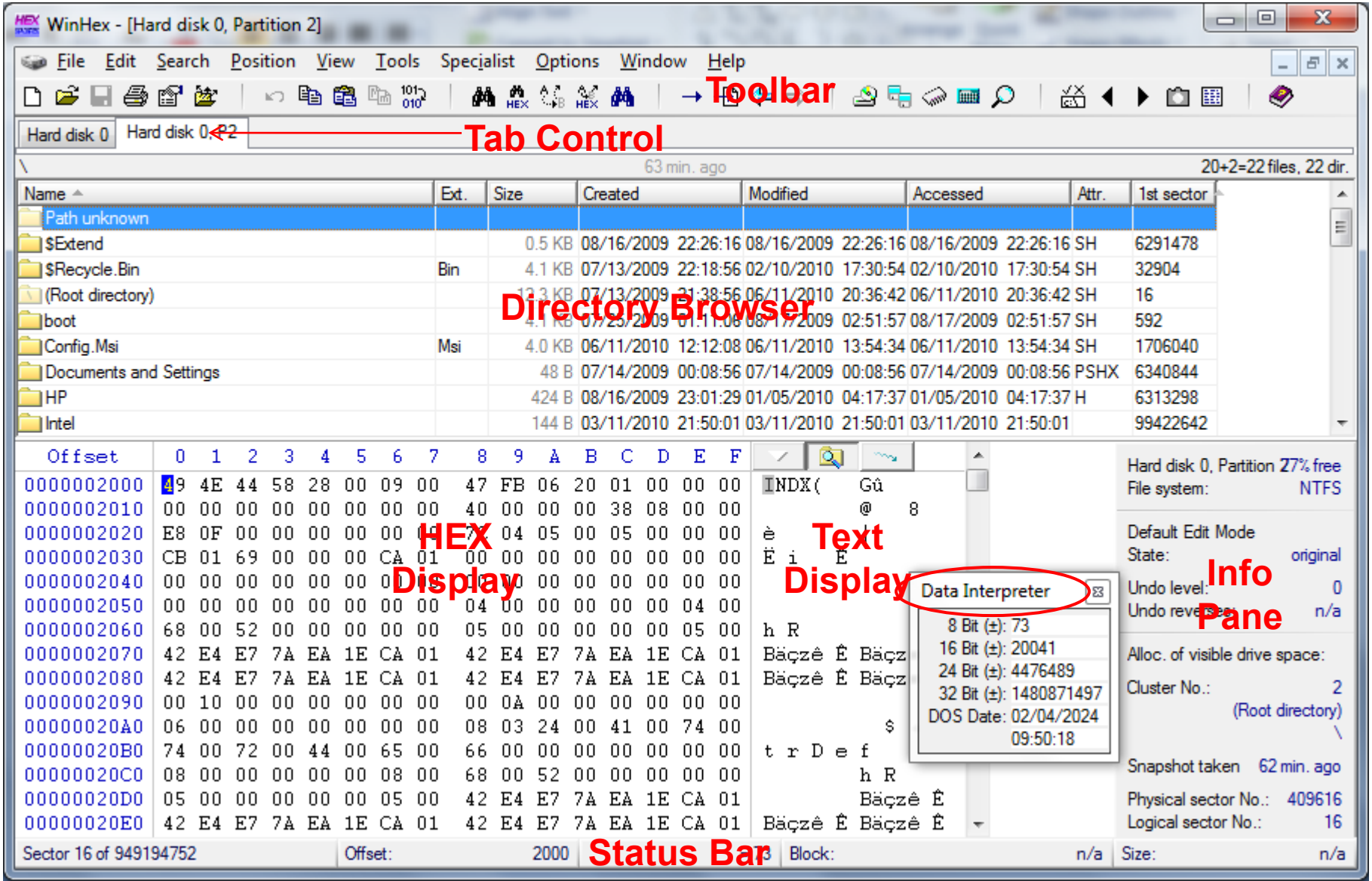
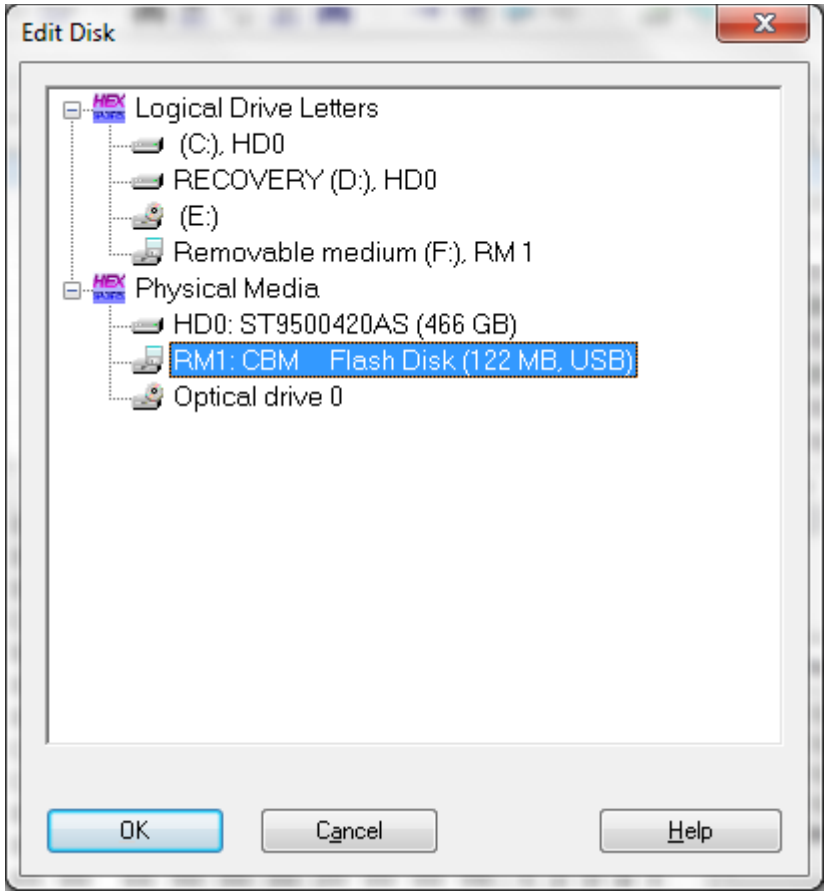
Intro to WinHex

Graphical User Interface

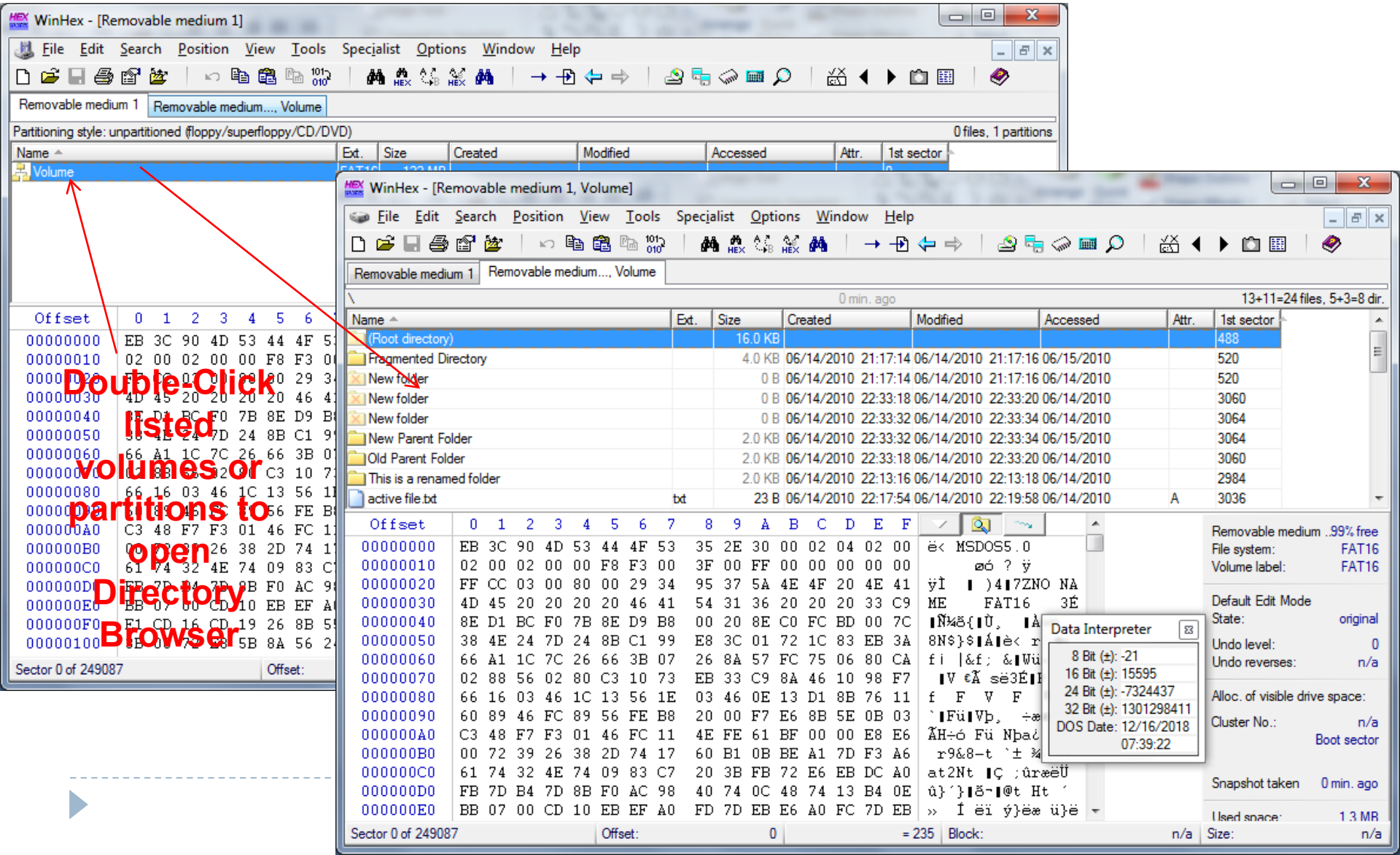


Opening a disk

- If using Vista or Win7, must run WinHex with elevated permissions by selecting the "Run as Administrator" option when launching the program.
  - Without elevated permissions, physical devices can not be accessed.
- From the WinHex GUI menu, select "Tools/Open Disk"
- Select the disk you wish to open and click "OK"



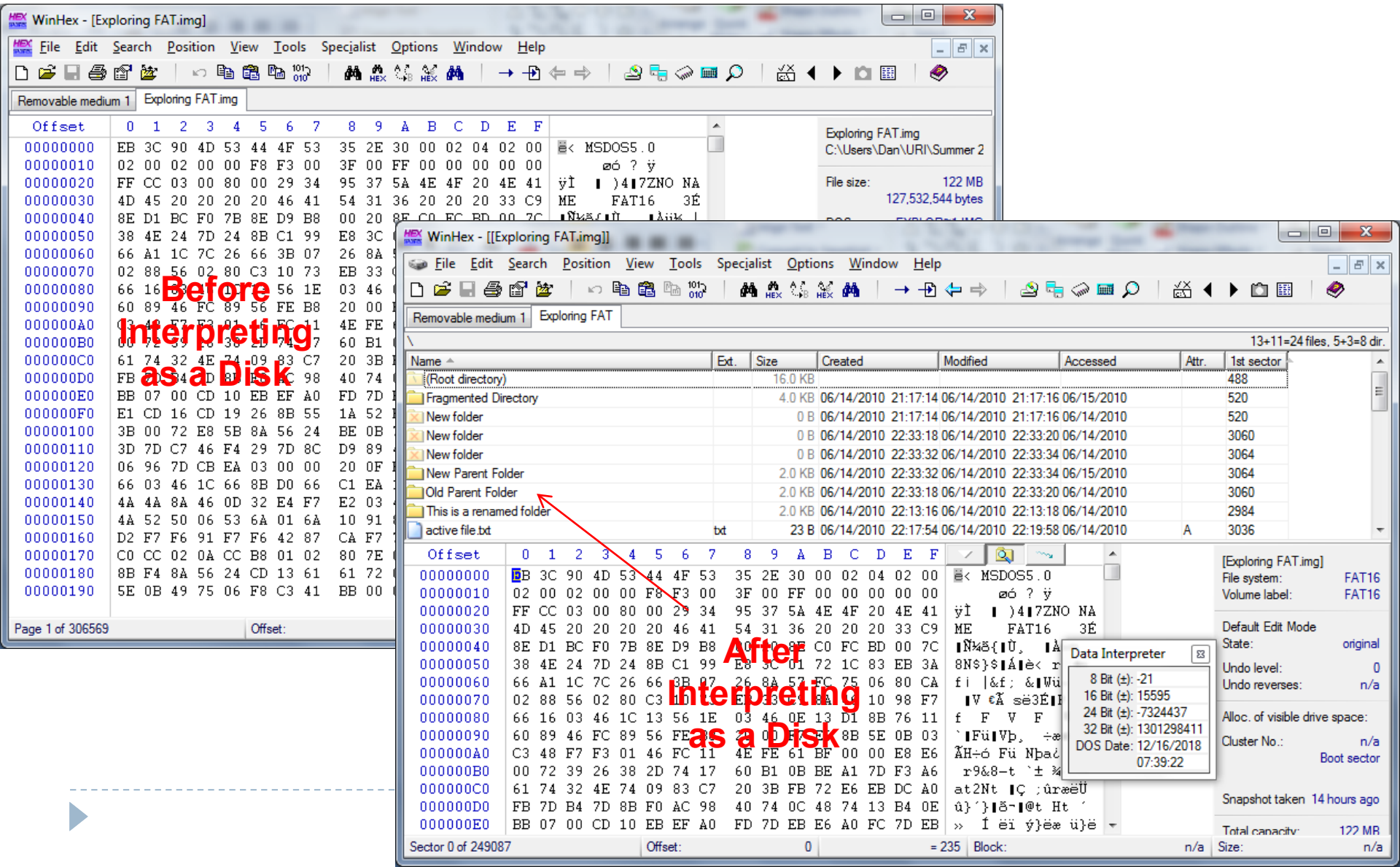
Opening a disk



Opening a forensic bit-stream image

- From the WinHex GUI menu, select "File/Open" or click on the "Open" button on the Toolbar
- Browse to your image file, select it and click "Open"
- You must tell WinHex that this file is an image of a disk so that can interpret the raw data.
  - From the menu, select "Specialist/Interpret Image File As Disk"

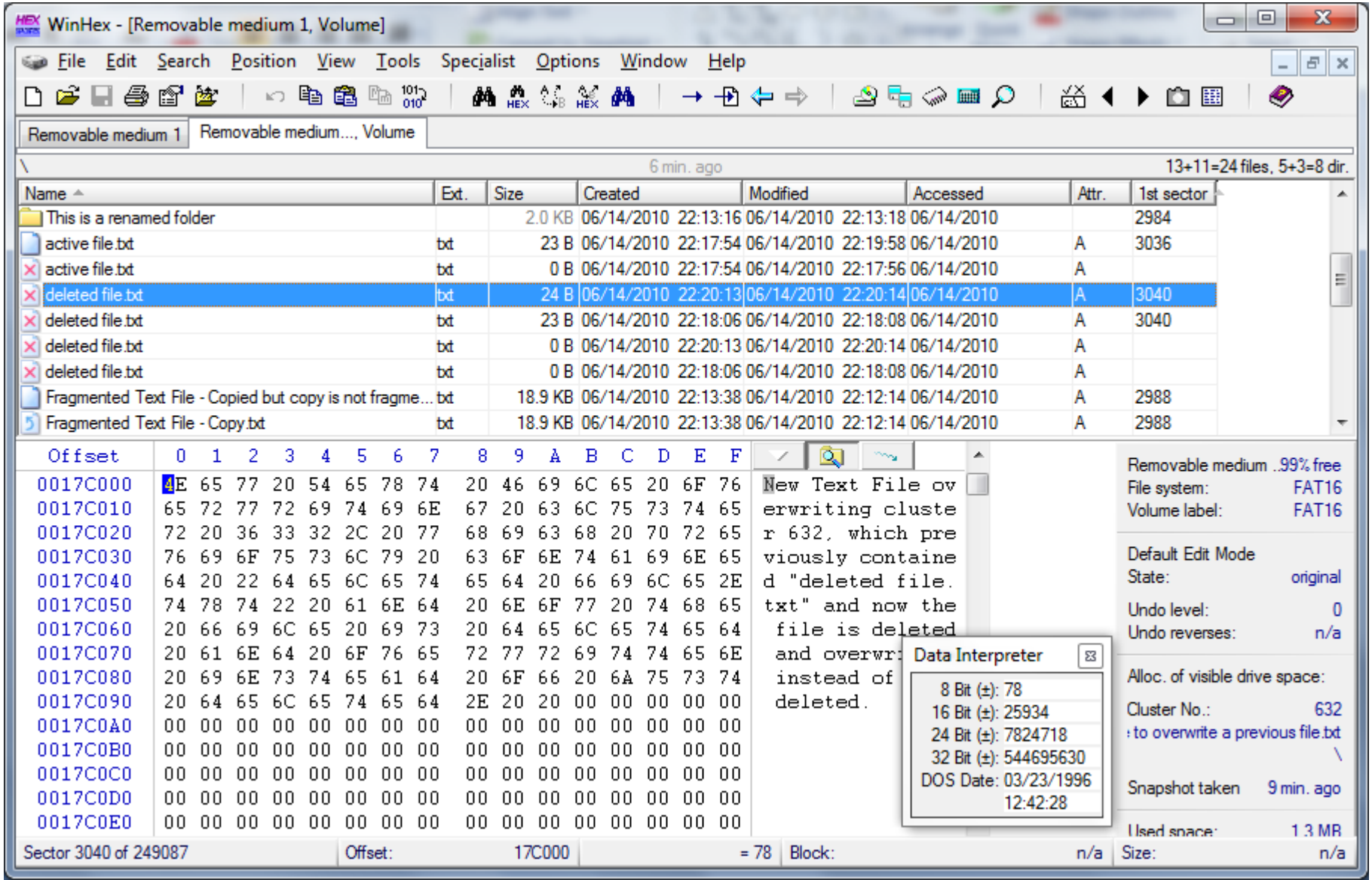
Opening a forensic bit-stream image



Viewing Files/Folders

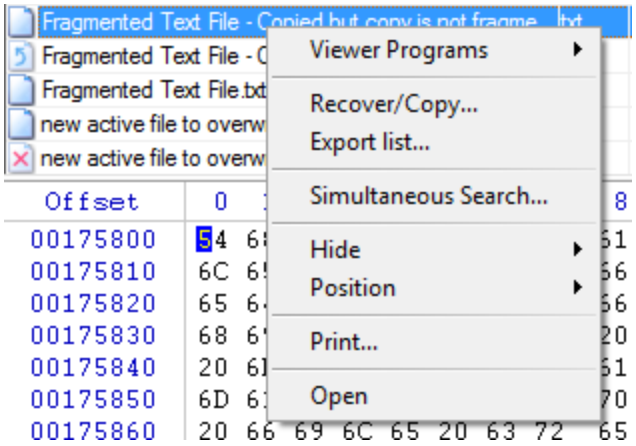
- To view the Hex/Text of any file or folder on a disk or in a forensic image, simply click on the file/folder in the Directory Browser.
- Scroll up/down through file/folder using scroll bar to the right of the "Text Display" window in the GUI.
- The icons in the Directory Browser for each file/folder indicate the "status" of the file/folder, as to whether it is an active file, deleted file but recoverable, deleted file that is overwritten and not recoverable, file was moved/renamed, etc.

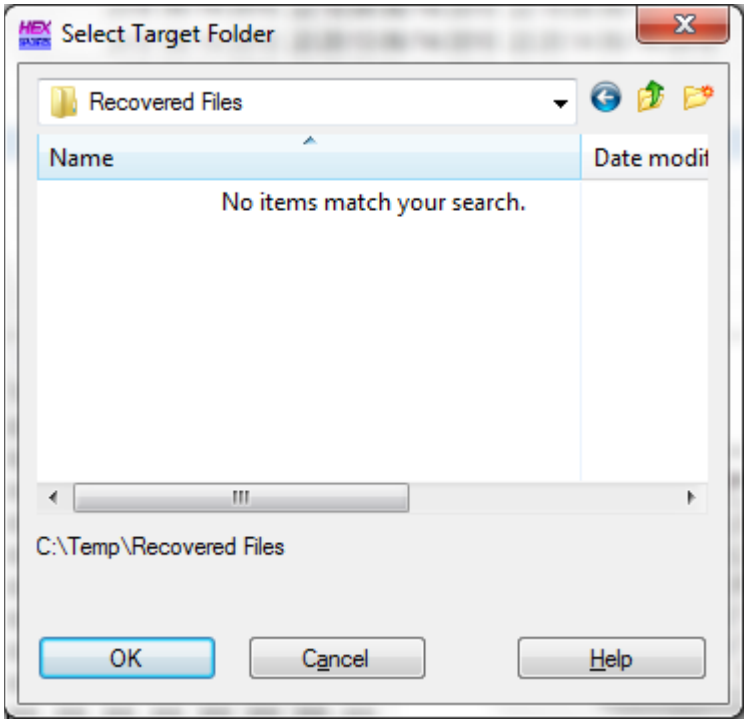
Viewing Files/Folders



Copying out (Recovering) Files/Folders

- In the Directory Browser, right-click on the desired file/folder and select Recover/Copy and select the path you wish to recover/copy the files to.





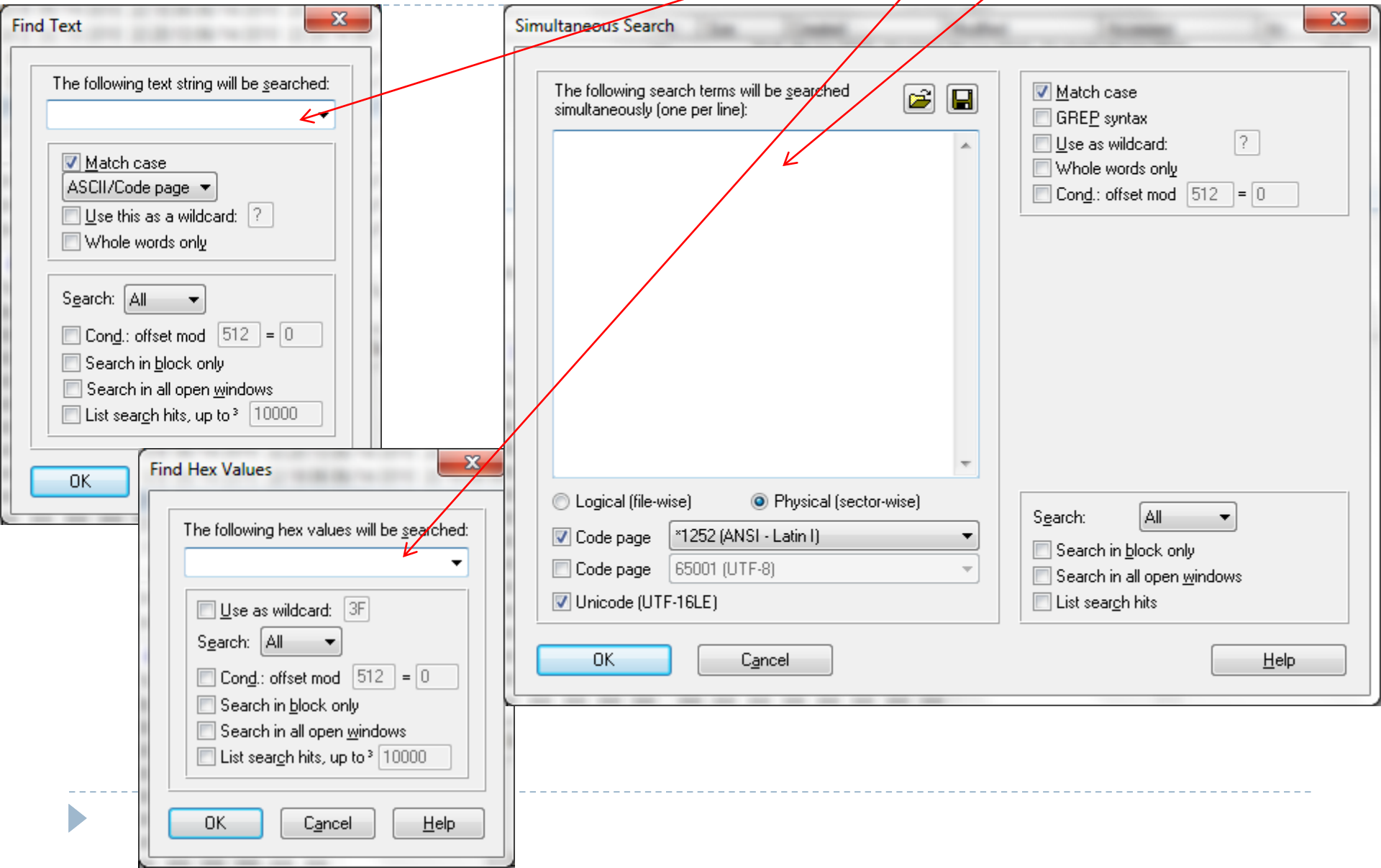
Editing data

- You must place WinHex into either Default Edit Mode or In-Place Edit Mode to make changes.
  - From the menu, select Options/Edit Mode
  - In Default Edit Mode you must click the "Save" button to commit any data changes you make.
  - In In-Place Edit Mode changes take place immediately as you type them.
- Changes can be made by typing HEX characters into the Hex Display window or typing text characters into the Text Display window.
- Disks or data (selected bytes) can be wiped using the Edit /Fill Disk Sectors or Edit Fill Block option from the menu.

Searching (HEX/Text)

- Click on appropriate toolbar button or select appropriate option from Search menu to open Find Text, Find HEX Values search dialog boxes to search for a single string or value.
  - Use F3 key to continue search using same option(s).
- Use the Simultaneous Search option to search for multiple strings or values in a single search operation.
  - Allows you to perform a logical or physical search. Logical searching will find strings/values that are not contiguous due to file fragmentation.
- "List Search Hits" check box will search the whole disk/image and provide you a listing of "hits".

Searching (Hex or Text)



Status Bar and Info Pane

- The status bar tells you:
  - Sector # of selected byte
  - Offset (from beginning of disk/partition) of selected byte
  - Offset range of highlighted bytes
  - Size (in bytes) of block of highlighted bytes
- Info bar tells you:
  - A variety of information about the disk or image you have opened
  - The cluster # and name of file/folder/disk area that the selected byte belongs to.
  - Current edit status (i.e. Read-Only, Default Edit mode, In-Place Edit mode) and many other application settings…

Interpreting HEX values

- In addition to using the Windows calculator to convert Hex to Decimal or Binary, we can also use the Data Interpreter that is built into WinHex.
- To change the list of items that Data Interpreter will list, select Options/Data Interpreter and select the desired date format and/or other integer types you wish to interpret.
- To use the Data Interpreter, simply click on the "left most" byte of any byte or group of bytes and the Data Interpreter will read the bytes to the right of the byte you click on and show the interpretation of those bytes.

Interpreting HEX values