

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.

Virtual Machines

Test IE11 and Microsoft Edge Legacy using free Windows 10 virtual machines you download and manage locally

Select a download

Virtual Machines

MSEdge on Win10 (x64) Stable 1809

Choose a VM platform:

VirtualBox

Download .zip >

ⓘ Before installing, please note:

These virtual machines expire after 90 days. We recommend setting a snapshot when you first install the virtual machine which you can roll back to later. Mac users will need to use a tool that supports zip64, like [The Unarchiver](#), to unzip the files.
The password to your VM is "Passw0rd!"

Task 1. Install WinHex

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

Computer forensics software made in Germany

[Order now, get quotes](#)
[Upgrades, renewals](#)
Products

X-Ways Forensics
Integrated computer forensics software

X-Ways Investigator
Investigator version of X-Ways Forensics

Excire PhotoAI
Photo analysis with AI

WinHex
License types
Setup info
Forensic features
All features

X-Ways Imager
Disk imaging and more

Services
[Training](#)
[Certification](#)
[User forum](#)

[Contact X-Ways](#)
[Corporate info](#)

WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor

Windows XP/2003/Vista/2008/7/8/8.1/2012/10/2016/2019/11, 32 Bit/64 Bit*

WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of [computer forensics](#), [data recovery](#), low-level data processing, and IT security. An advanced tool for everyday and emergency use: inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from [digital camera cards](#). Features *depend on the license type* ([license type comparison](#)), among them:

- **Disk editor** for hard disks, floppy disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash, ...
- Native support for FAT12/16/32, exFAT, NTFS, Ext2/3/4, [Next3@](#), CDFS, UDF
- Built-in interpretation of RAID systems and dynamic disks
- Various data recovery techniques
- **RAM editor**, providing access to physical RAM and other processes' virtual memory
- **Data interpreter**, knowing 20 data types
- Editing data structures using [templates](#) (e.g. to repair partition table/boot sector)
- Concatenating and splitting files, unifying and dividing odd and even bytes/words
- **Analyzing** and comparing files
- Particularly flexible search and replace functions
- **Disk cloning** (under DOS with X-Ways Replica)
- Drive images & backups (optionally compressed or split into 650 MB archives)
- Simple **scripting**
- 256-bit AES encryption, checksums, CRC32, hashes (MD5, SHA-1, ...)
- Erase (wipe) confidential files securely, hard drive **cleansing** to protect your privacy
- Import all clipboard formats, incl. ASCII hex values
- Convert between binary, hex ASCII, Intel Hex, and Motorola S
- Character sets: ANSI ASCII, IBM ASCII, EBCDIC, (Unicode)
- Instant window switching, Printing, Random-number generator.
- Supports files of any size. Very fast. Easy to use. Extensive program help.
- **More**

Nov 15, 2022
WinHex 20.7

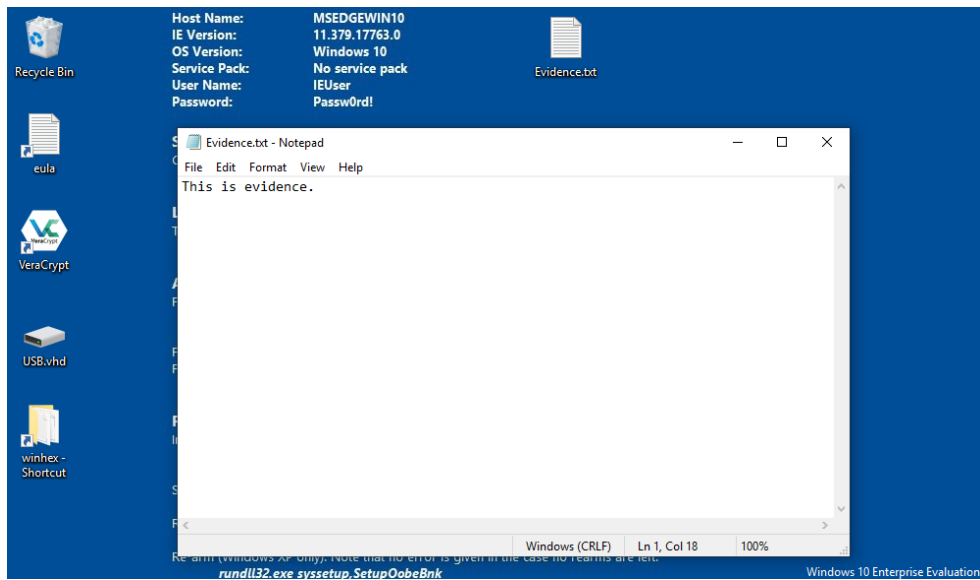
HEX
[Download](#)
[User manual](#)

Having all the bits and bytes in a computer at your fingertips has become a reality. Try before you buy. **Computer forensics edition of WinHex** with even more features: [X-Ways Forensics](#).

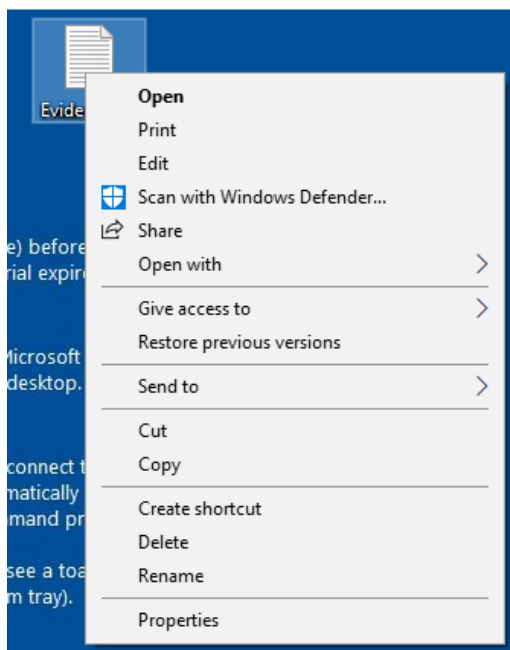
Task 2. Create a text file

The screenshot shows a Windows 10 desktop environment. On the left, there are icons for Recycle Bin, eula, VeraCrypt, USB.vhd, and winhex - Shortcut. The main area displays system information (Host Name: MSEDGEWIN10, IE Version: 11.379.17763.0, OS Version: Windows 10, Service Pack: No service pack, User Name: IEUser, Password: Passw0rd!), licensing notes, and activation instructions. A right-click context menu is open over the text area, showing options like View, Sort by, Refresh, Paste, Paste shortcut, Undo Delete, New, Display settings, and Personalize. The 'New' option is highlighted, and a sub-menu is visible showing 'Folder', 'Shortcut', 'Bitmap image', 'Contact', 'Rich Text Document', 'Text Document', and 'Compressed (zipped) Folder'. The 'Text Document' option is selected.

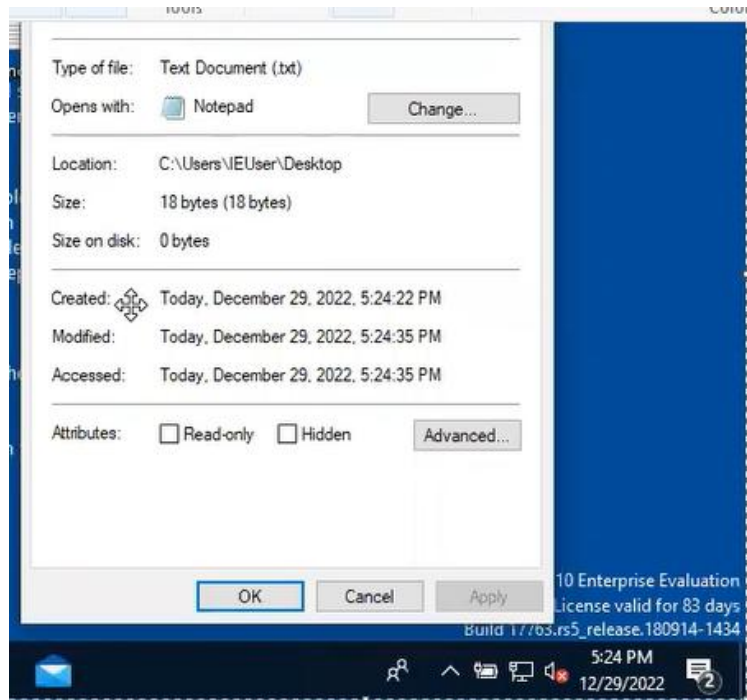
1. Right click where you would like to create a text file and navigate to New > "Text Document"



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

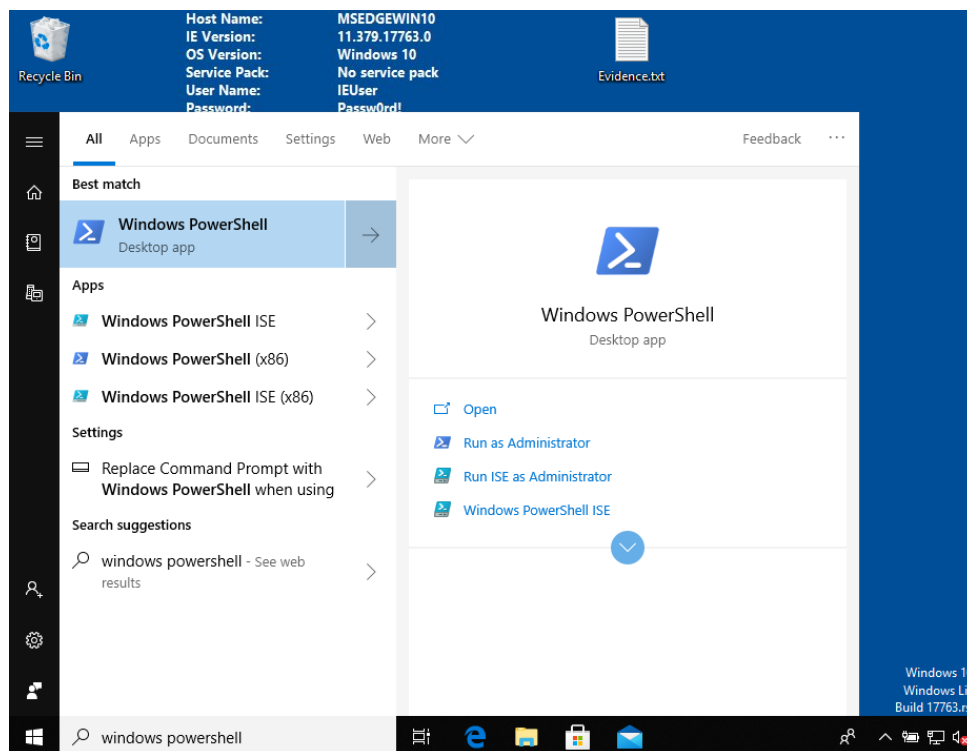


3. Right click your file and click "Properties".

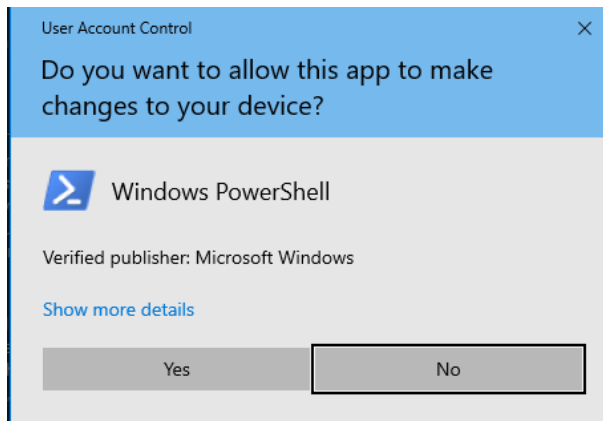


4. You should be able to see the file's location, created time, modified time, and accessed time. Take a screenshot of this (as well as the time you took the screenshot) or record this information somewhere.

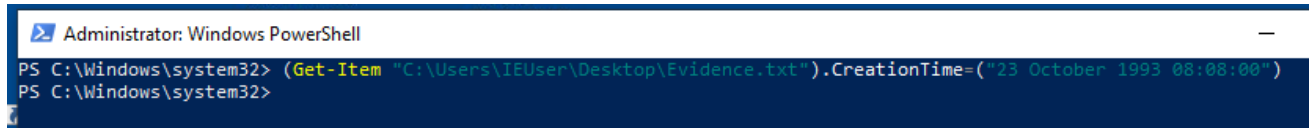
Task 3. Timestamp a file using Windows PowerShell



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



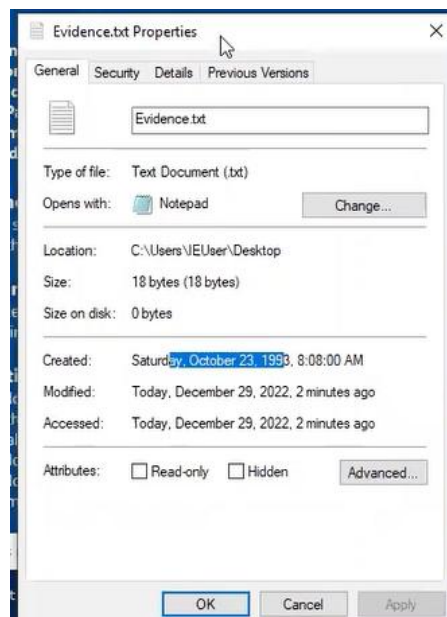
3. If you receive this pop up, click "Yes".



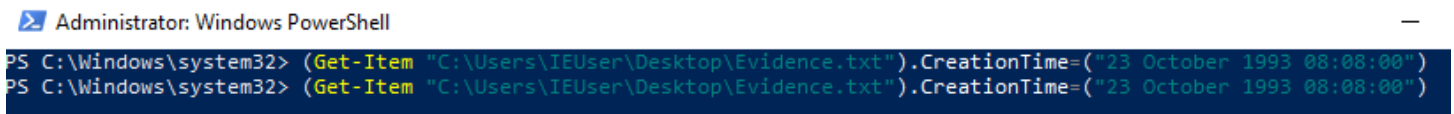
4. The command to change the creation time uses this format:
(Get-Item "[LOCATION]\[FILE NAME]").CreationTime=("DAY MONTH YEAR TIME")

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.



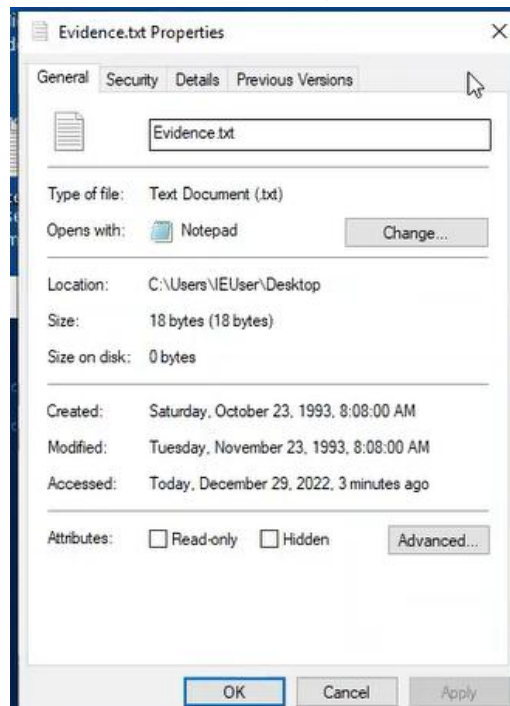
6. Press the up arrow to get a copy of the last command.



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:

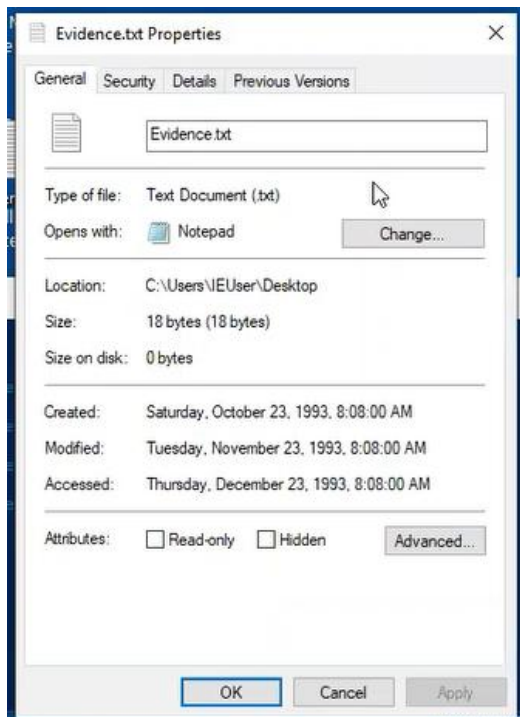
```
(Get-Item "C:\Users\IEUser\Desktop\Evidence.txt").LastAccessTime=("23 December 1993 08:08:00")
```

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
```

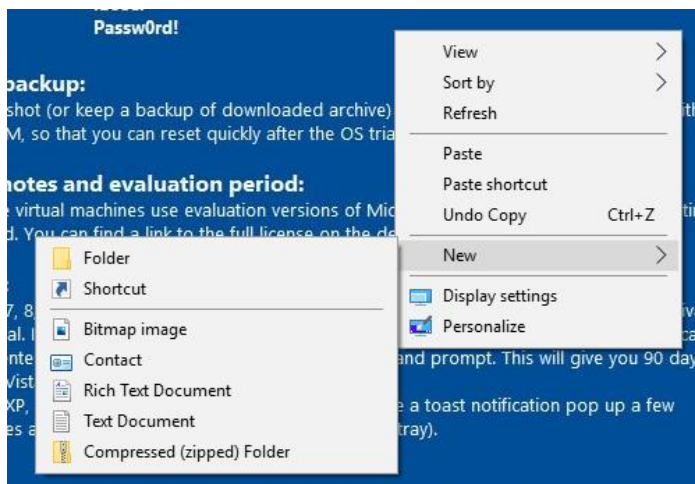
```
PS C:\Windows\system32> fsutil behavior set disablelastaccess 1
DisableLastAccess = 1 (User Managed, Enabled)
PS C:\Windows\system32>
```

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

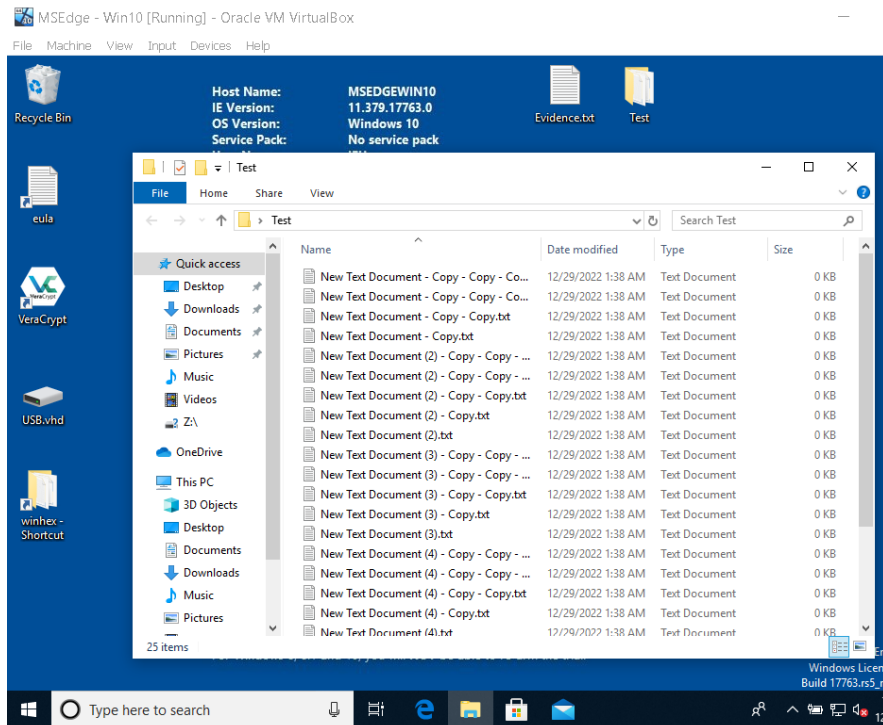


12. Now we can see that all the times have been changed.

Task 4. Create a directory with many files in it

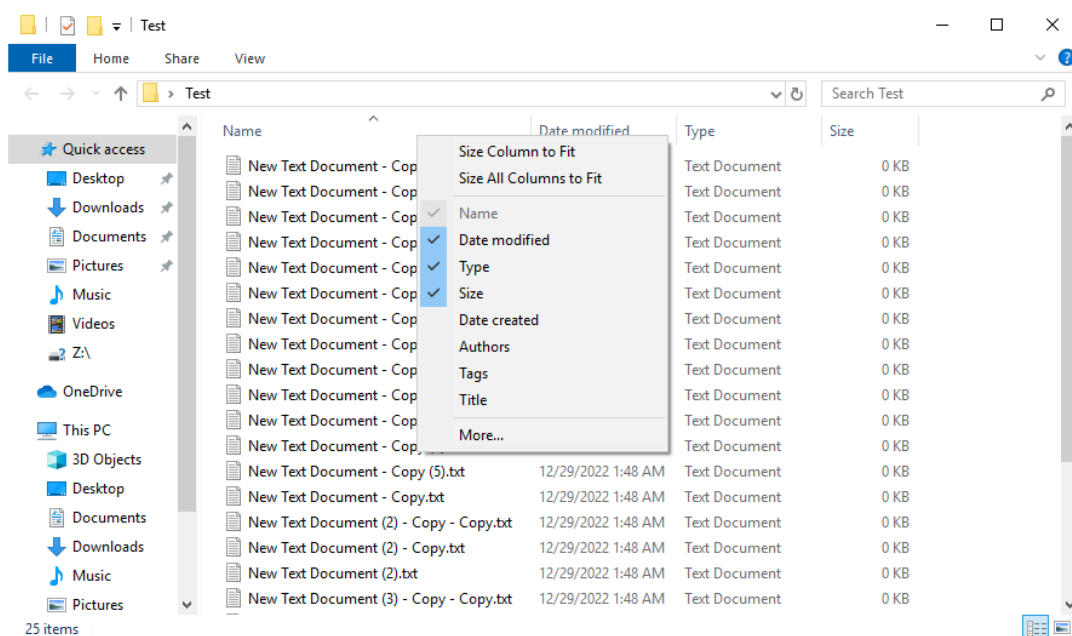


1. Right click where you would like to create a directory and navigate to New > Folder

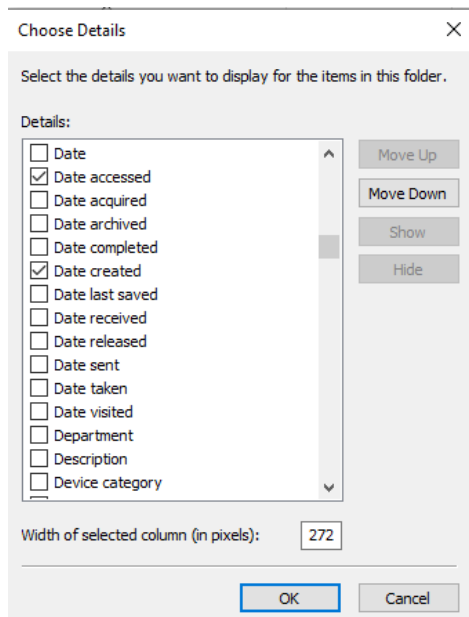


2. Name your folder and create many text files inside of it.

Task 5. Timestamp an entire directory using Windows Powershell



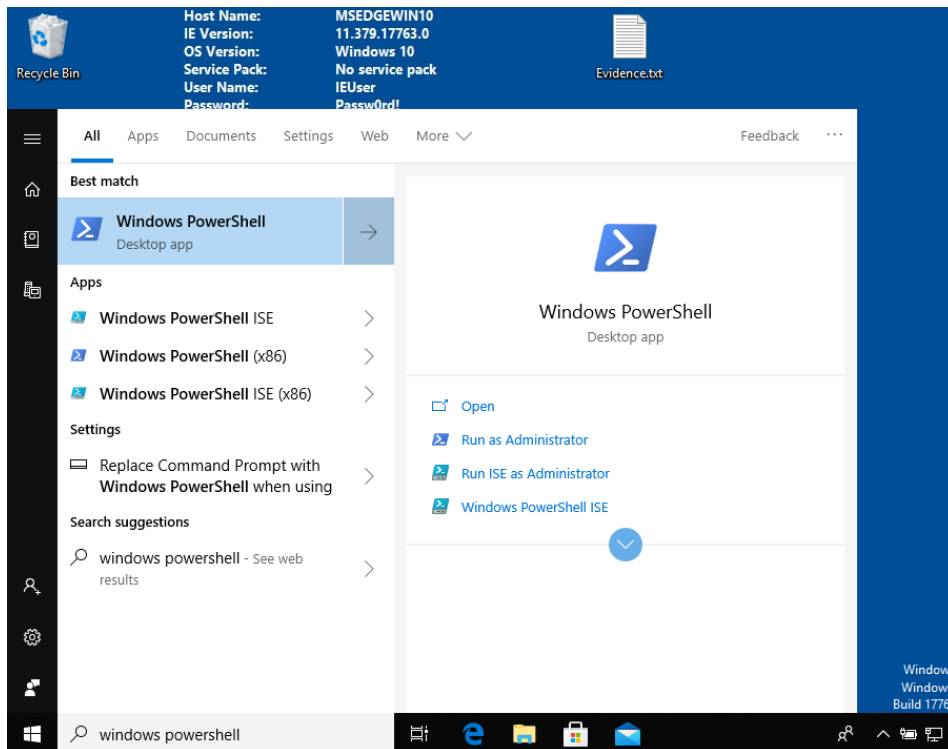
1. Right click the headers of the directory you just created and click "More..."



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"

Name	Date modified	Date accessed	Date created
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy (3).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy (4).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy (5).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy (3).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy (4).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy (5).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document (2) - Copy - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document (2) - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM
New Text Document (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	12/29/2022 1:48 AM

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>
```

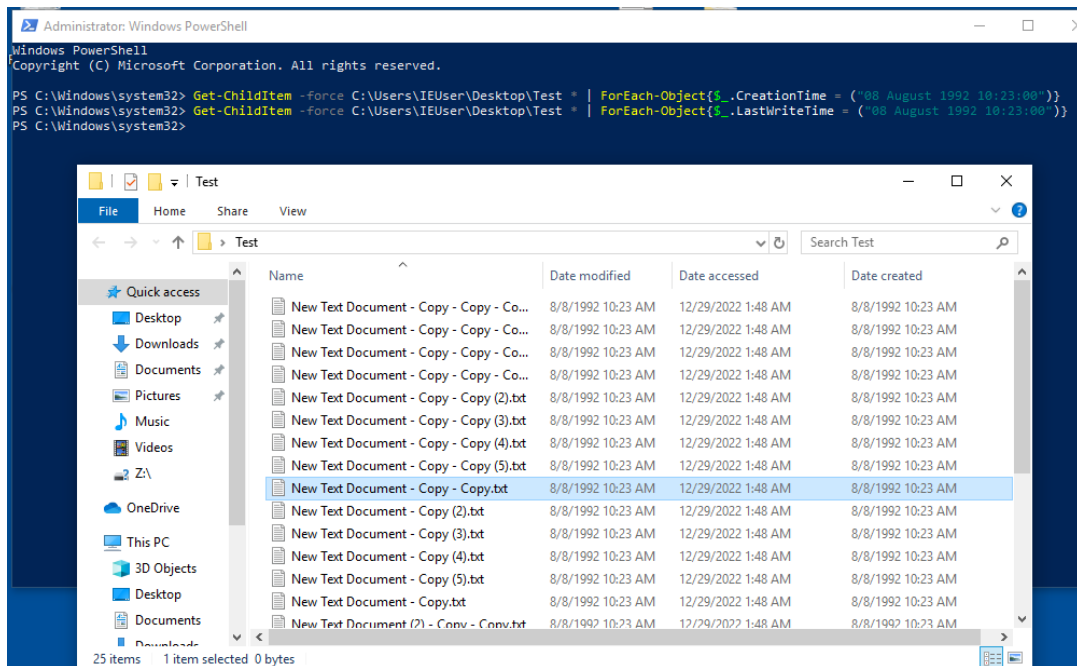
5. The command to change the creation time for a directory uses this format:
`Get-ChildItem -force [LOCATION]\[DIRECTORY NAME] * | ForEach-Object{$_CreationTime = ("DAY MONTH YEAR TIME")}`

Example command used in the image:

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

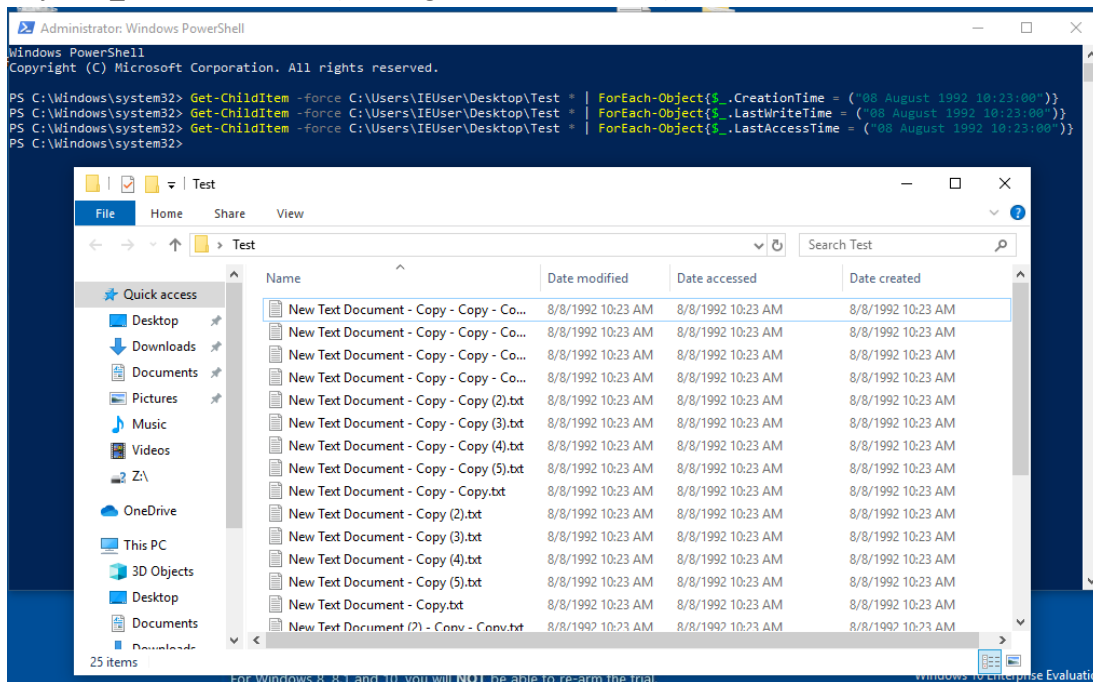
Name	Date modified	Date accessed	Date created
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy - Co...	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy (3).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy (4).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy (5).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy (3).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy (4).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy (5).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document (2) - Copy - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document (2) - Copy.txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM
New Text Document (2).txt	12/29/2022 1:48 AM	12/29/2022 1:48 AM	8/8/1992 10:23 AM

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:

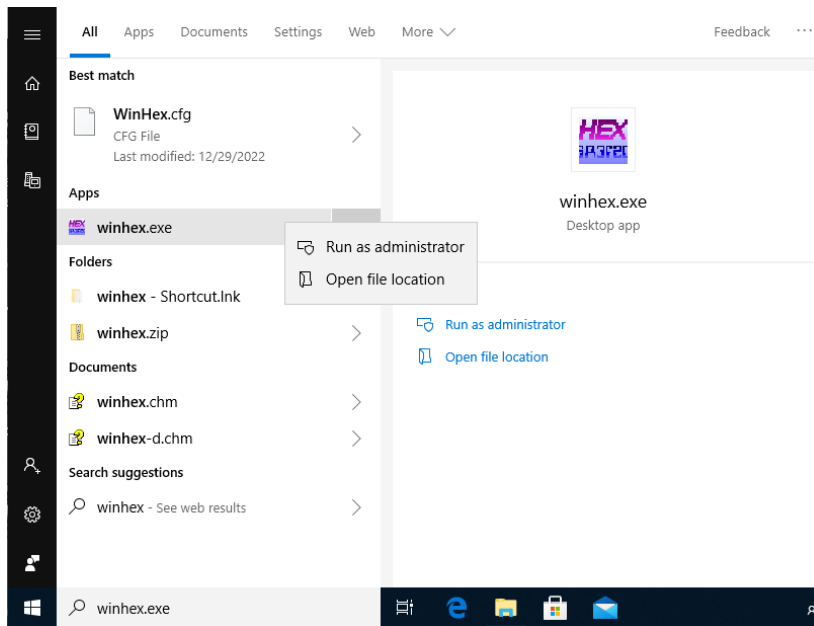
```
Get-ChildItem -force C:\Users\IEUser\Desktop\Test * | ForEach-Object{$_.LastWriteTime = ("08 August 1992 10:23:00")}
```



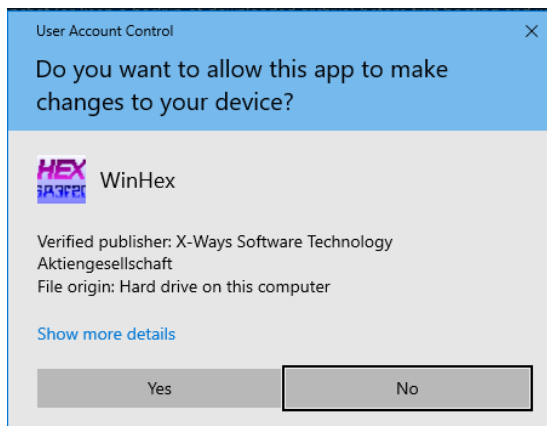
Example command used in the image:

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

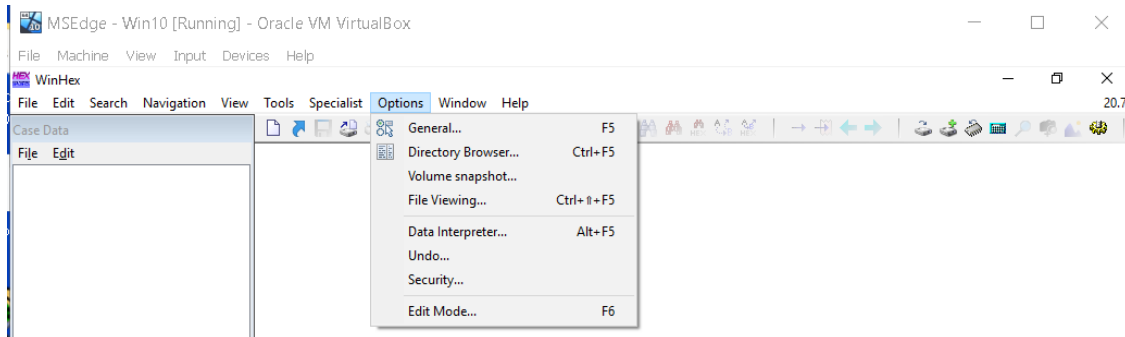
Task 6. Detect the timestomping using WinHex



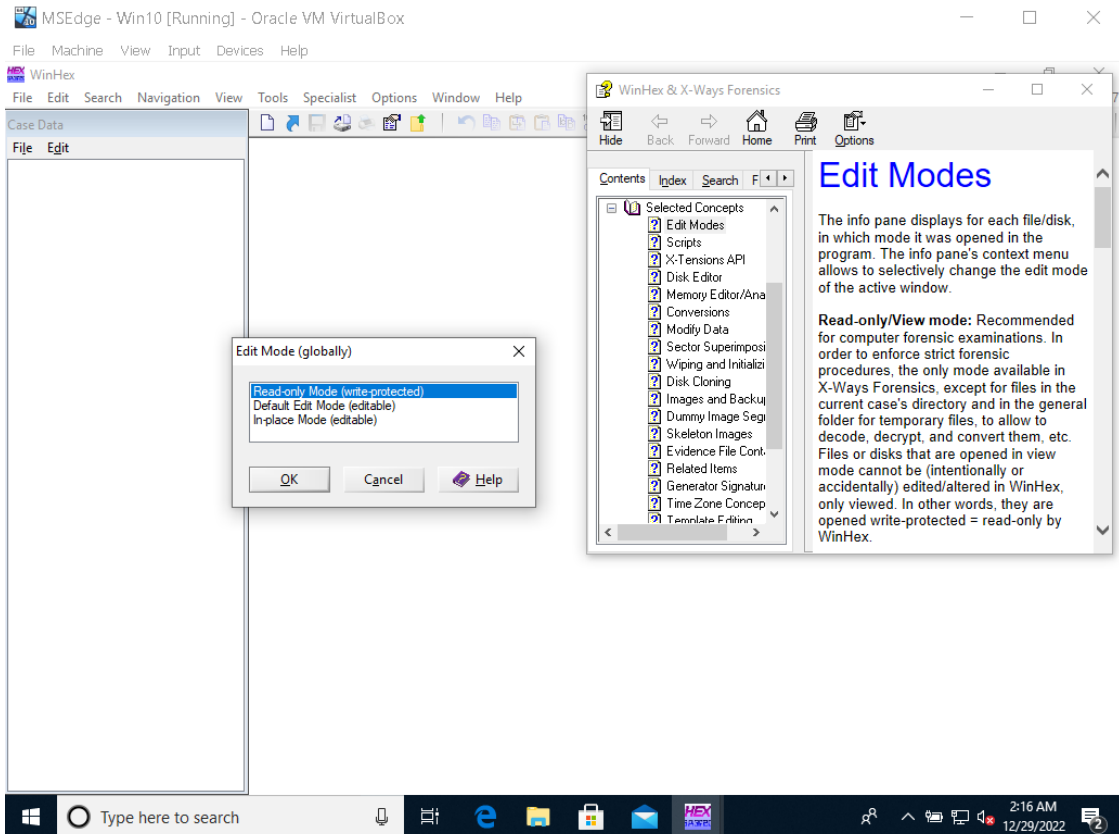
1. Run WinHex as an administrator



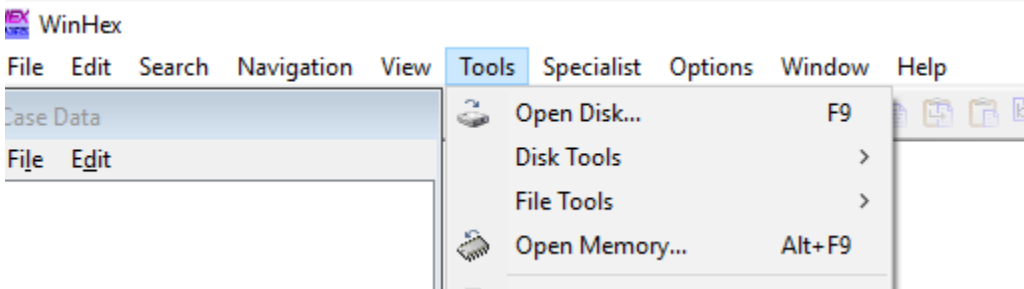
2. Click "Yes"



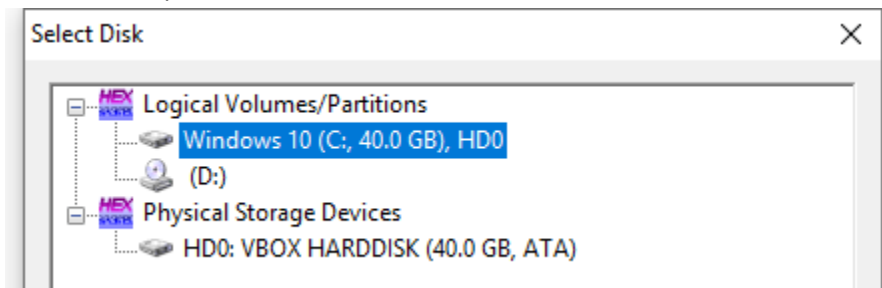
3. Navigate to Options > Edit Mode...



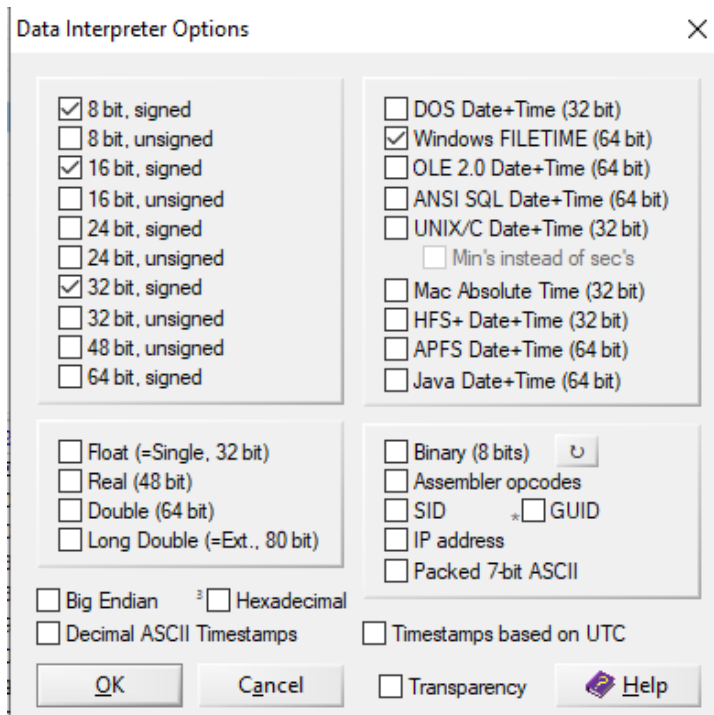
4. In the Select Mode dialog box, click **Read-Only Mode (=write protected)**, as shown in Figure 2, and then click **OK**.



5. Click Tools, Open Disk from the menu



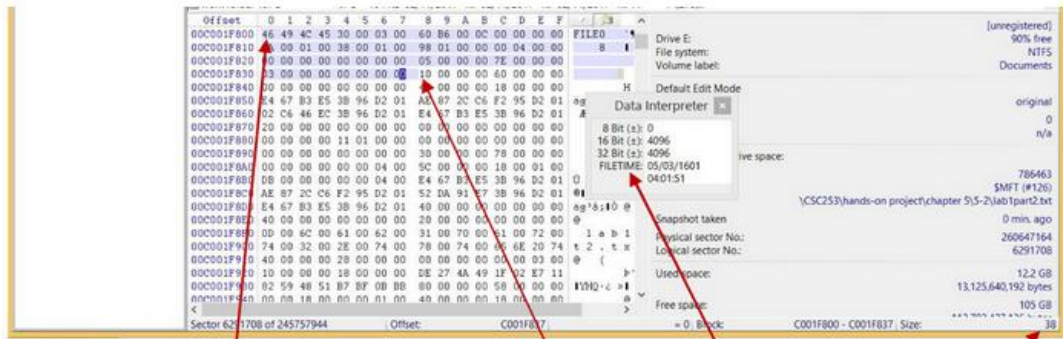
6. In the View Disk dialog box, click the drive where you saved the "Evidence.txt" text file from Task 1, and then click OK. If you're prompted to take a new snapshot, click Take a new one. Depending on the size and quantity of data on your disk, it might take several minutes for WinHex to traverse all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

Drive C:									
\Users\IEUser\Desktop									
0 min. ago									
5 files, 1 dir.									
Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector		
.. = IEUser		8.3 KB	03/19/2019 02:49:34	12/29/2022 16:29:53	12/29/2022 16:29:53		4,236,288		
. = Desktop		4.1 KB	03/19/2019 02:49:34	12/29/2022 17:28:32	12/29/2022 17:28:32	IR	963,320		
Test		12.3 KB	12/29/2022 17:28:29	12/29/2022 17:28:48	12/29/2022 17:28:48	I	613,248		
desktop.ini	ini	282 B	03/19/2019 02:49:49	03/19/2019 03:27:24	03/19/2019 03:27:24	SHA	6,459,536		
eula.lnk	lnk	0.9 KB	03/19/2019 02:50:54	03/19/2019 02:50:54	03/19/2019 02:50:54	A	5,776,024		
Evidence.txt	txt	18 B	10/23/1993 07:08:00	11/23/1993 08:08:00	12/29/2022 17:27:59	IA	6,331,230		
USB.vhd	vhd	256 MB	12/26/2022 08:42:31	12/26/2022 08:51:20	12/26/2022 08:51:20	A	67,609,232		
winhex - Shortcut.lnk	lnk	0.9 KB	12/29/2022 00:42:31	12/29/2022 00:42:31	12/29/2022 00:42:33	A	33,745,368		

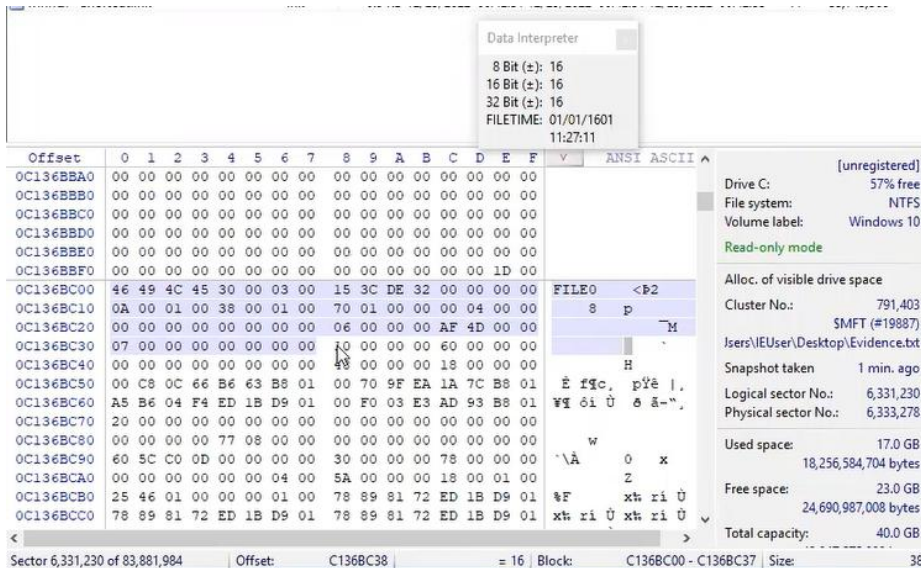
8. Now you need to navigate to your work folder where you saved your Evidence.txt in WinHex. In the upper-right pane of WinHex, scroll down until you see your work folder. Double-click each folder in the path and then click the Evidence.txt file.
9. Click at the beginning of the record, on the letter 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.



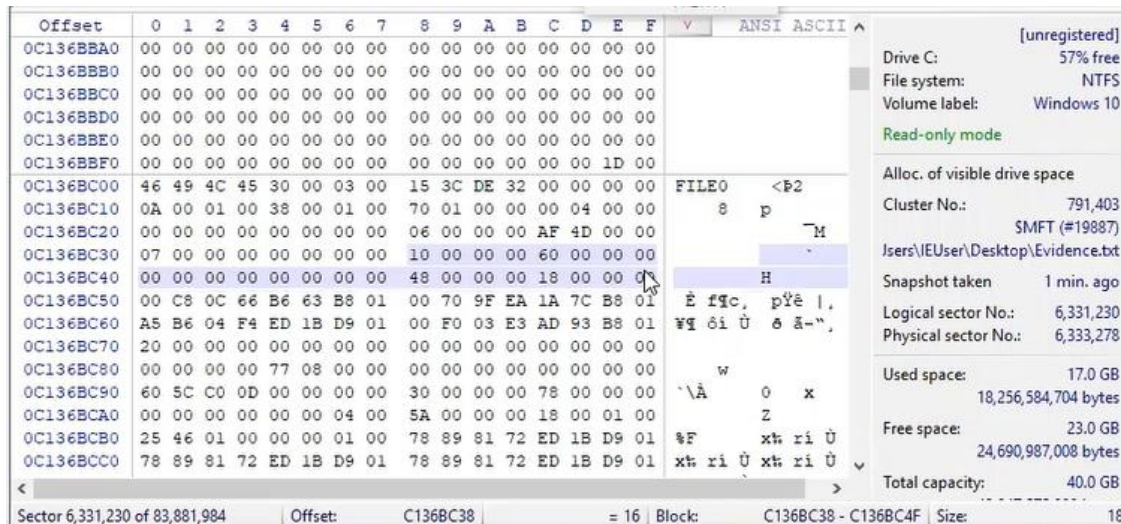
You may find needed date/time here Offset counter

Click here and drag down until the offset counter shows the number you want

After dragging, release mouse button and click here to interpret the data follows



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



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

Data Interpreter

8 Bit (±): 0
 16 Bit (±): -14,336
 32 Bit (±): 1,712,113,664
 FILETIME: 10/23/1993
 15:08:00

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		ANSI	ASCII
0C136BBA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BC00	46	49	4C	45	30	00	03	00	15	3C	DE	32	00	00	00	00	FILE0	<B2	
0C136BC10	0A	00	01	00	38	00	01	00	70	01	00	00	00	04	00	00	8	p	
0C136BC20	00	00	00	00	00	00	00	00	06	00	00	00	00	AF	4D	00		M	
0C136BC30	07	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00		H	
0C136BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
0C136BC50	00	C8	0C	66	B6	63	B8	01	00	70	9F	EA	1A	7C	B8	01	È fgc, pÿè l,		
0C136BC60	A5	B6	04	F4	ED	1B	D9	01	00	F0	03	E3	AD	93	B8	01	Wt ôi Û ô ä=".		
0C136BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BC80	00	00	00	00	77	08	00	00	00	00	00	00	00	00	00	00		w	
0C136BC90	60	5C	C0	0D	00	00	00	00	30	00	00	00	78	00	00	00	À	0 x	
0C136BCA0	00	00	00	00	00	00	04	00	5A	00	00	00	18	00	01	00		Z	
0C136BCB0	25	46	01	00	00	00	01	00	78	89	81	72	ED	1B	D9	01	%F	x% ri Û	
0C136BCC0	78	89	81	72	ED	1B	D9	01	78	89	81	72	ED	1B	D9	01	x% ri Û	x% ri Û	

Sector 6,331,230 of 83,881,984
Offset: C136BC50
= 0 Block: C136BC38 - C136BC4F
Size: 18

[unregistered]
 Drive C: 57% free
 File system: NTFS
 Volume label: Windows 10
 Read-only mode
 Alloc. of visible drive space
 Cluster No.: 791,403
 SMFT (#19887)
 IUsers\IEUser\Desktop\Evidence.txt
 Snapshot taken 1 min. ago
 Logical sector No.: 6,331,230
 Physical sector No.: 6,333,278
 Used space: 17.0 GB
 18,256,584,704 bytes
 Free space: 23.0 GB
 24,690,987,008 bytes
 Total capacity: 40.0 GB

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

how many hours is utc from pst during daylight savings

All
Images
Books
News
Shopping
More
Tools

About 6,330,000 results (0.40 seconds)

Places in this zone observe standard time by subtracting eight hours from Coordinated Universal Time (UTC-08:00). During daylight saving time, a time offset of **UTC-07:00** is used.

https://en.wikipedia.org/wiki/Pacific_Time_Zone

Pacific Time Zone - Wikipedia

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.

Data Interpreter																
8 Bit (±): 0																
16 Bit (±): 28,672																
32 Bit (±): -358,649,856																
FILETIME: 11/23/1993																
16:08:00																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0C136BBA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	1D	00	
0C136BC00	46	49	4C	45	30	00	03	00	15	3C	DE	32	00	00	00	00
0C136BC10	0A	00	01	00	38	00	01	00	70	01	00	00	00	04	00	00
0C136BC20	00	00	00	00	00	00	00	00	06	00	00	00	AF	4D	00	00
0C136BC30	07	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
0C136BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
0C136BC50	00	C8	0C	66	B6	63	B8	01	00	70	9F	EA	1A	7C	B8	01
0C136BC60	A5	B6	04	F4	ED	1B	D9	01	00	F0	03	E3	AD	93	B8	01
0C136BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BC80	00	00	00	00	77	08	00	00	00	00	00	00	00	00	00	00
0C136BC90	60	5C	C0	0D	00	00	00	00	30	00	00	00	78	00	00	00
0C136BCA0	00	00	00	00	00	00	04	00	5A	00	00	00	18	00	01	00
0C136BCB0	25	46	01	00	00	00	01	00	78	89	81	72	ED	1B	D9	01
0C136BCC0	78	89	81	72	ED	1B	D9	01	78	89	81	72	ED	1B	D9	01

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.

Data Interpreter																
8 Bit (±): 0																
16 Bit (±): -4,096																
32 Bit (±): -486,281,216																
FILETIME: 12/23/1993																
16:08:00																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0C136BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	1D	00	
0C136BC00	46	49	4C	45	30	00	03	00	15	3C	DE	32	00	00	00	00
0C136BC10	0A	00	01	00	38	00	01	00	70	01	00	00	00	04	00	00
0C136BC20	00	00	00	00	00	00	00	00	06	00	00	00	AF	4D	00	00
0C136BC30	07	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
0C136BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
0C136BC50	00	C8	0C	66	B6	63	B8	01	00	70	9F	EA	1A	7C	B8	01
0C136BC60	A5	B6	04	F4	ED	1B	D9	01	00	F0	03	E3	AD	93	B8	01
0C136BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C136BC80	00	00	00	00	77	08	00	00	00	00	00	00	00	00	00	00
0C136BC90	60	5C	C0	0D	00	00	00	00	30	00	00	00	78	00	00	00
0C136BCA0	00	00	00	00	00	00	04	00	5A	00	00	00	18	00	01	00
0C136BCB0	25	46	01	00	00	00	01	00	78	89	81	72	ED	1B	D9	01
0C136BCC0	78	89	81	72	ED	1B	D9	01	78	89	81	72	ED	1B	D9	01
0C136BCD0	78	89	81	72	ED	1B	D9	01	00	00	00	00	00	00	00	00
0C136BCE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
0C136BCF0	0C	03	45	00	76	00	69	00	64	00	65	00	6E	00	63	00

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI ASCII	
0C136BBA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1D	00		
0C136BC00	46	49	4C	45	30	00	03	00	15	3C	DE	32	00	00	00	00	FILE0	<B2	
0C136BC10	0A	00	01	00	38	00	01	00	70	01	00	00	00	04	00	00	8	p	
0C136BC20	00	00	00	00	00	00	00	00	06	00	00	00	AF	4D	00	00			
0C136BC30	07	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00			
0C136BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
0C136BC50	00	C8	0C	66	B6	63	B8	01	00	70	9F	EA	1A	7C	B8	01			
0C136BC60	A5	B6	04	F4	ED	1B	D9	01	00	F0	03	E3	AD	93	B8	01			
0C136BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BC80	00	00	00	00	77	08	00	00	00	00	00	00	00	00	00	00			
0C136BC90	60	5C	C0	0D	00	00	00	00	30	00	00	00	78	00	00	00			
0C136BCA0	00	00	00	00	00	00	04	00	5A	00	00	00	18	00	01	00			
0C136BCB0	25	46	01	00	00	00	01	00	78	89	81	72	ED	1B	D9	01			
0C136BCC0	78	89	81	72	ED	1B	D9	01	78	89	81	72	ED	1B	D9	01			

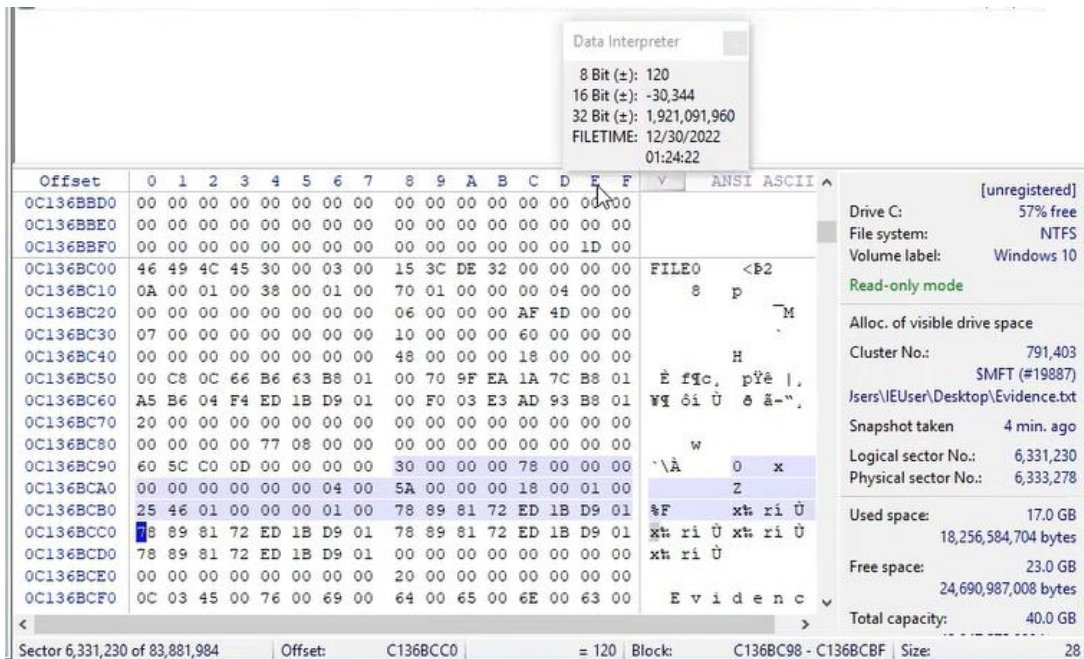
Sector 6,331,230 of 83,881,984 Offset: C136BC98 = 48 Block: C136BC38 - C136BC5F Size: 28

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

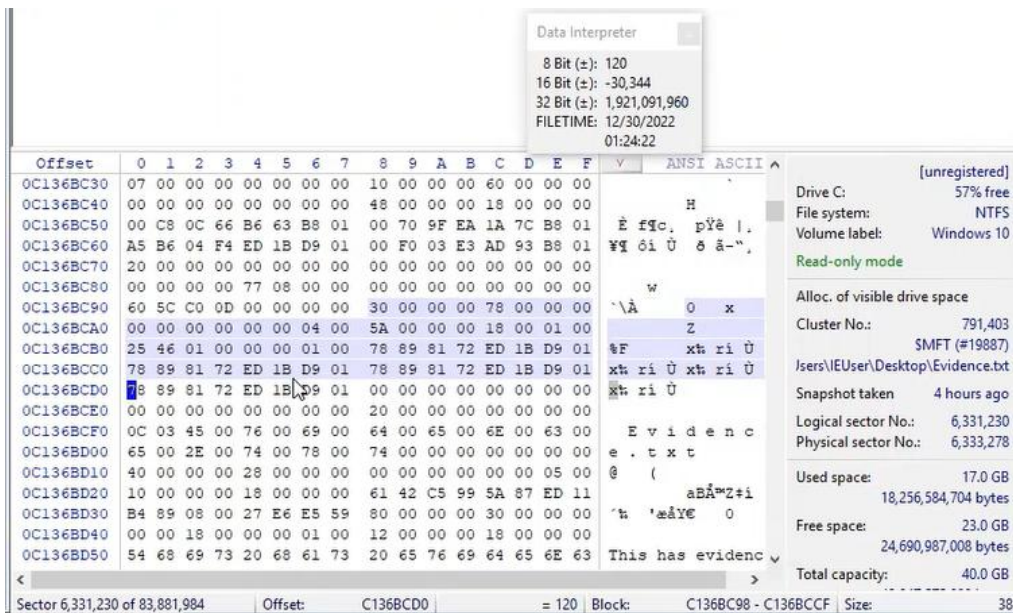
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI ASCII	
0C136BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1D	00		
0C136BC00	46	49	4C	45	30	00	03	00	15	3C	DE	32	00	00	00	00	FILE0	<B2	
0C136BC10	0A	00	01	00	38	00	01	00	70	01	00	00	00	04	00	00	8	p	
0C136BC20	00	00	00	00	00	00	00	00	06	00	00	00	AF	4D	00	00			
0C136BC30	07	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00			
0C136BC40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
0C136BC50	00	C8	0C	66	B6	63	B8	01	00	70	9F	EA	1A	7C	B8	01			
0C136BC60	A5	B6	04	F4	ED	1B	D9	01	00	F0	03	E3	AD	93	B8	01			
0C136BC70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
0C136BC80	00	00	00	00	77	08	00	00	00	00	00	00	00	00	00	00			
0C136BC90	60	5C	C0	0D	00	00	00	00	30	00	00	00	78	00	00	00			
0C136BCA0	00	00	00	00	00	00	04	00	5A	00	00	00	18	00	01	00			
0C136BCB0	25	46	01	00	00	00	01	00	78	89	81	72	ED	1B	D9	01			
0C136BCC0	78	89	81	72	ED	1B	D9	01	78	89	81	72	ED	1B	D9	01			
0C136BCD0	78	89	81	72	ED	1B	D9	01	00	00	00	00	00	00	00	00			
0C136BCE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
0C136BCF0	0C	03	45	00	76	00	69	00	64	00	65	00	6E	00	63	00			

Sector 6,331,230 of 83,881,984 Offset: C136BCB8 = 120 Block: C136BC98 - C136BCB7 Size: 20

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 timestamped 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?