

CIPHER /w TO WIPE DELETED FILES FROM A HARD DRIVE OR FLASH DRIVE

HIGH-LEVEL EXECUTIVE SUMMARY

You can use the "cipher /w" command-line command to wipe deleted files from the hard drives of computers running "Windows.. This will prevent someone running a software program such as the free "Recuva Free Edition" from recovering files that you have deleted.

DETAILED DESCRIPTION

You can use the
cipher /w:C:
command-line command to remove deleted files permanently so that software such as the free [Recuva software utility](#) cannot be used to "undelete" files/folders that you have deleted.

To wipe deleted files from a drive other than C:, substitute the actual drive letter that you wish to scan:

For example, to scan the M: drive, type in
cipher /w:m:

You can use the free [Recuva software utility](#) to verify that the "cipher /w" command has succeeded in "wiping" recently-deleted files/folders from a hard drive or a USB flash drive.

Please note that many online and print magazine articles erroneously tell you to type in

cipher /w:c

Since "c" is not a valid path designation in Windows.., "cipher /w:c" is seen by "Windows.." as "cipher /w" which then defaults to wiping free space in the C: drive.

If you type in

cipher /w:f

when you want to wipe the F: drive, "Windows.." ignores the "f" and "cipher /w:f" defaults to "cipher /w" which will wipe your C: drive instead.

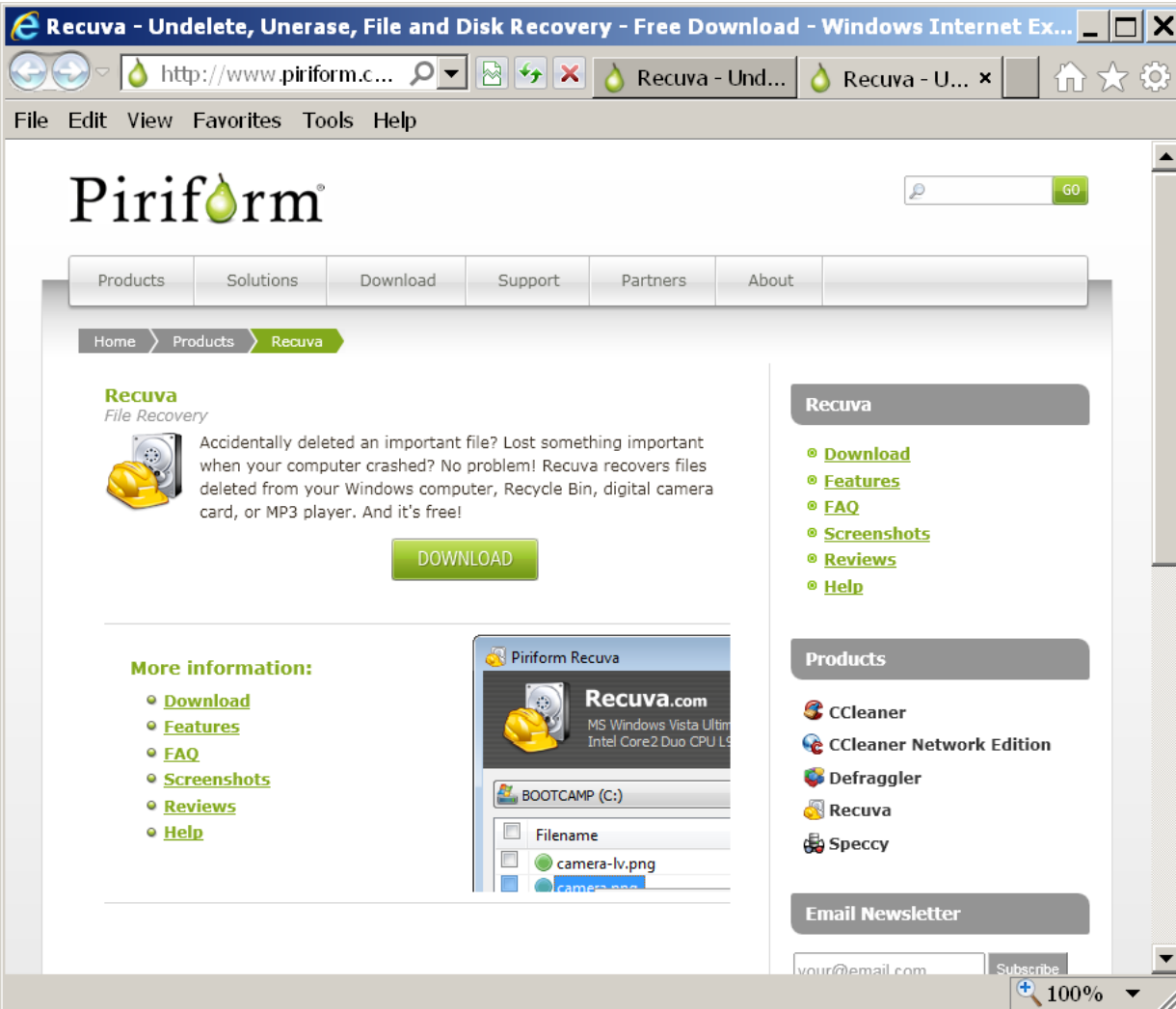
STEP-BY-STEP PROCEDURE

Step 1:

If you have not already done so, go to

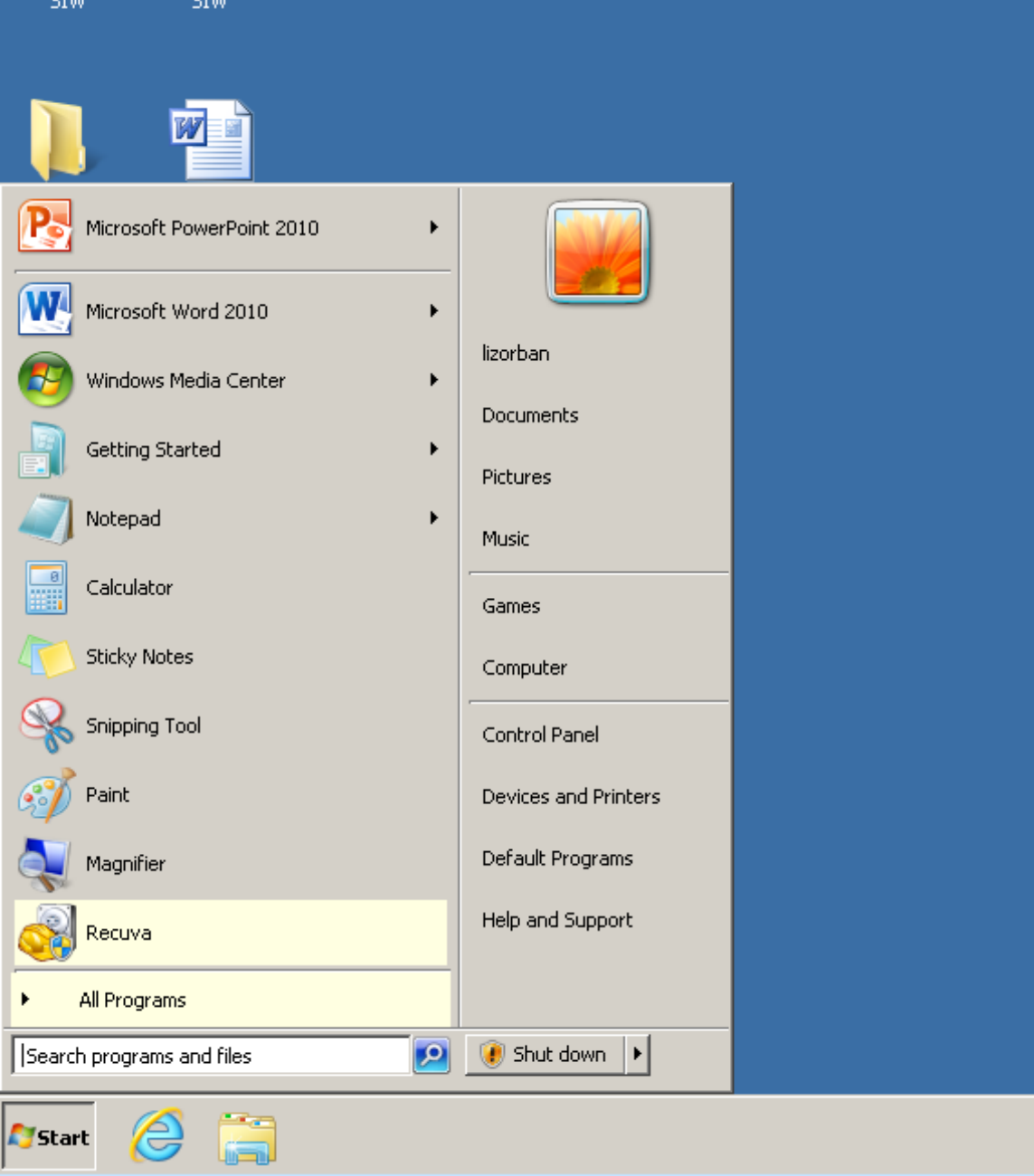
<http://www.piriform.com/recuva>

and download and install the free version of the "Recuva" program:

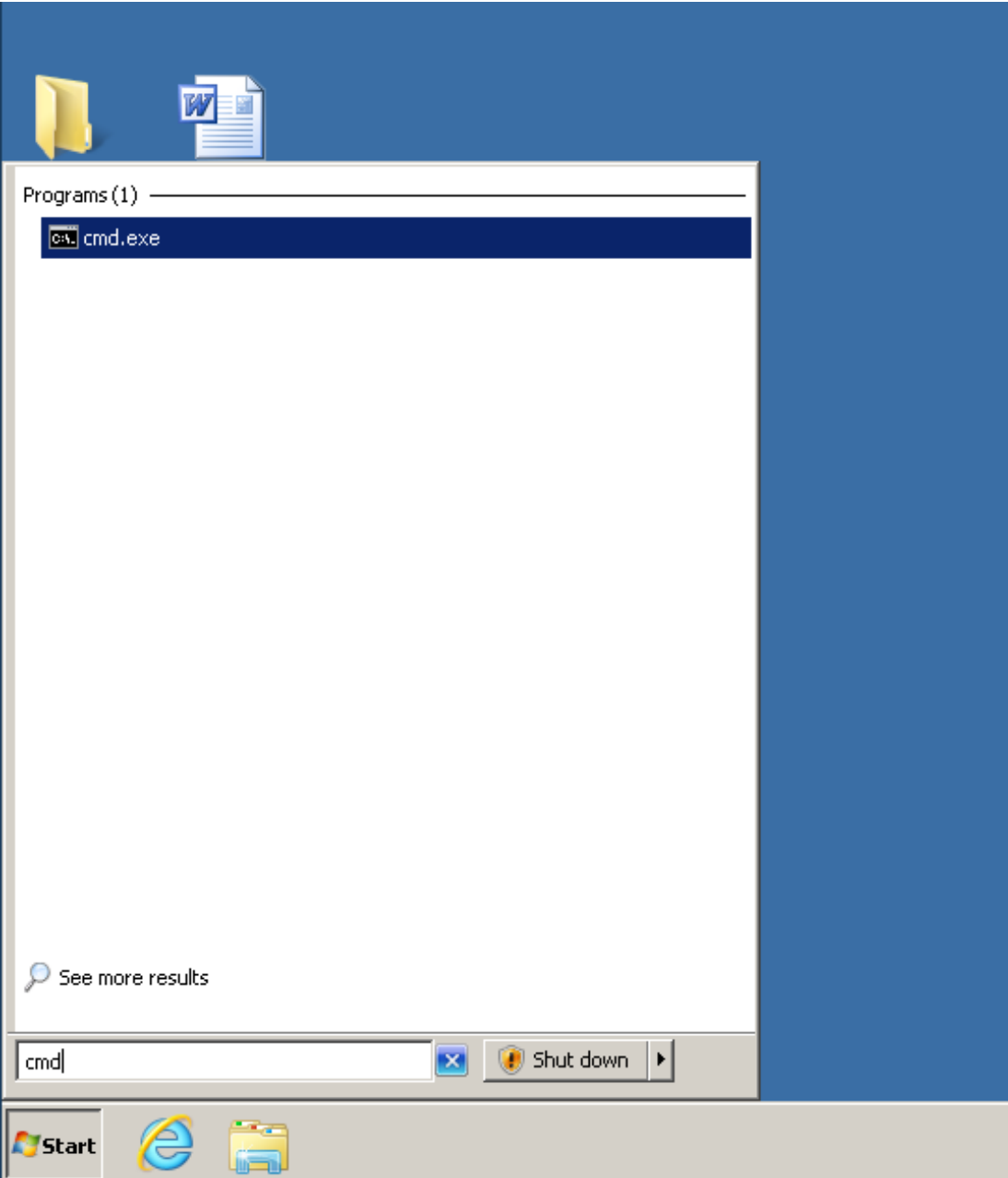


The screenshot shows a Windows Internet Explorer browser window displaying the Piriform Recuva website. The browser's address bar shows the URL <http://www.piriform.com/recuva>. The website features a navigation menu with links for Products, Solutions, Download, Support, Partners, and About. The main content area highlights the Recuva product, described as a file recovery tool. A prominent green 'DOWNLOAD' button is visible. To the right, there is a sidebar with a 'Recuva' section containing links for Download, Features, FAQ, Screenshots, Reviews, and Help. Below this, a 'Products' section lists other software like CCleaner, Defraggler, and Speccy. At the bottom, there is an 'Email Newsletter' subscription form. The browser's status bar at the bottom right indicates a zoom level of 100%.

Step 2:
Click on the Windows "Start" button:



Step 3:
Type
cmd
into the Search or Run box:



Step 4:

"cmd.exe" will be displayed by the "Start" menu.

Step 5:

Use the right mouse button to click on "cmd.exe".

Step 6:

A pop-up context menu will be displayed:

Step 7:

Click on "Run as administrator" in the pop-up context menu:



Programs (1)

cmd.exe

Open

- Run as administrator
- Scan with Microsoft Security Essentials...
- Pin to Taskbar
- Pin to Start Menu
- Restore previous versions

Send to ▶

Cut
Copy

Delete

Open file location

Properties

See more results

cmd

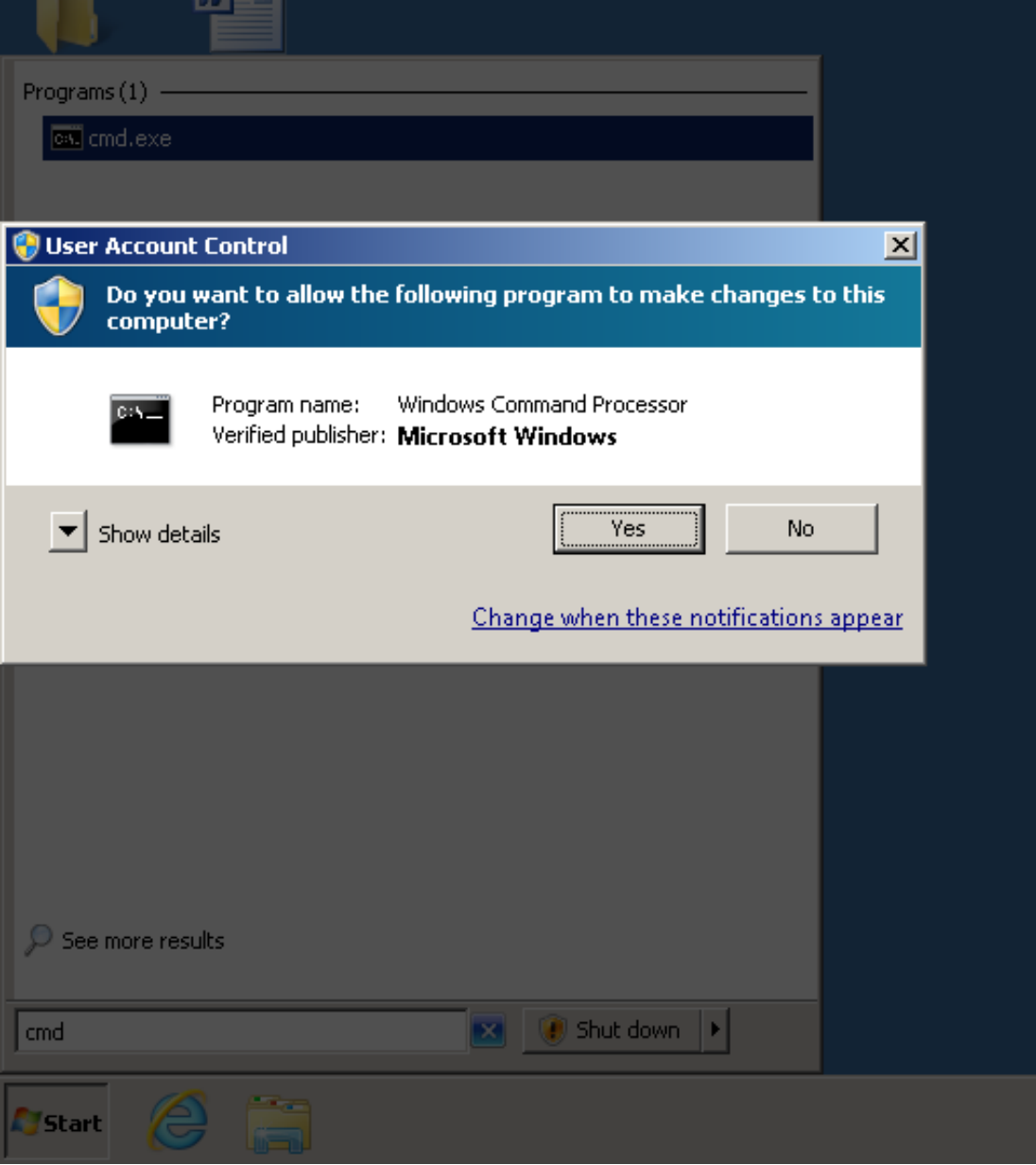


Shut down ▶

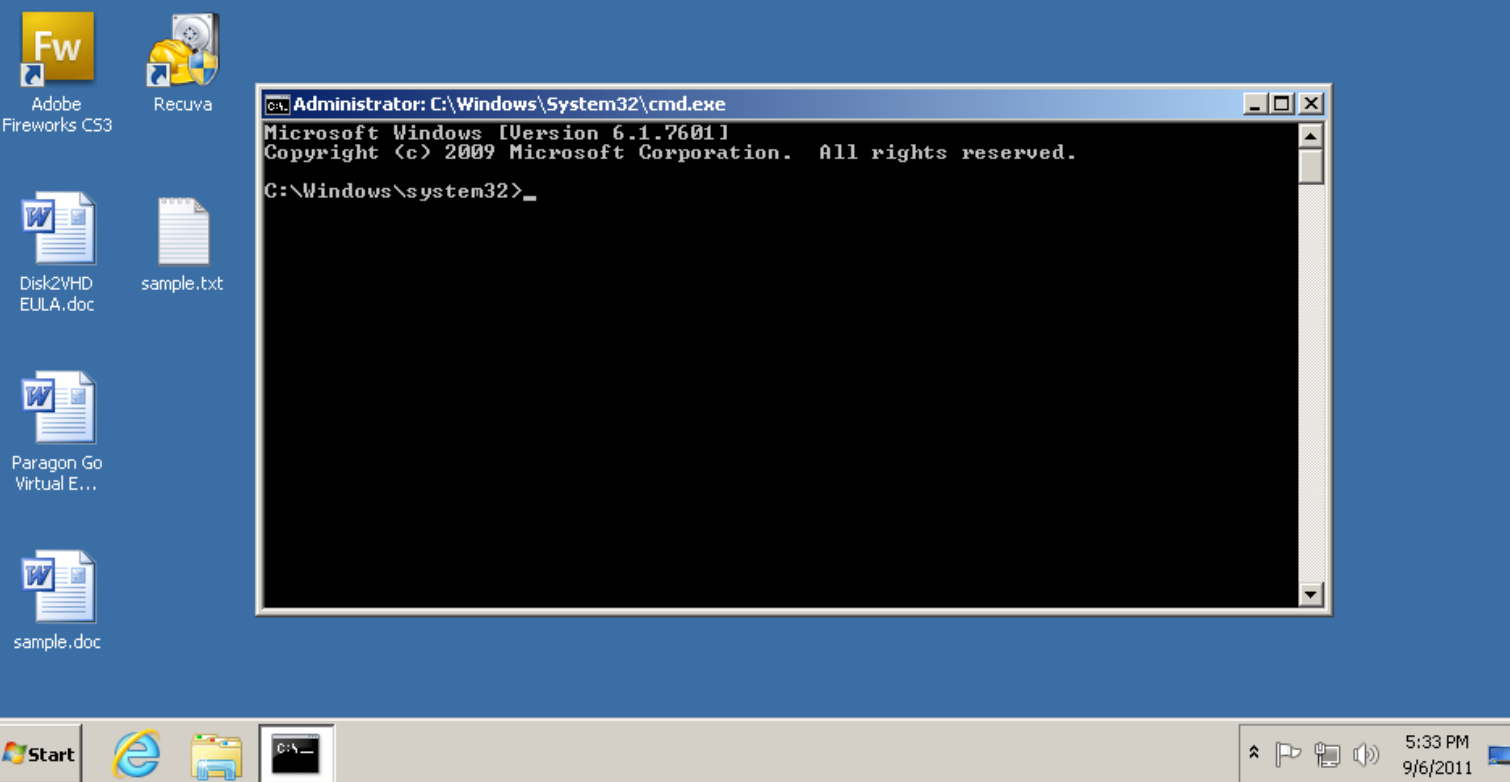
Start



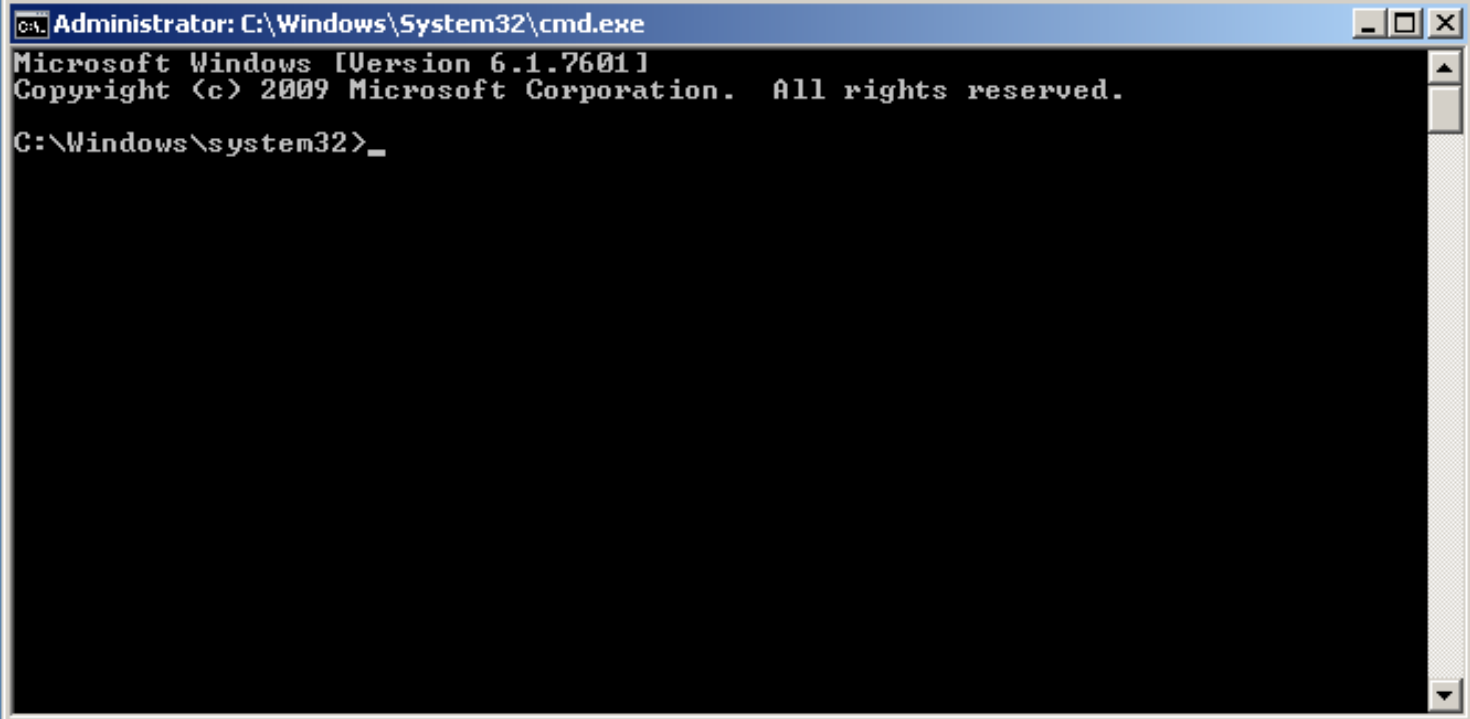
Step 8:
If a "User Account Control" box is displayed, click on its "Yes" button:



Step 9:
A black "Command Prompt" window will be displayed:



*



Step 10:

Type in

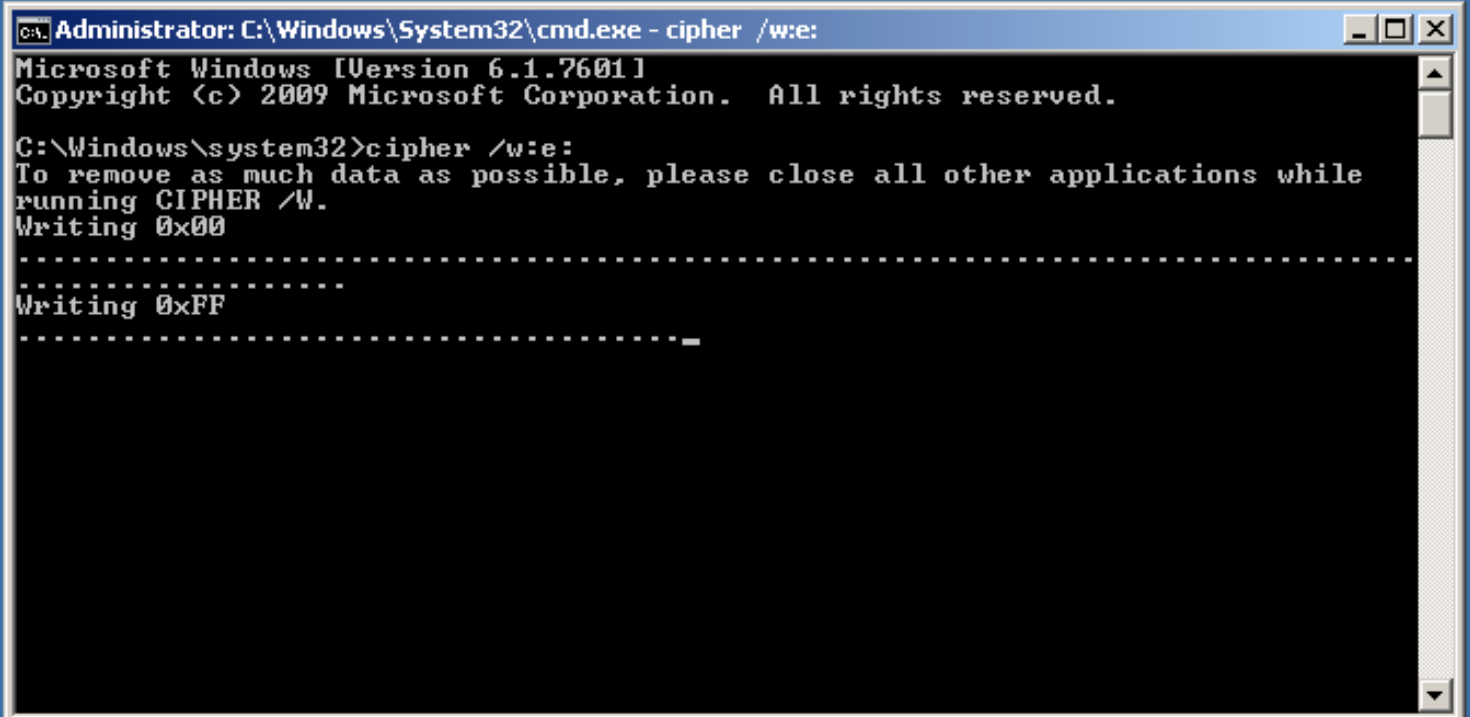
`cipher /w:e:`

Type at least one space between the "r" in "cipher" and the "/".

There must be one colon to the right of the "w".

There must be one colon to the right of the "e".

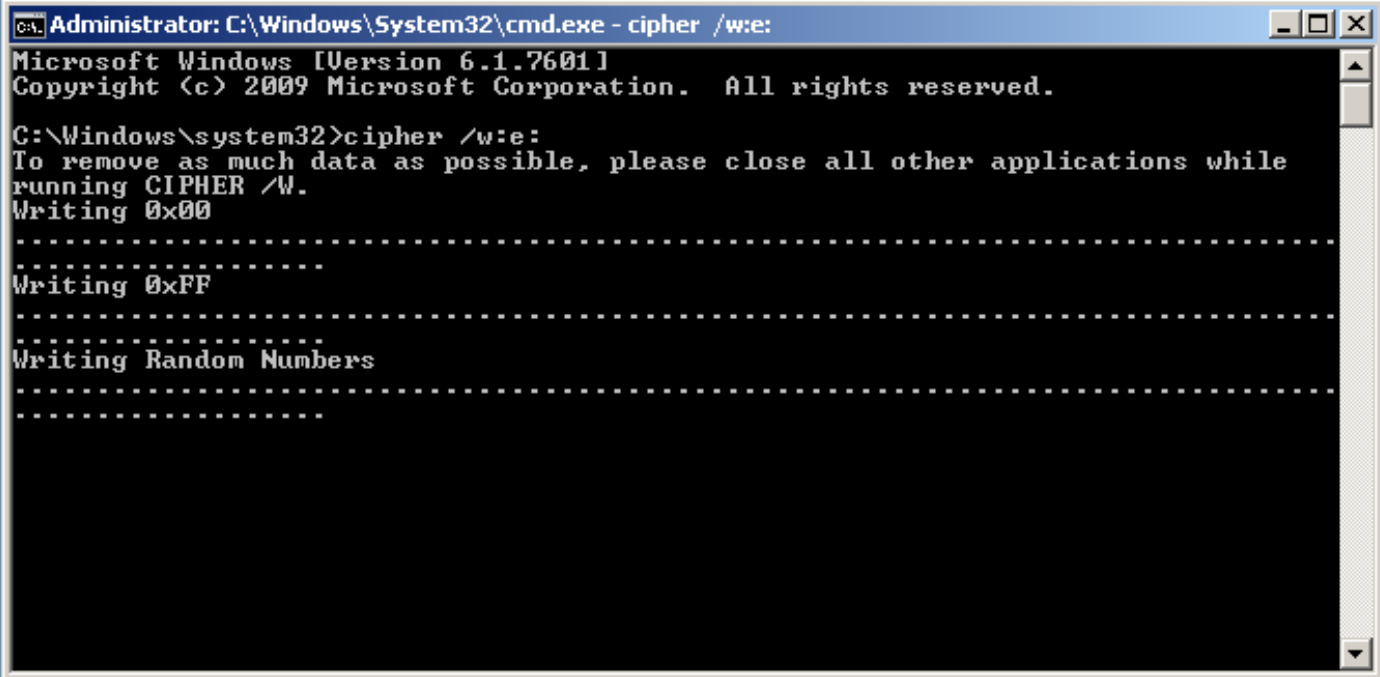
However, instead of "e", you might have to substitute the drive letter of the actual drive that you wish to wipe:



```
Administrator: C:\Windows\System32\cmd.exe - cipher /w:e
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cipher /w:e:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....
Writing 0xFF
.....
```

Step 11:
Press the Enter key of the keyboard.

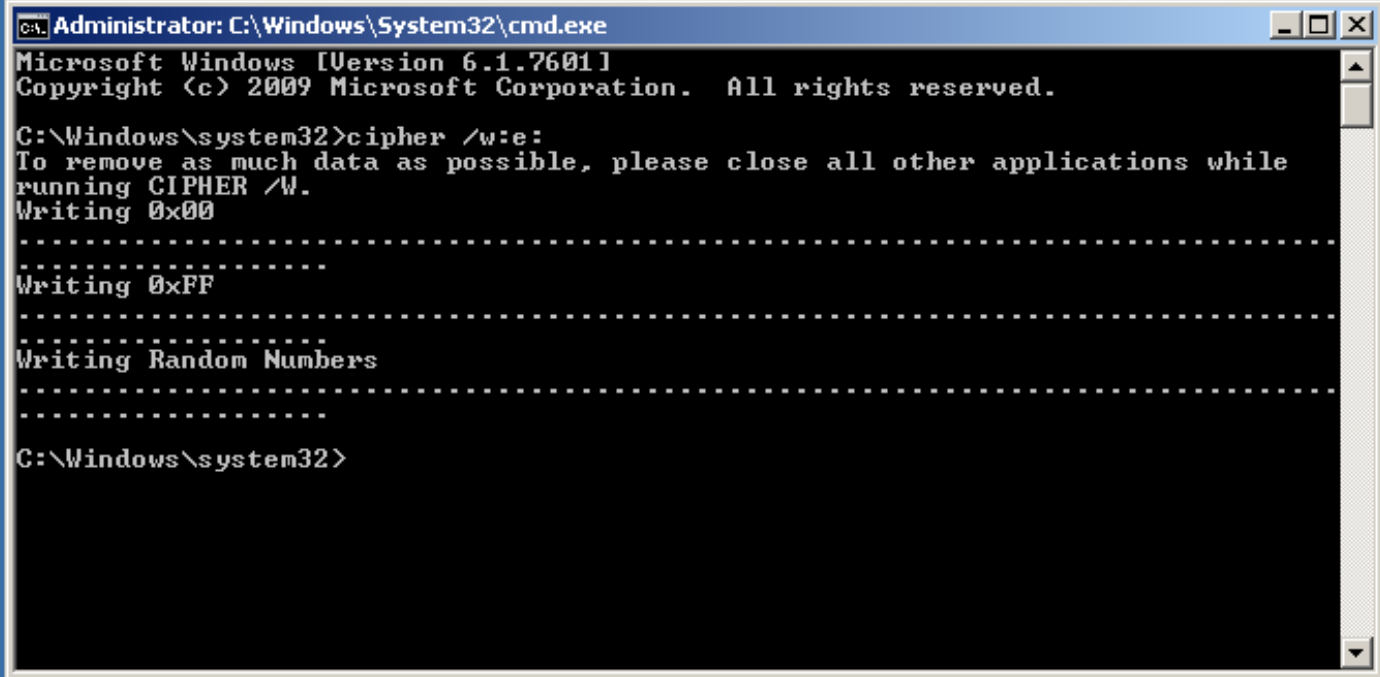


```
Administrator: C:\Windows\System32\cmd.exe - cipher /w:e
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cipher /w:e
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....
Writing 0xFF
.....
Writing Random Numbers
.....
```

Step 12:

The wiping process is done when the command prompt is displayed:



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cipher /w:e:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....
Writing 0xFF
.....
Writing Random Numbers
.....

C:\Windows\system32>
```

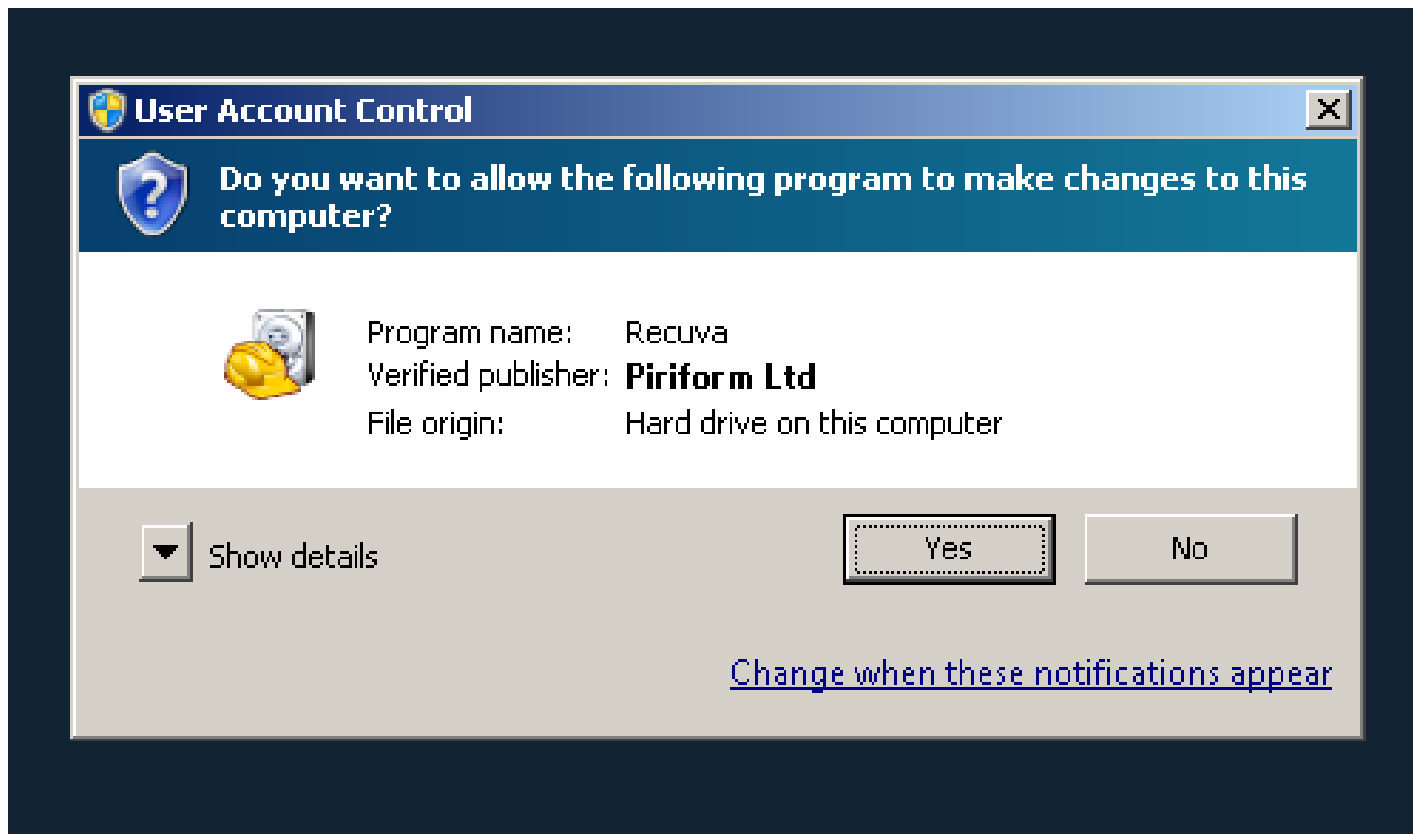
Step 13:

Start the "Recuva" program:



Step 14:

If a "User Account Control" box is displayed, click on its "Yes" button:



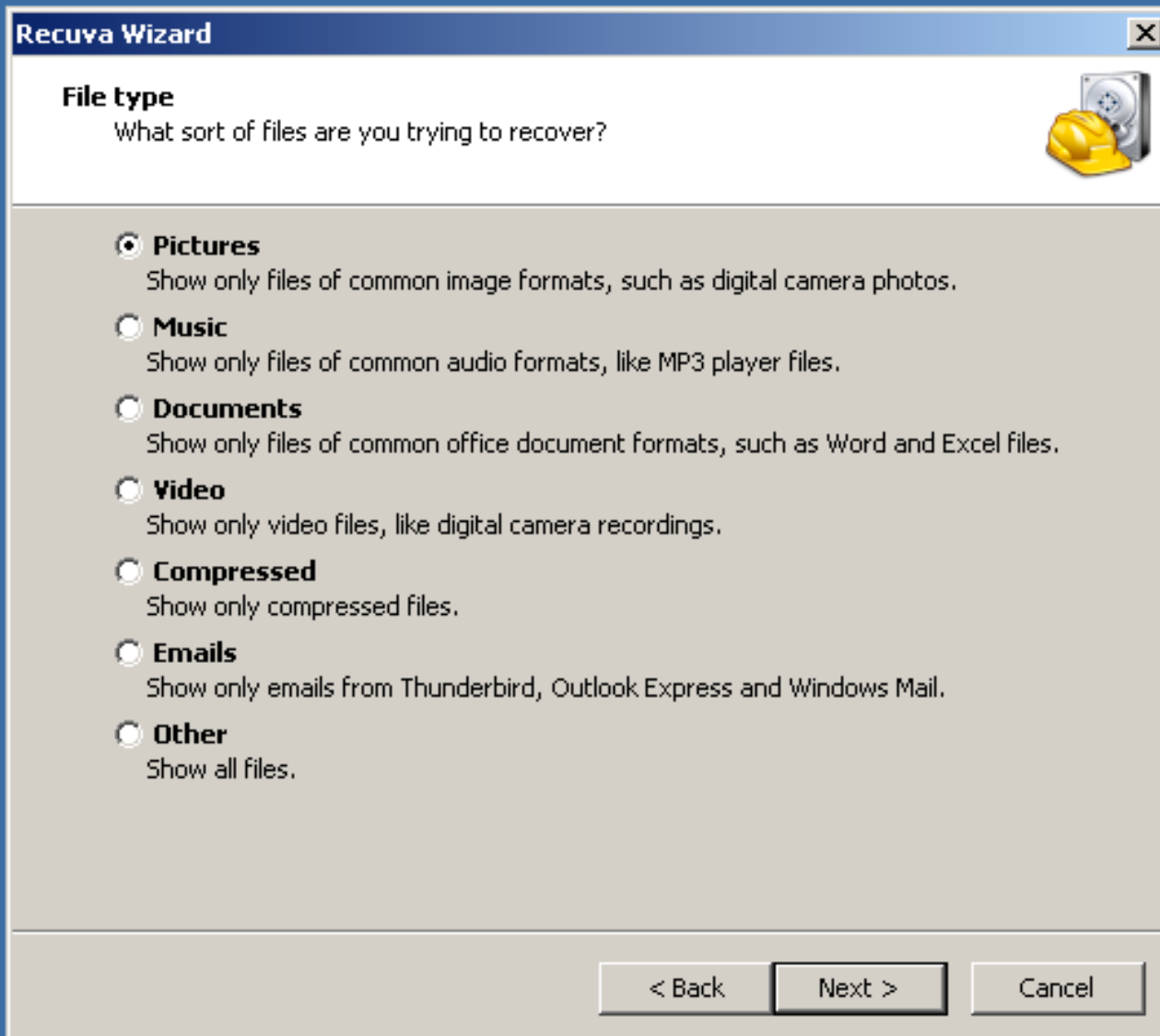
Step 15:

Click on the "Next" button of the "Recuva Wizard" box:

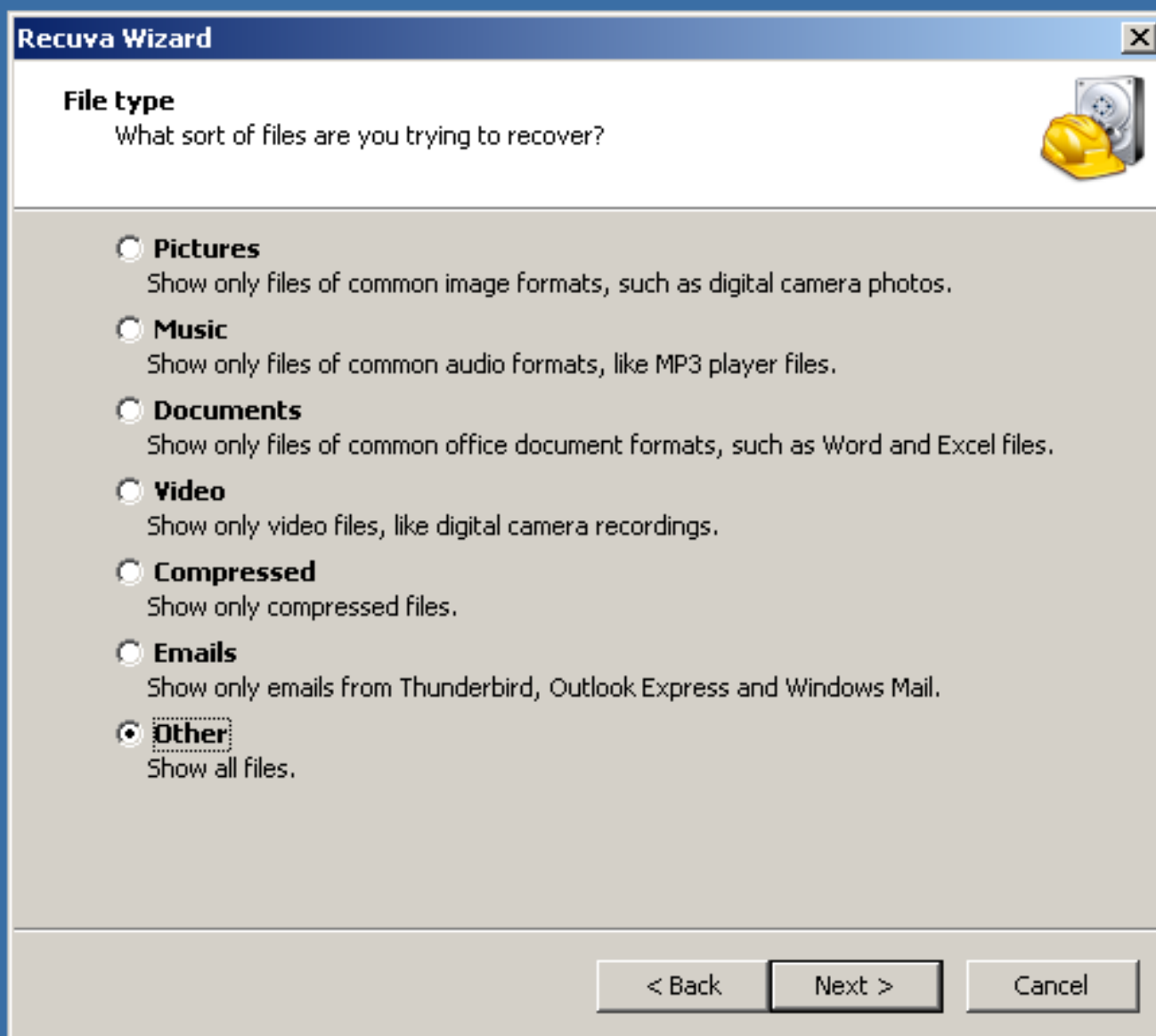


Step 16:

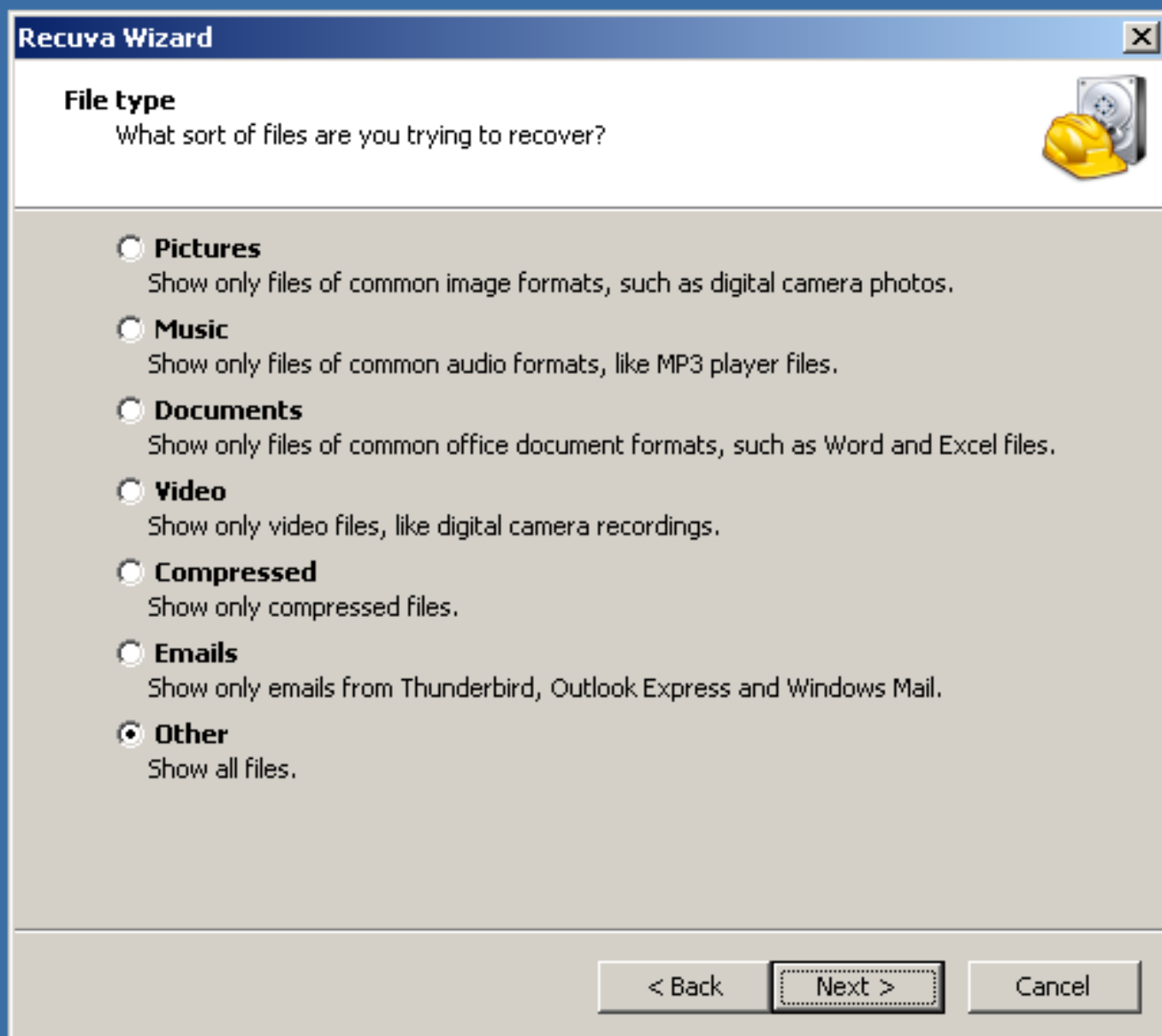
A "File type" box will be displayed:



Step 17:
Select the "Other" option:



Step 18:
Click on the "Next" button of the "File type" box:

The image shows a Windows-style dialog box titled "Recuva Wizard". The window has a blue title bar with a close button (X) in the top right corner. Below the title bar, the text "File type" is displayed in bold, followed by the question "What sort of files are you trying to recover?". To the right of this text is an icon of a yellow hard hat and a silver hard drive. Below the question, there is a list of radio button options, each with a bold label and a descriptive sentence. The "Other" option is selected, indicated by a filled radio button. At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Recuva Wizard [X]

File type
What sort of files are you trying to recover?

Pictures
Show only files of common image formats, such as digital camera photos.

Music
Show only files of common audio formats, like MP3 player files.

Documents
Show only files of common office document formats, such as Word and Excel files.

Video
Show only video files, like digital camera recordings.

Compressed
Show only compressed files.

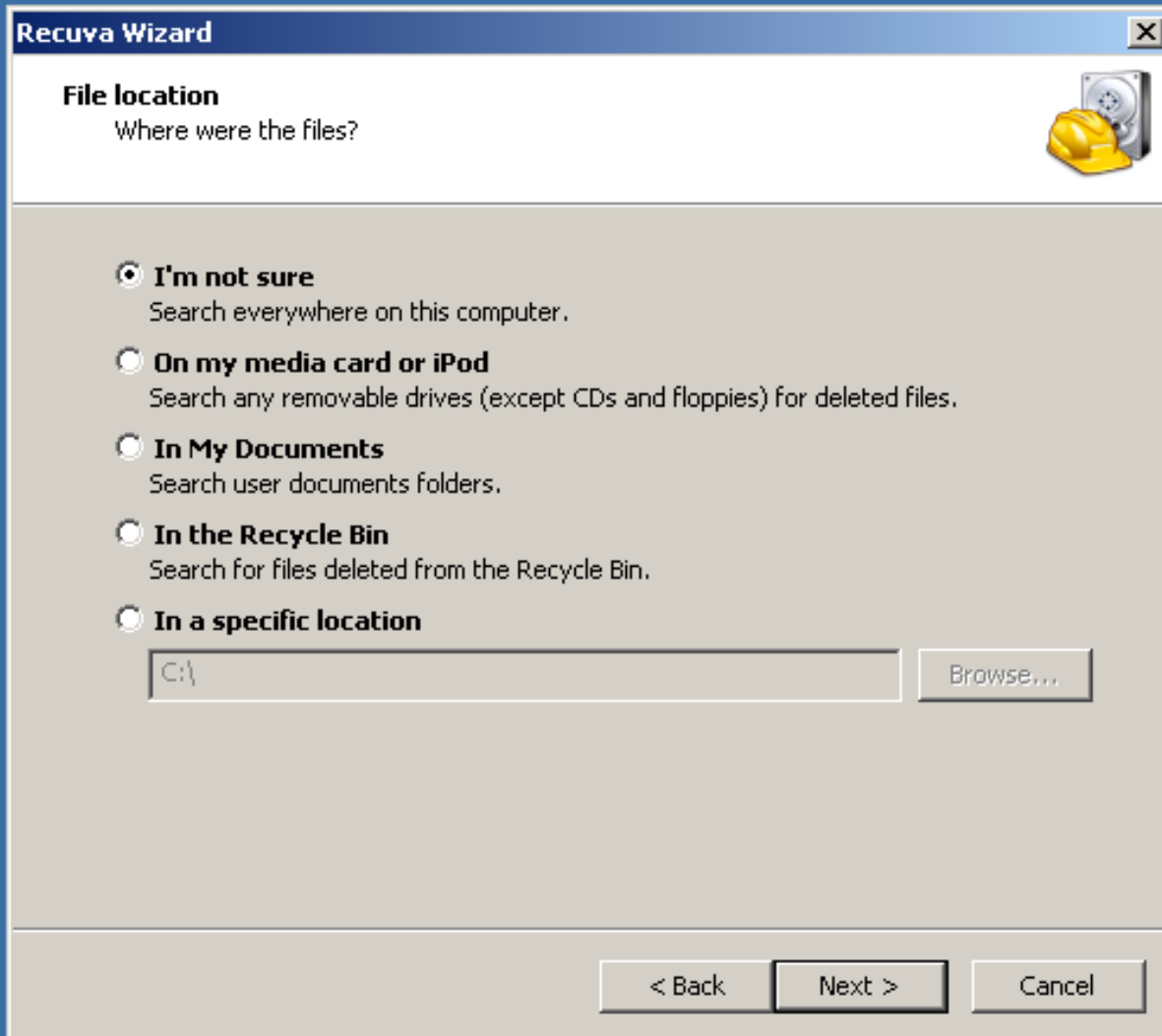
Emails
Show only emails from Thunderbird, Outlook Express and Windows Mail.

Other
Show all files.

< Back **Next >** Cancel

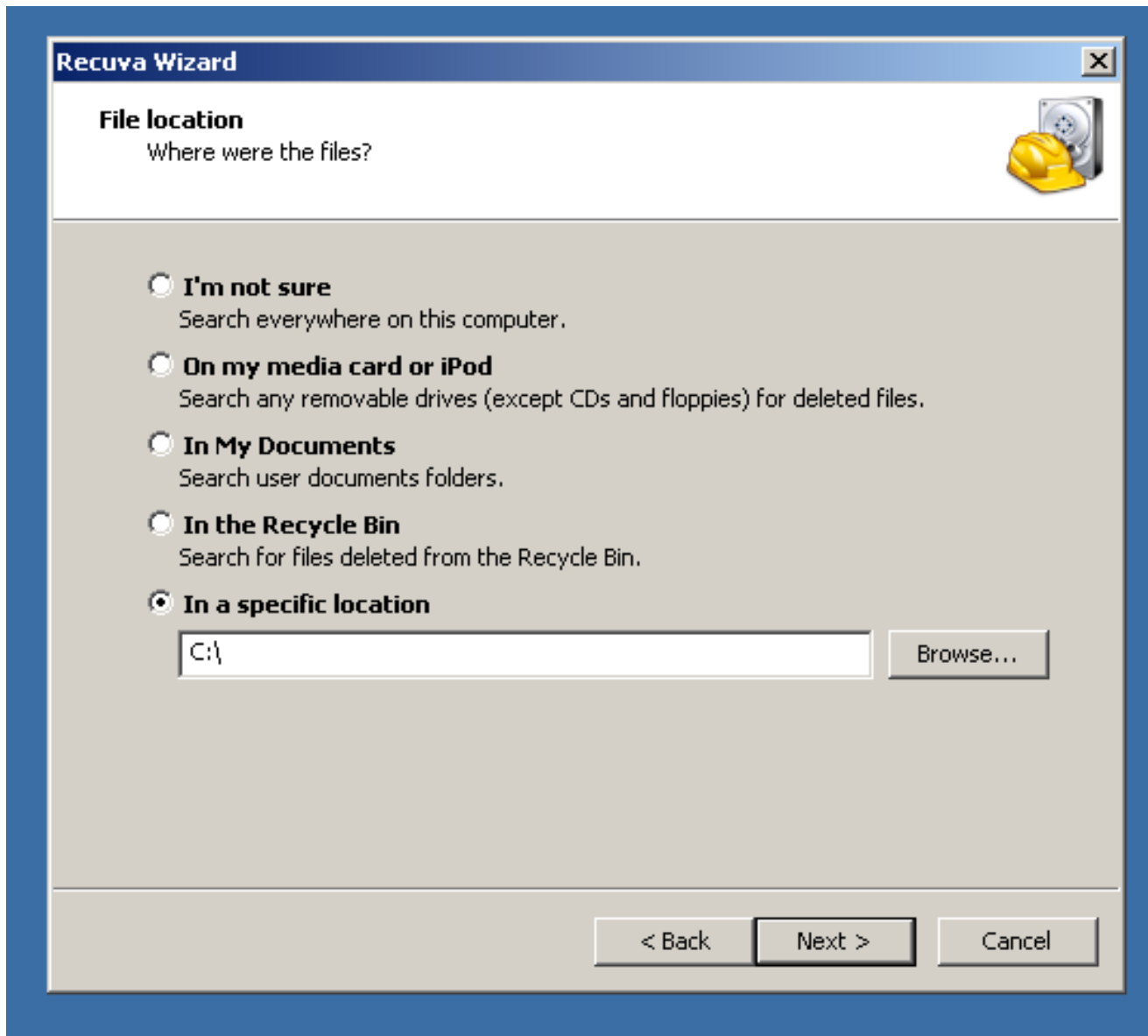
Step 19:

A "File location" box will be displayed:



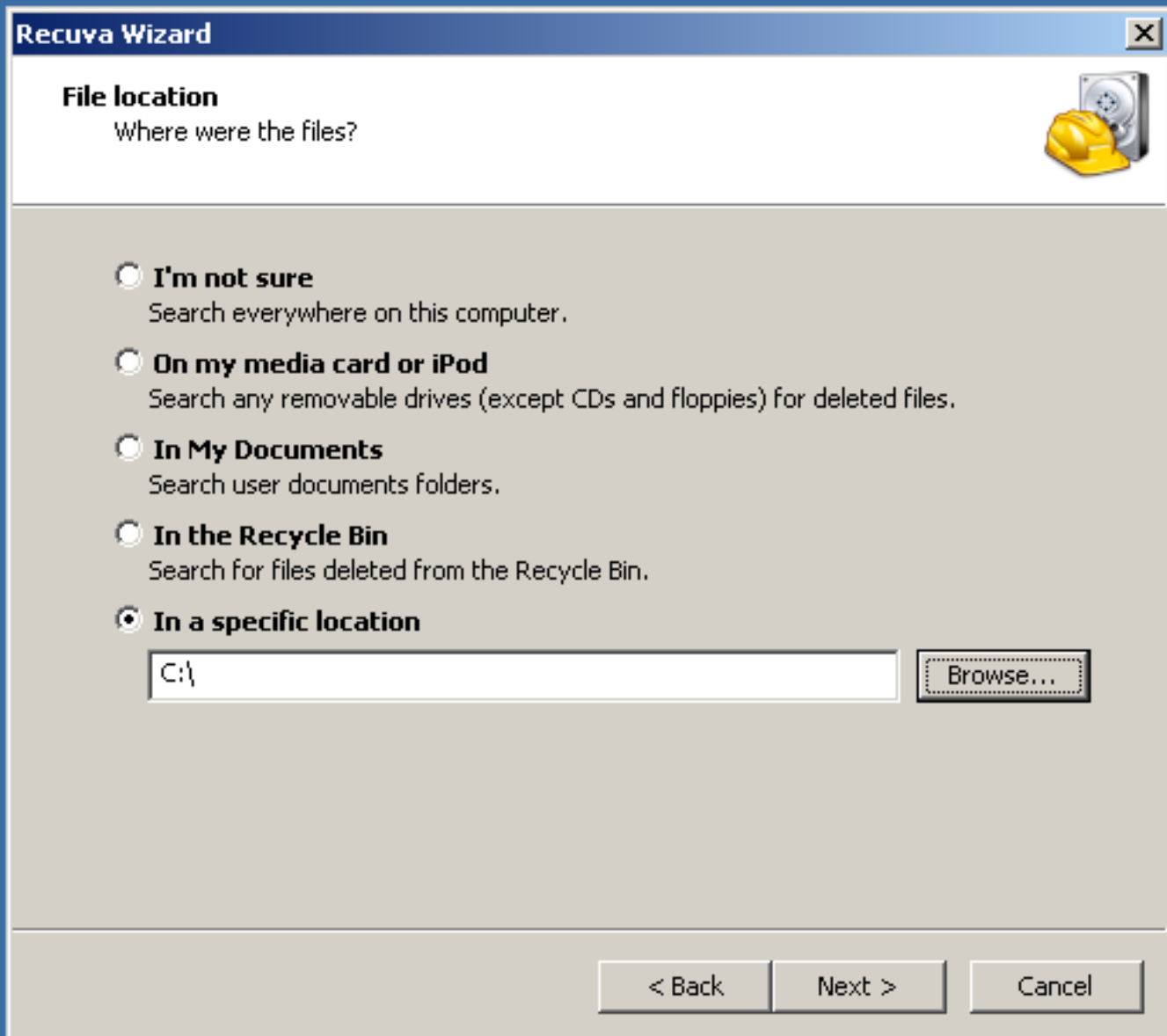
Step 20:

Select the "In a specific location" option of the "File location" box:

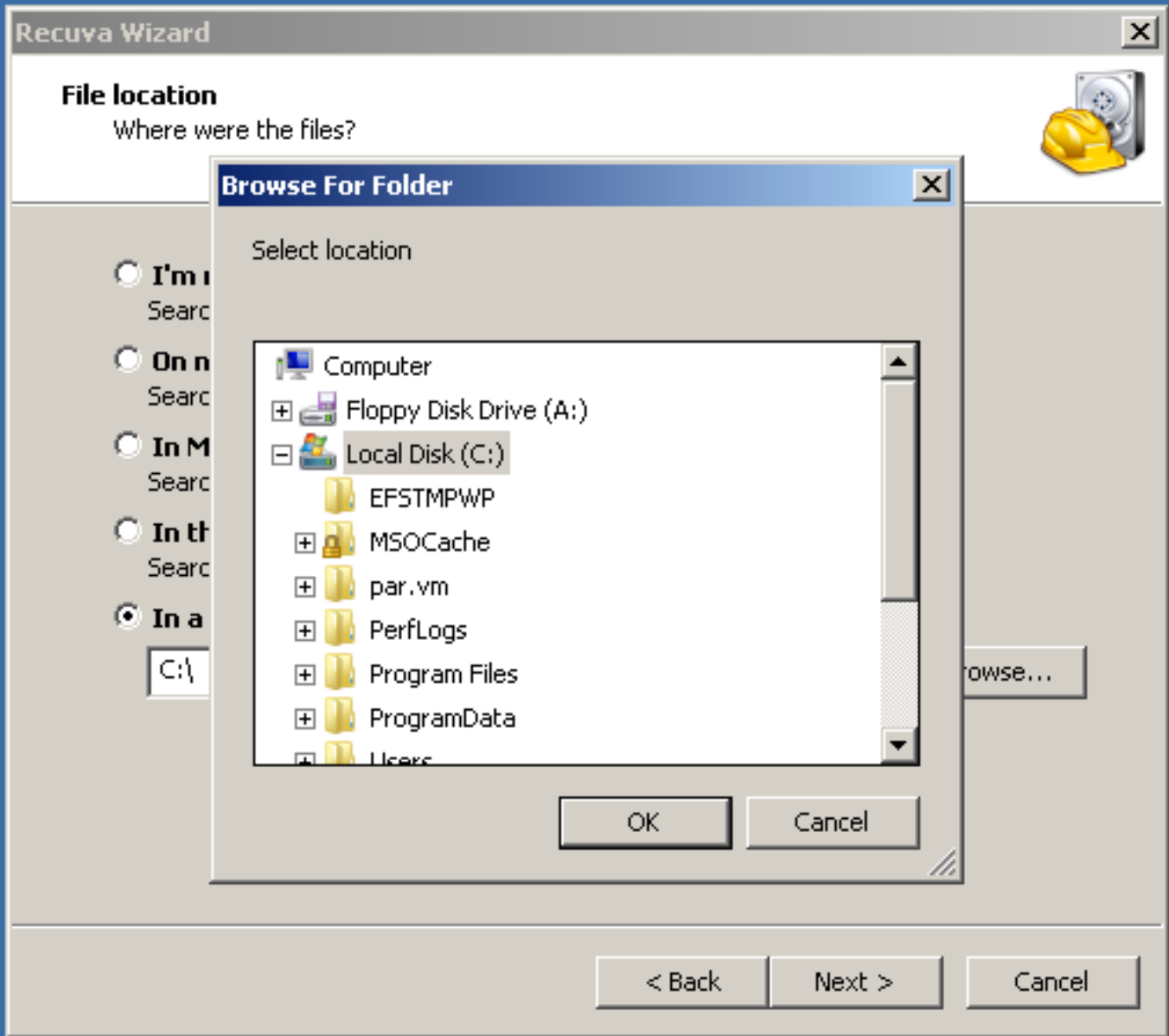


Step 21:

Click on the "Browse..." button:

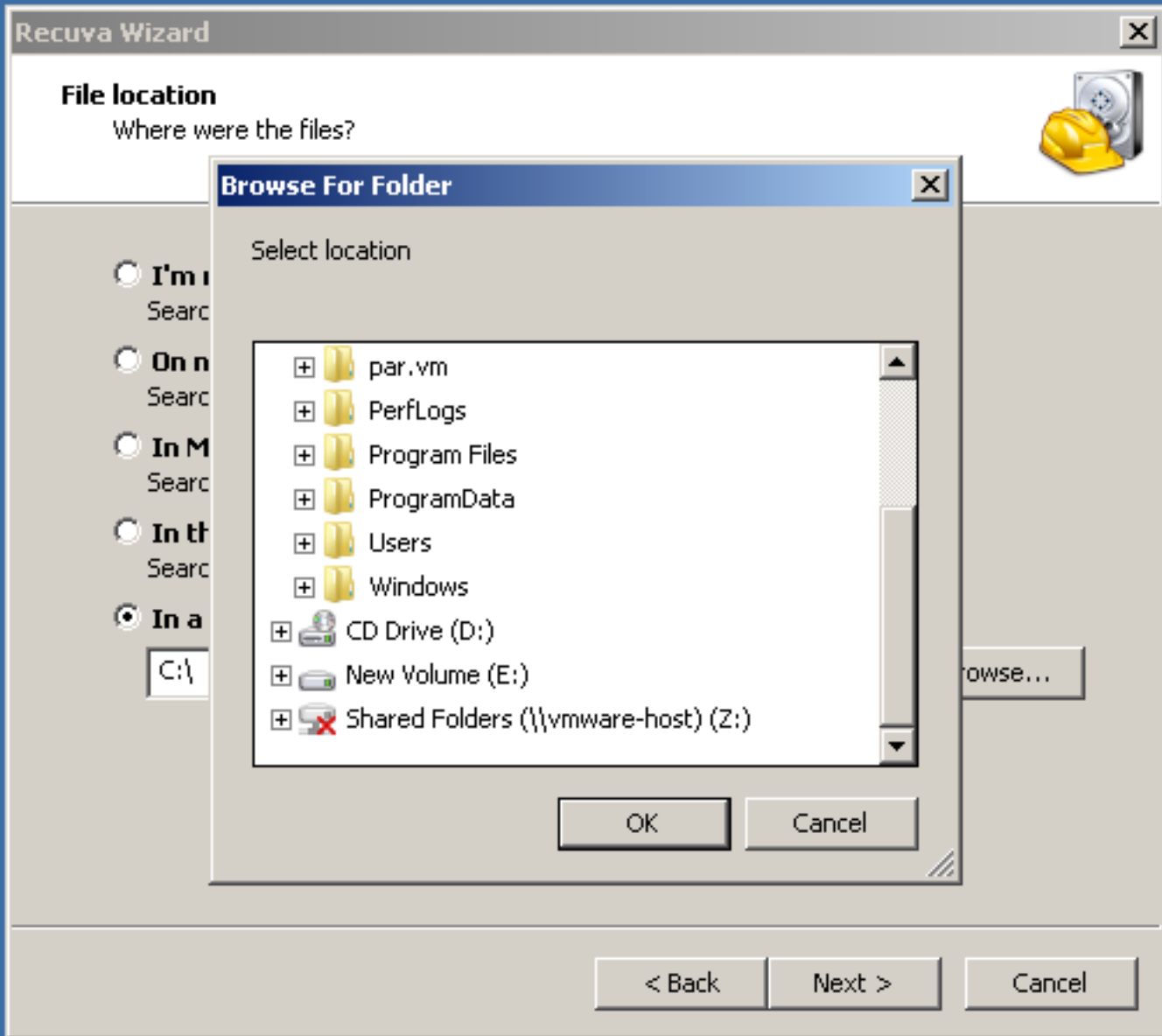


Step 22:
A "Browse for Folder" box will be displayed:



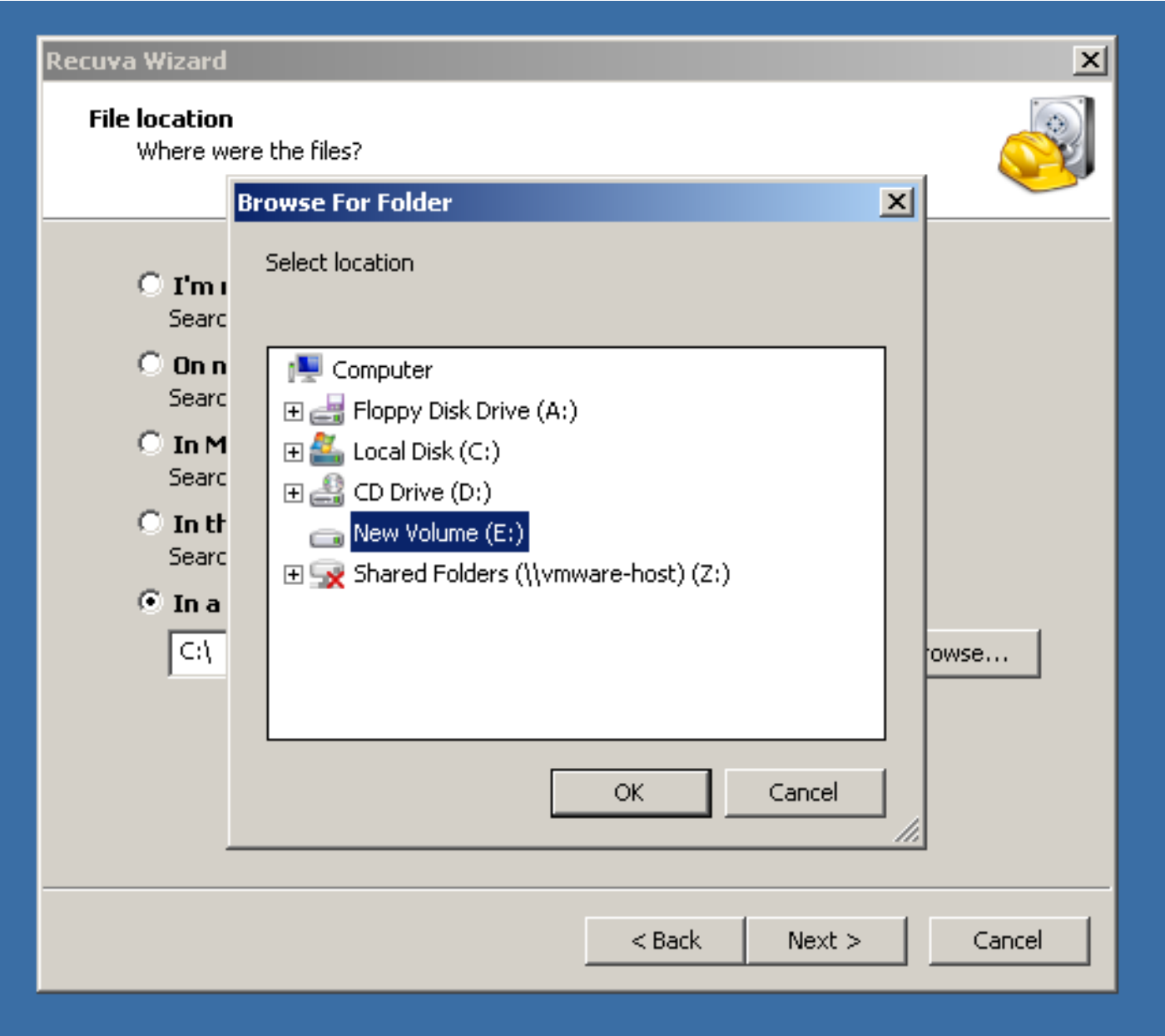
Step 23:

Use the vertical scroll bar to scroll down to locate the hard drive or USB flash drive that you wish to attempt to restore deleted files from:



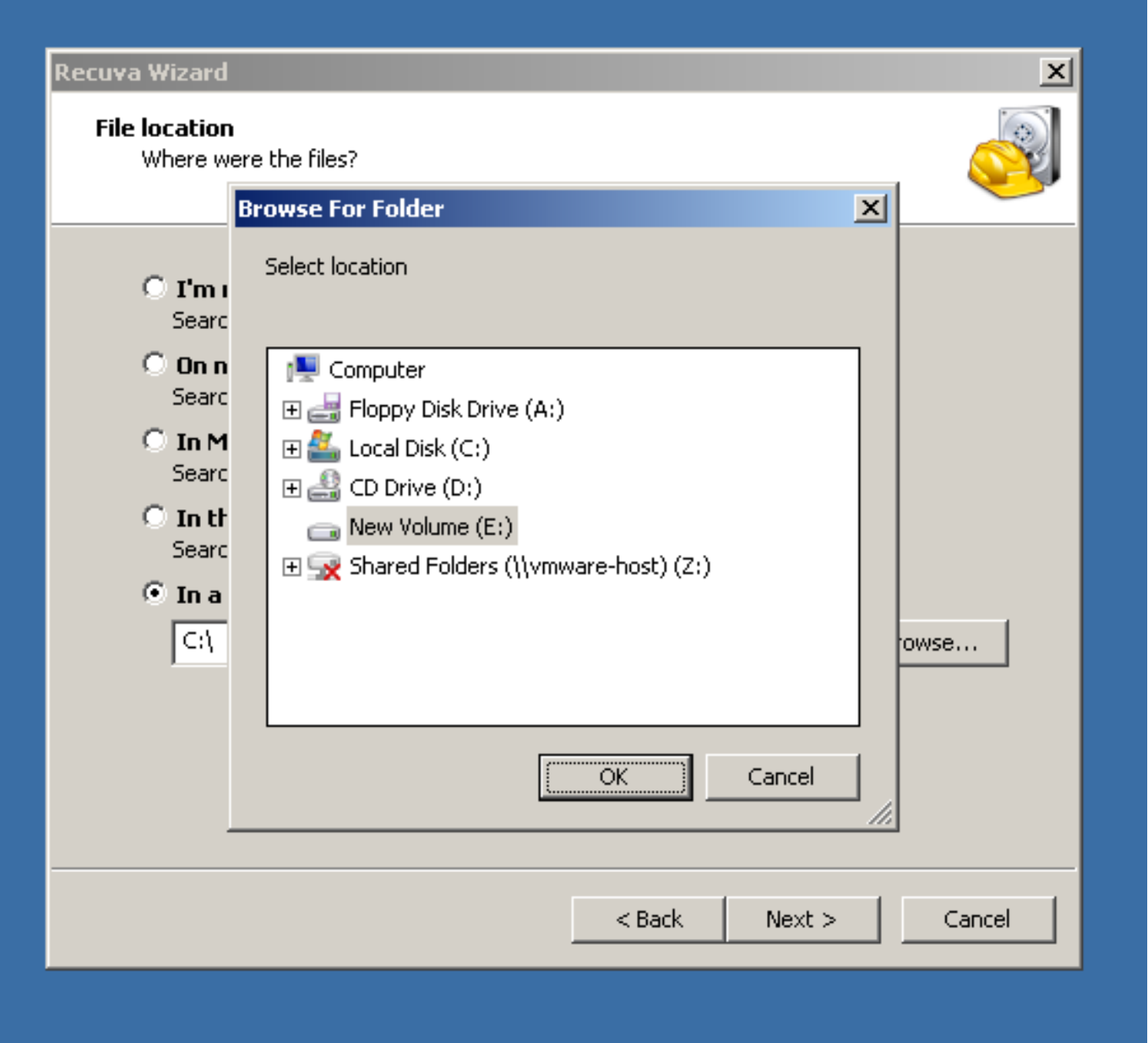
Step 24:

Click on the hard drive or USB flash drive that you wish to attempt to restore deleted files from:



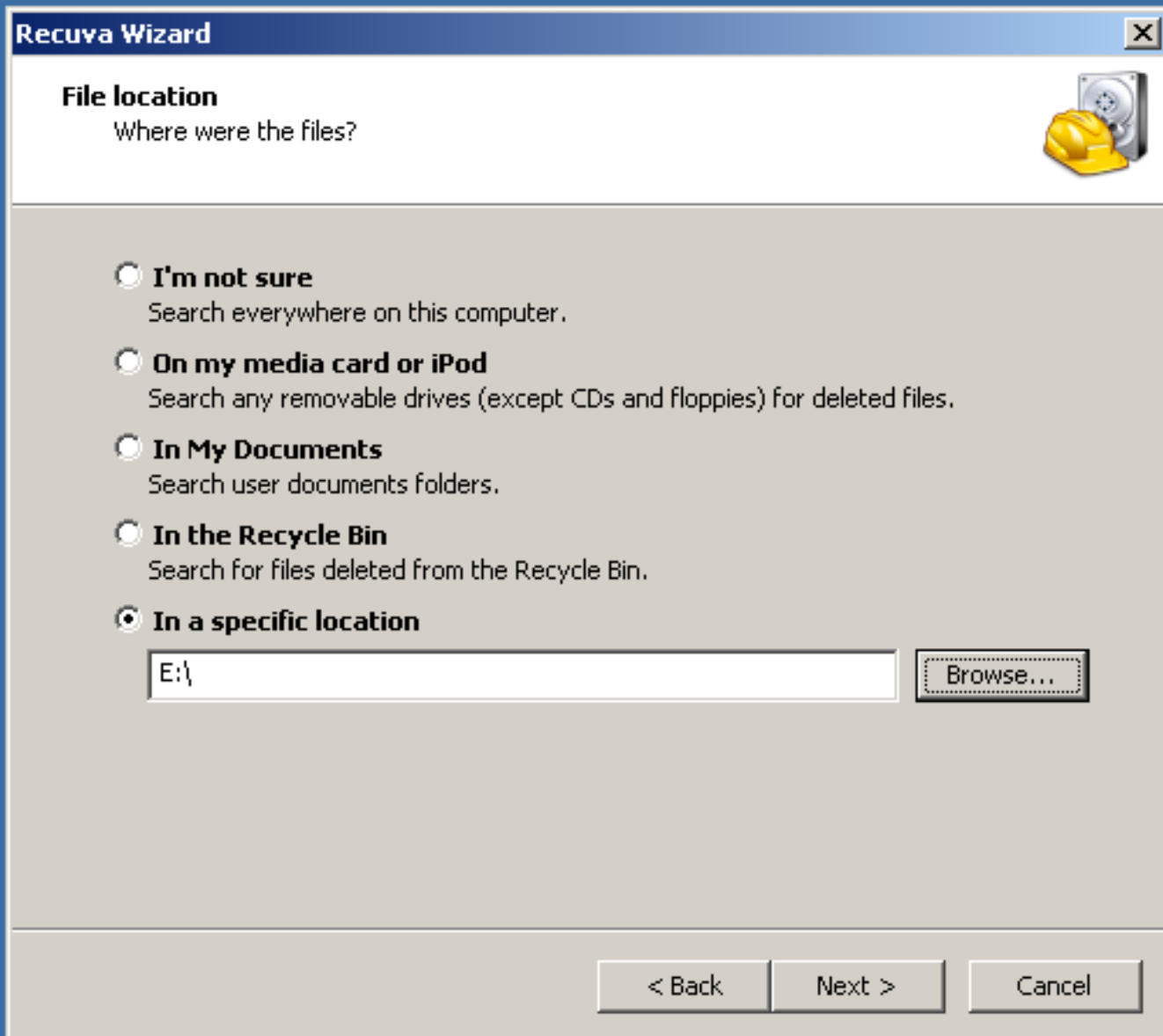
In this example, we clicked on the E: drive.

Step 25:
Click on the "OK" button of the "Browse for Folder" box:



Step 26:

The letter of the target hard drive or USB flash drive will now be displayed in the field below "In a specific location":

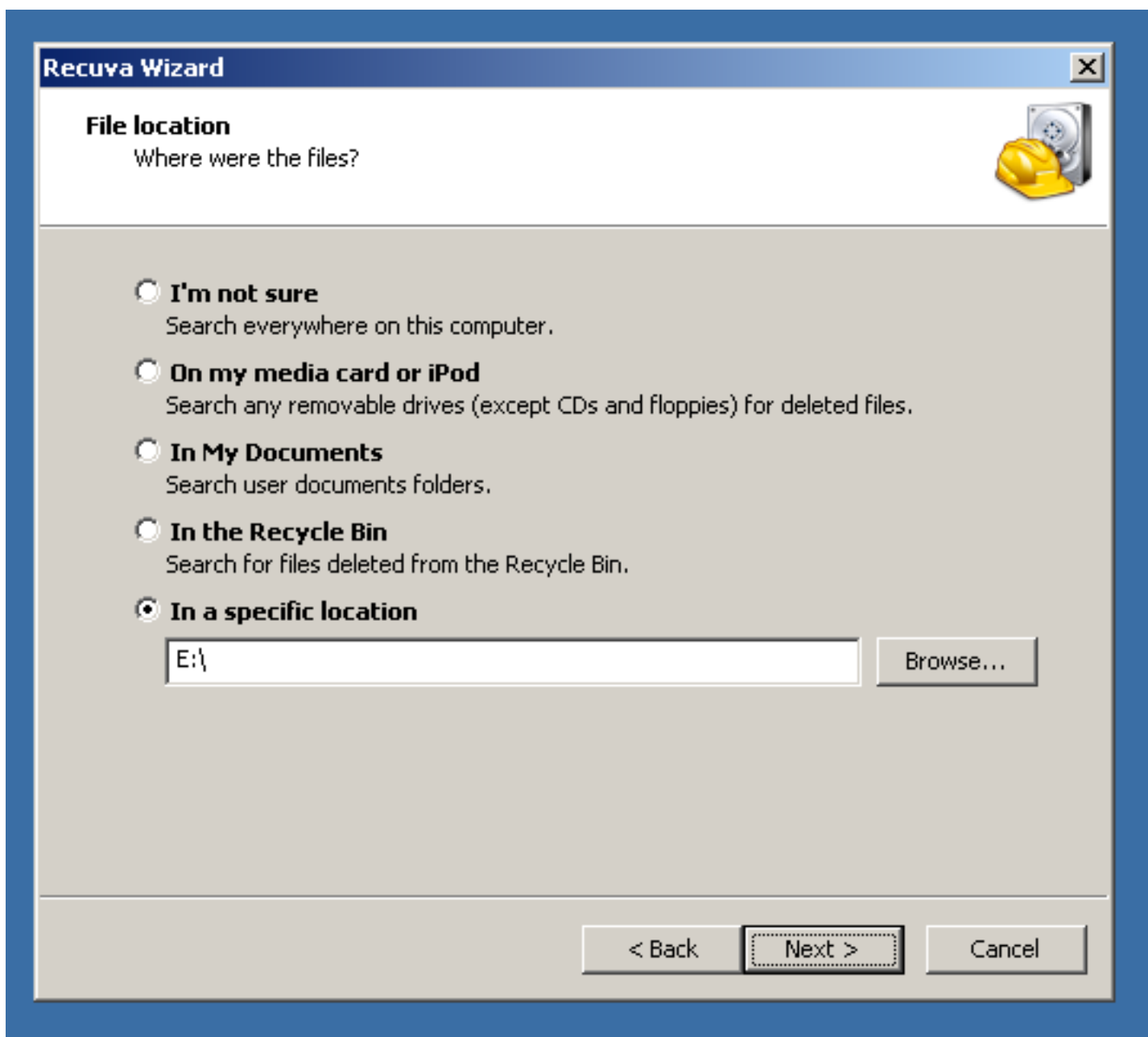
The image shows a Windows-style dialog box titled "Recuva Wizard". The window has a blue title bar with a close button (X) in the top right corner. Below the title bar, the text "File location" is displayed in bold, followed by the question "Where were the files?". To the right of this text is an icon of a yellow hard hat and a silver hard drive. Below this, there are five radio button options:

- I'm not sure**
Search everywhere on this computer.
- On my media card or iPod**
Search any removable drives (except CDs and floppies) for deleted files.
- In My Documents**
Search user documents folders.
- In the Recycle Bin**
Search for files deleted from the Recycle Bin.
- In a specific location**

Under the "In a specific location" option, there is a text input field containing "E:\". To the right of the input field is a button labeled "Browse...". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

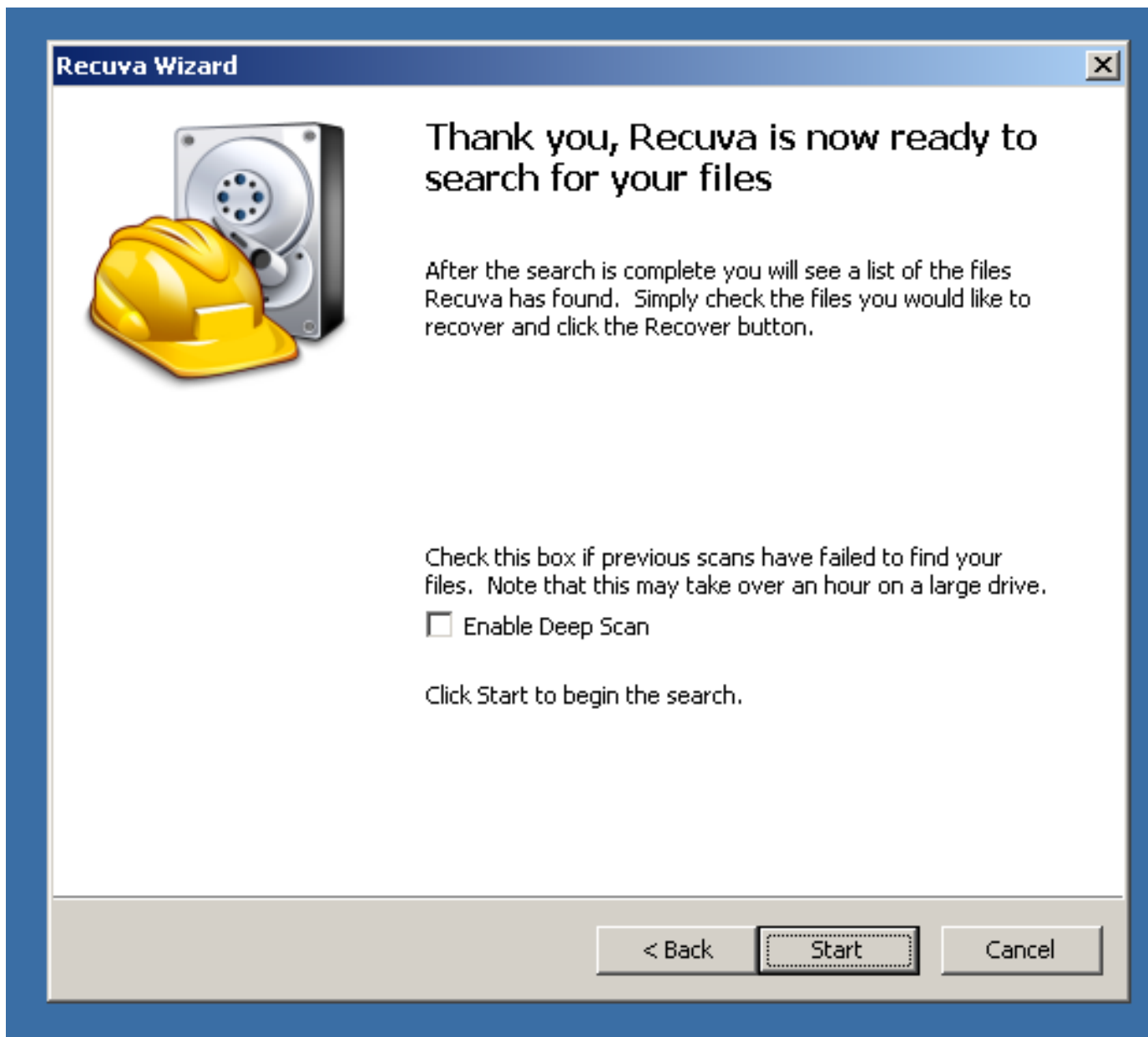
Step 27:

Click on the "Next" button of the "File location" box:



Step 28:

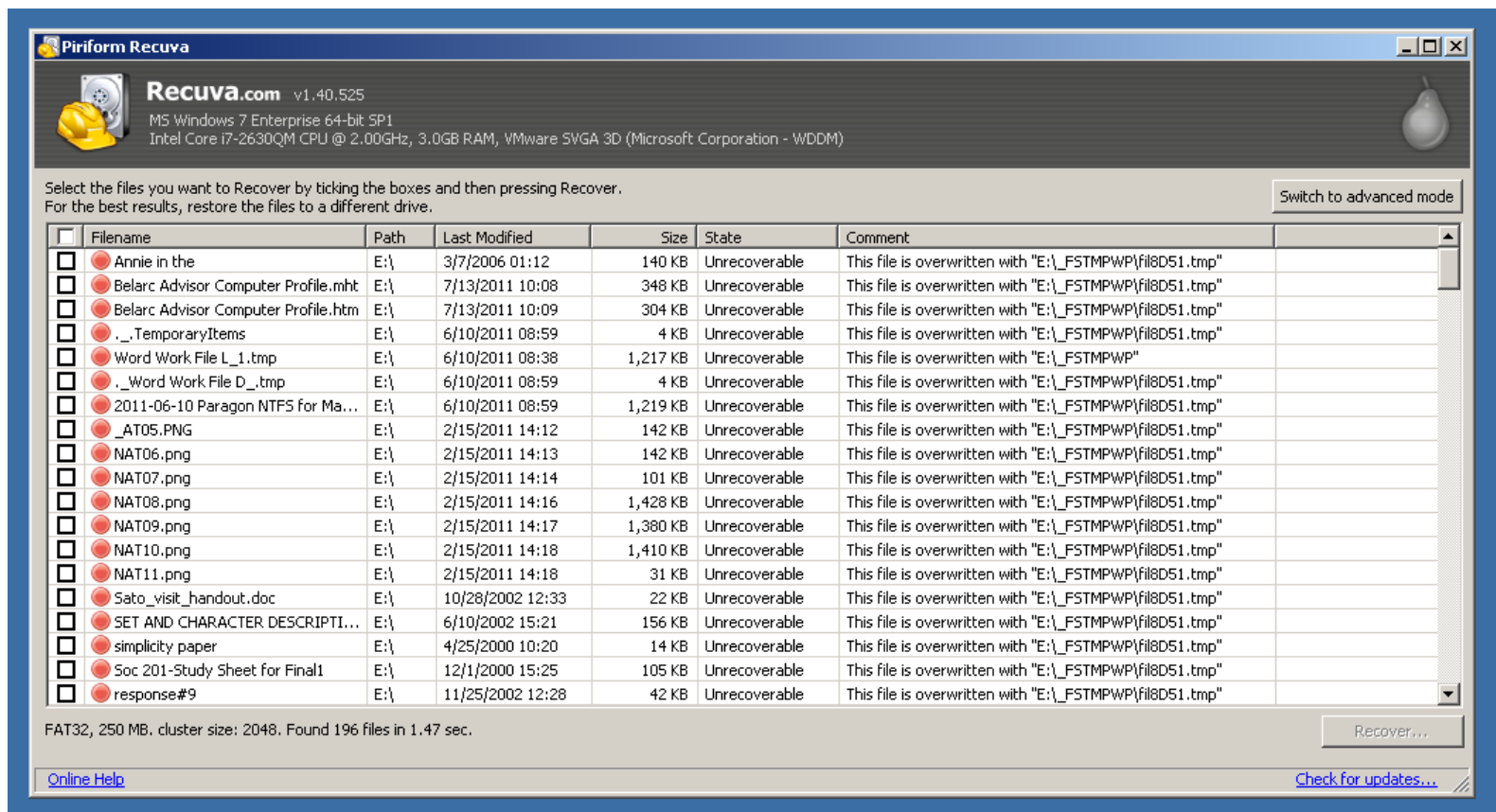
Click on the "Start" button of the "Thank you.." box:



Step 29:

After a while, the results will be displayed.

You want to see lots of red dots to the left of the file names that were discovered. If there are red dots to the left of all deleted files, then "Recuva" will be unable to restore these files and the above steps have been successful in wiping your hard drive or USB flash drive.



The screenshot shows the Piriform Recuva v1.40.525 interface. The window title is "Piriform Recuva". The top bar includes the Recuva logo and version information. Below the title bar, the system information is displayed: "MS Windows 7 Enterprise 64-bit SP1, Intel Core i7-2630QM CPU @ 2.00GHz, 3.0GB RAM, VMware SVGA 3D (Microsoft Corporation - WDDM)".

The main area contains a list of files with columns for Filename, Path, Last Modified, Size, State, and Comment. The files listed are:

Filename	Path	Last Modified	Size	State	Comment
Annie in the	E:\	3/7/2006 01:12	140 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
Belarc Advisor Computer Profile.mht	E:\	7/13/2011 10:08	348 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
Belarc Advisor Computer Profile.htm	E:\	7/13/2011 10:09	304 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
._TemporaryItems	E:\	6/10/2011 08:59	4 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
Word Work File L_1.tmp	E:\	6/10/2011 08:38	1,217 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP"
._Word Work File D_.tmp	E:\	6/10/2011 08:59	4 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
2011-06-10 Paragon NTFS for Ma...	E:\	6/10/2011 08:59	1,219 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
_AT05.PNG	E:\	2/15/2011 14:12	142 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT06.png	E:\	2/15/2011 14:13	142 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT07.png	E:\	2/15/2011 14:14	101 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT08.png	E:\	2/15/2011 14:16	1,428 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT09.png	E:\	2/15/2011 14:17	1,380 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT10.png	E:\	2/15/2011 14:18	1,410 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
NAT11.png	E:\	2/15/2011 14:18	31 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
Sato_visit_handout.doc	E:\	10/28/2002 12:33	22 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
SET AND CHARACTER DESCRIPTI...	E:\	6/10/2002 15:21	156 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
simplicity paper	E:\	4/25/2000 10:20	14 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
Soc 201-Study Sheet for Final1	E:\	12/1/2000 15:25	105 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"
response#9	E:\	11/25/2002 12:28	42 KB	Unrecoverable	This file is overwritten with "E:_FSTMPWP\fil8D51.tmp"

At the bottom of the window, it shows "FAT32, 250 MB, cluster size: 2048. Found 196 files in 1.47 sec." and a "Recover..." button. There are also links for "Online Help" and "Check for updates..."

