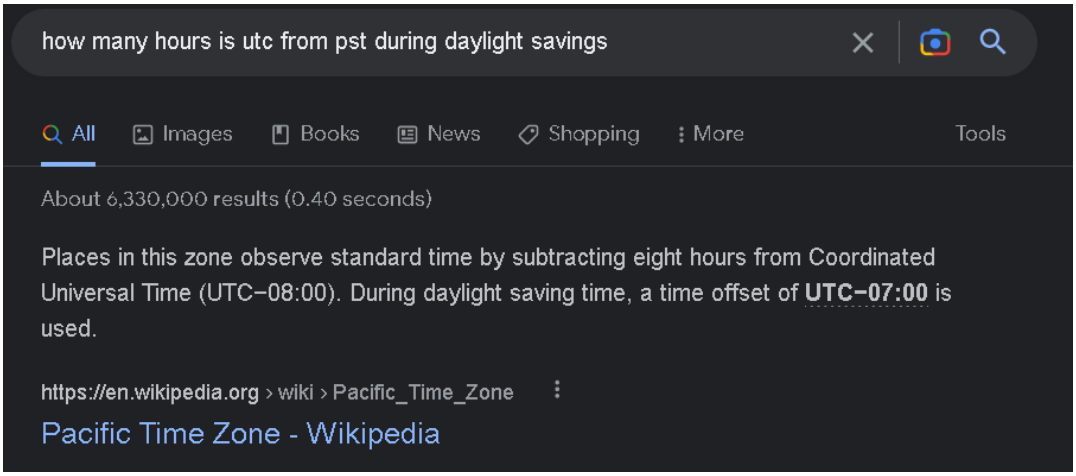
10. Your cursor should now be on the next byte.



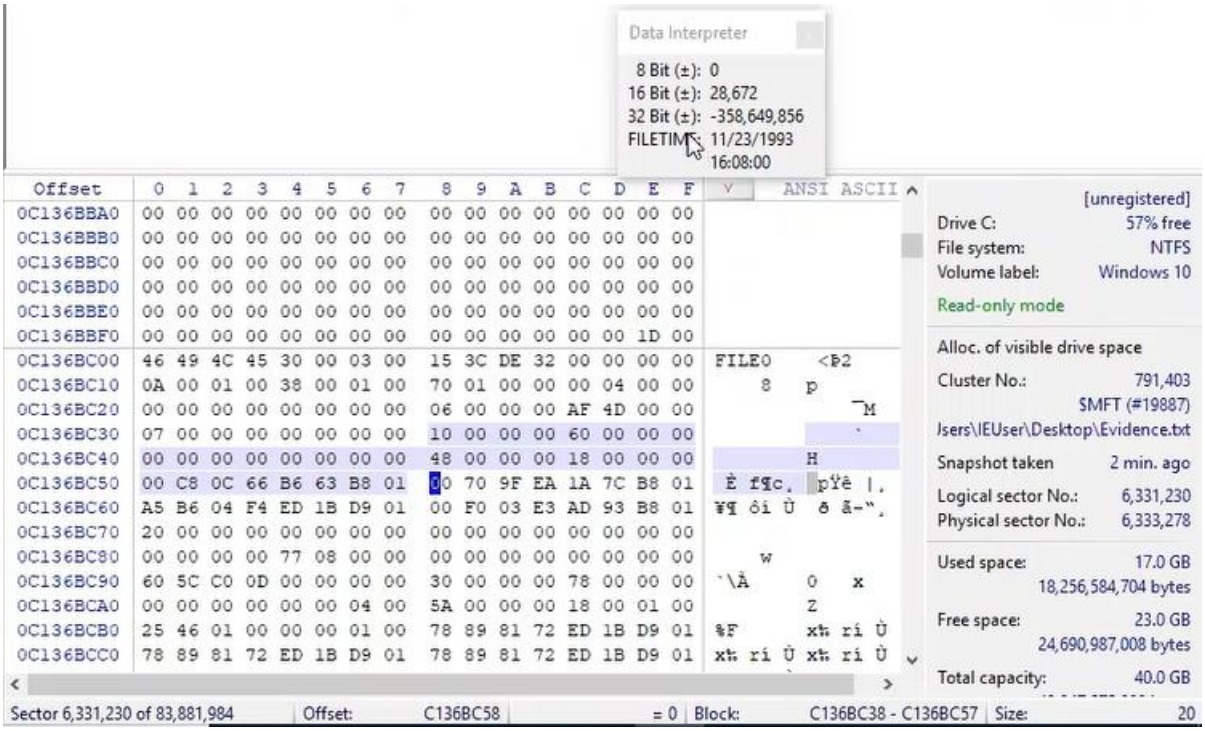
11. Click and drag until you are at offset 18.



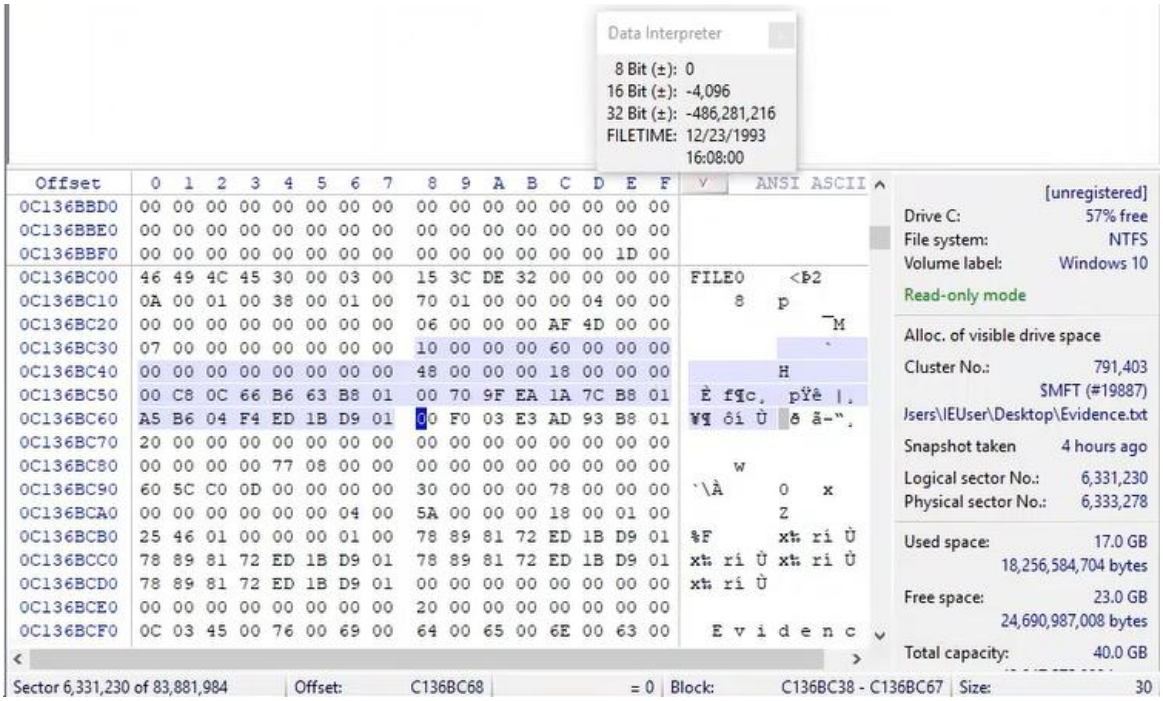
12. The next byte will show the spoofed time in the Data Interpreter.



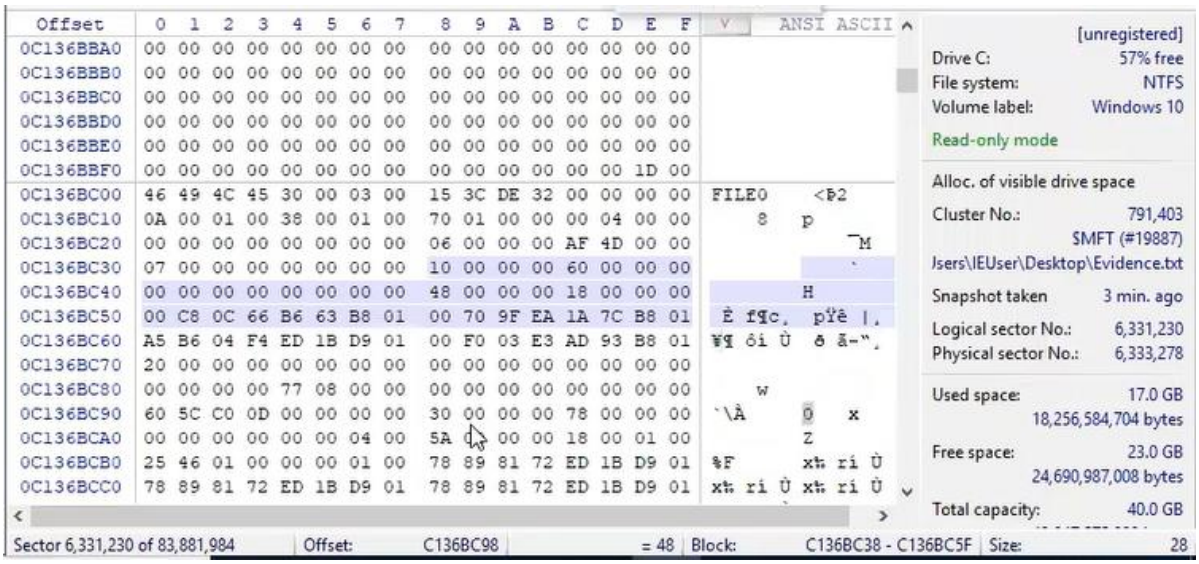
13. WinHex uses UTC time. By googling the Data Interpreter's time from UTC to PST, I can see the spoofed time in my time zone, PST. You may have a different time zone. Since 10/23 is during daylight savings time, if I subtract 7 hours from the time in WinHex which is 15:08 - 7:00 I end up with 8:08 which is my correct spoofed time.



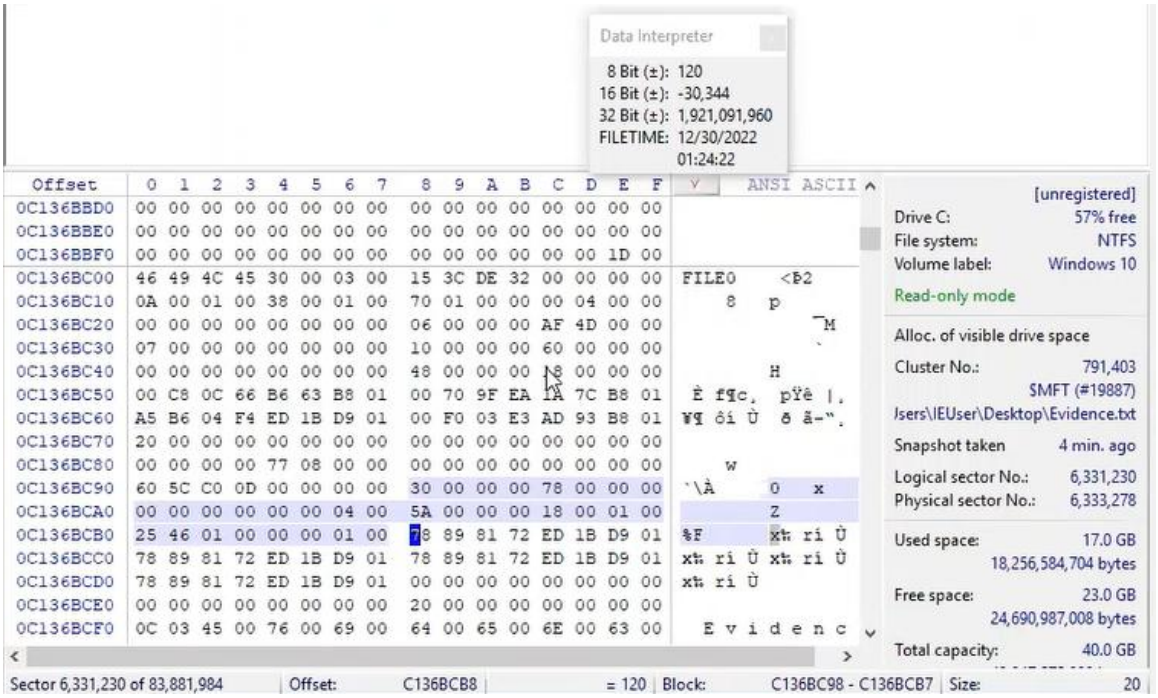
14. Offset 20 has the last modified date and time. 16:08 - 8:00 (because it's not daylight savings) is 11/23 8:08 which is correct.



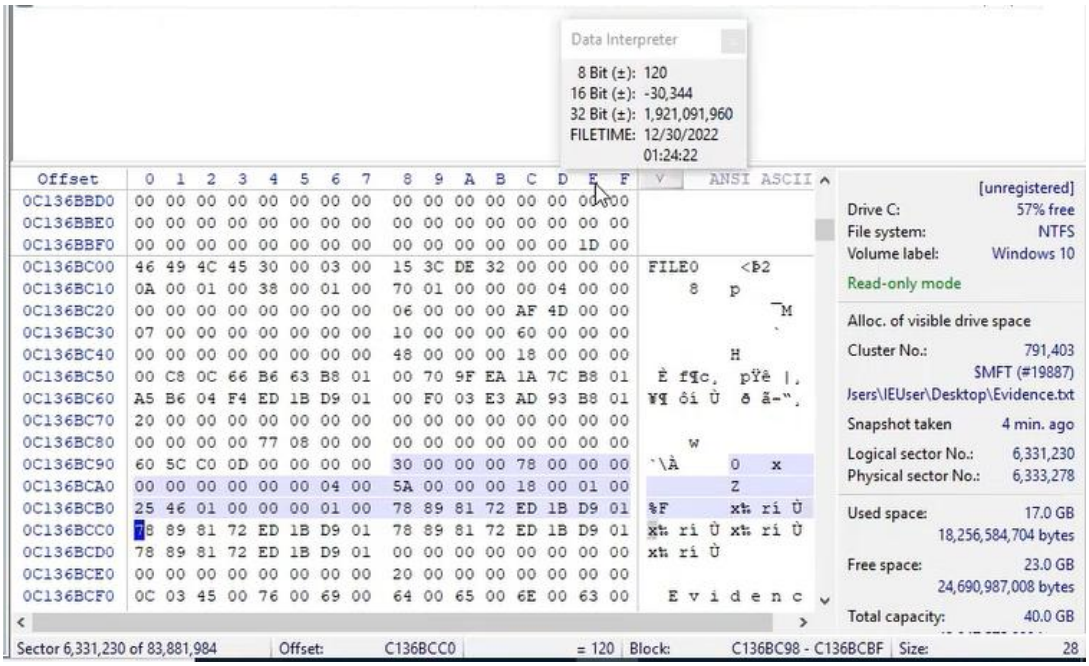
15. Offset 30 has the record access date and time. 16:08 - 8:00 = 12/23 8:08 is correct



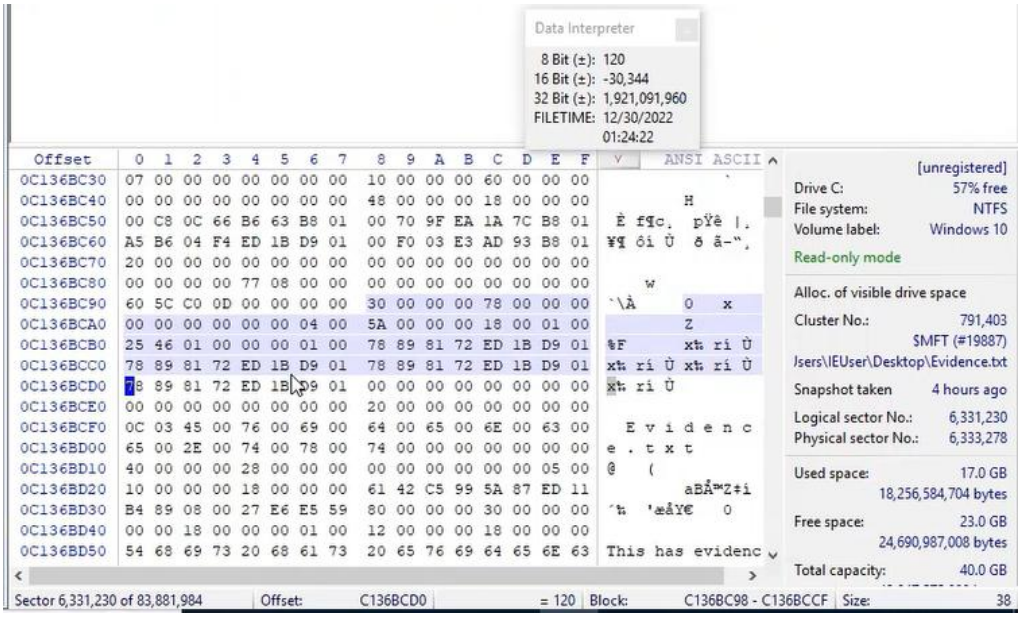
16. Now go to the next 30 Attribute to go to the File_Name data.



17. Offset 20 has the create date and time according to the system terminal, which cannot be edited by the user. 1:24- 8:00 (because daylight savings has ended) is equal to 5:24. And if I look back at my screenshots in Task 1 I can see that was actually when I created my Evidence.txt file.



18. Offset 28 has the last modified date and time which is 1:24 - 8:00 = 5:24.



19. Offset 38 has the record access date and time which is 1:24 - 8:00 = 5:24.

Questions:

1. What would be the command to set a file called “TextFile.txt” located in "C:\Users\IEUser\Desktop" to have a creation time of February 5, 1994 at 11:21:00?
2. Why is it recommended to use WinHex’s read-only mode in this situation?
3. Provide screenshots of your file’s timestomped created time and the created time shown in WinHex.
4. Explore the WinHex website and list at least 5 features of WinHex.
5. What’s the difference between the powershell commands get-item and get-childitem?