Project 8 for CNIT 121: NTFS Data Runs (25 points)

Purpose

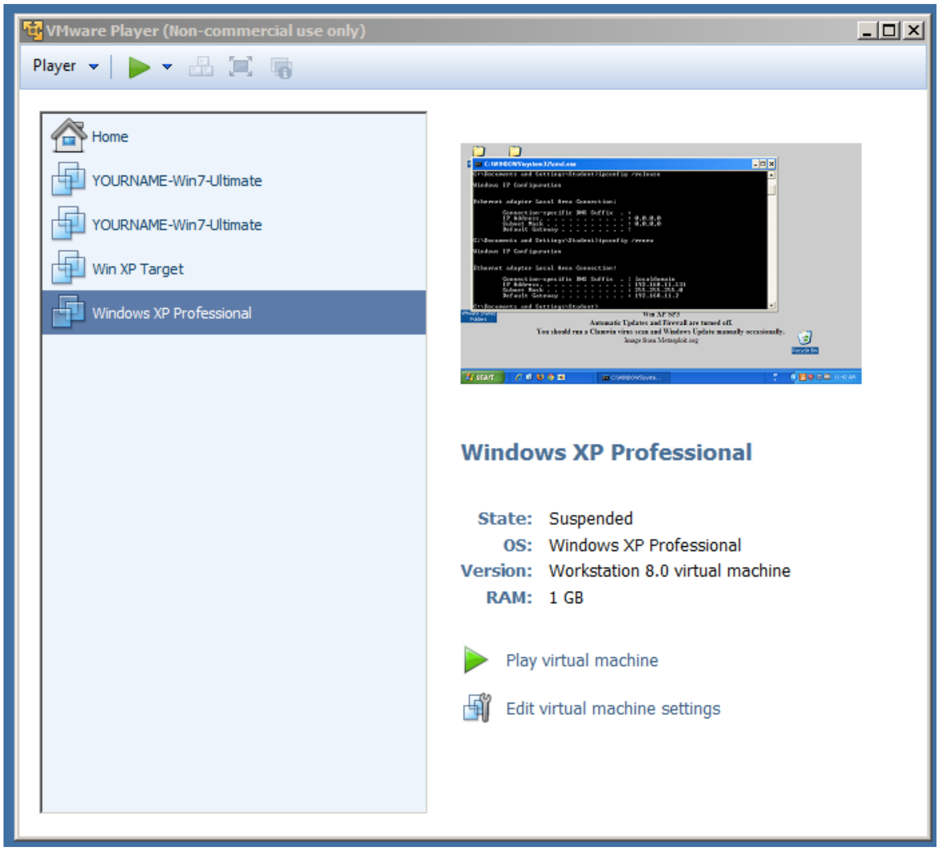
To examine and adjust NTFS directory structure directly at the binary level.

What You Need

- A Windows machine, of any type. I wrote the instructions using VMware fusion, and the Windows Server 2008 guest you have used in previous projects.
- You could also do this project with a single physical machine and use a USB flash drive as the target drive.

Adding a Small Disk to the Virtual Machine

Launch VMware Player. If your virtual machine is "Suspended" as shown below, start it and shut it down properly.



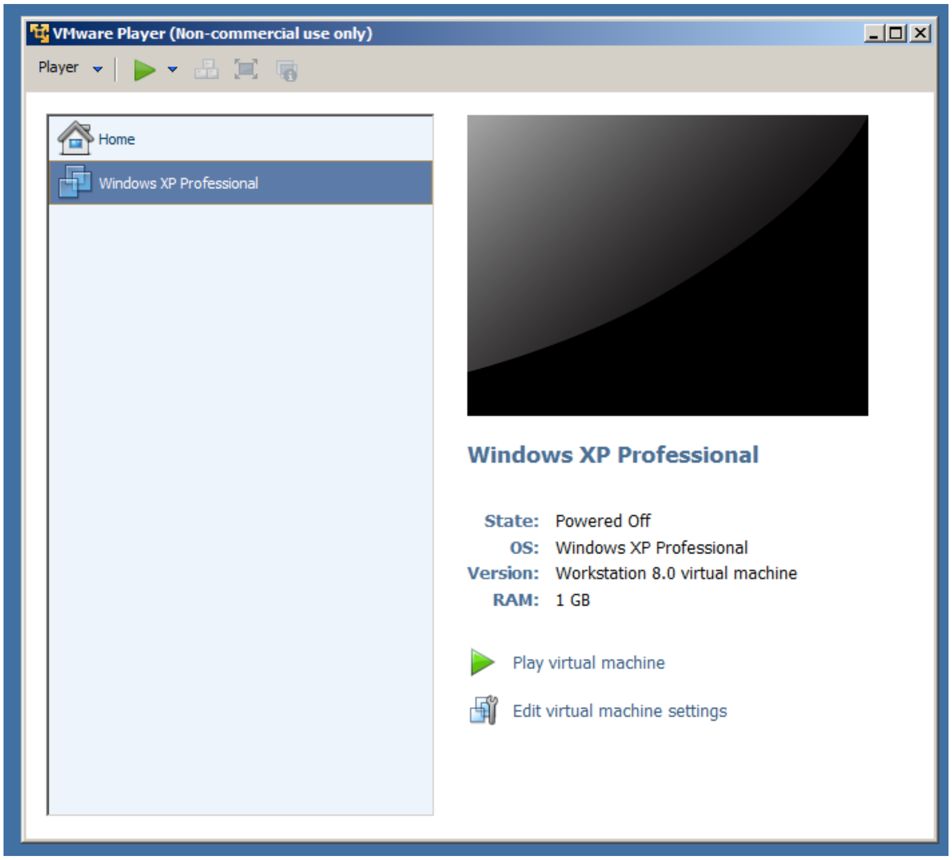
Windows XP Professional

State: Suspended
OS: Windows XP Professional
Version: Workstation 8.0 virtual machine
RAM: 1 GB

If VMware Player closed, open it again.

Your virtual machine should now be "Powered Off", as shown below.

On the lower right, click the "**Edit virtual machine settings**" link.



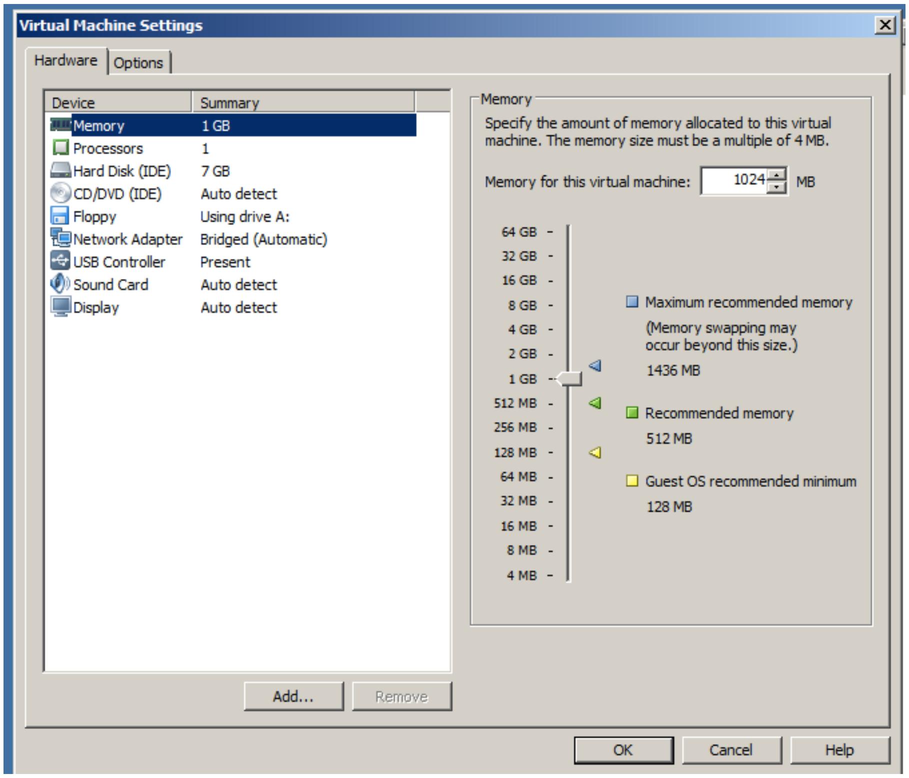
VMware Player (Non-commercial use only)
Player
Home
Windows XP Professional
Play virtual machine
Edit virtual machine settings

Windows XP Professional

State: Powered Off
OS: Windows XP Professional
Version: Workstation 8.0 virtual machine
RAM: 1 GB

The "Virtual Machine Settings" opens, as shown below.

On the lower left, click the **Add...** button.



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	7 GB
CD/DVD (IDE)	Auto detect
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 1024 MB

Maximum recommended memory
(Memory swapping may occur beyond this size.)
1436 MB

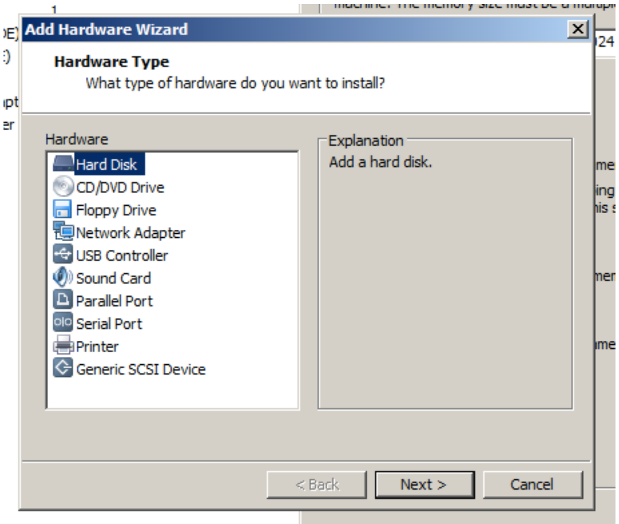
Recommended memory
512 MB

Guest OS recommended minimum
128 MB

The "Add Hardware Wizard" opens, as shown below.

In the left pane, accept the default selection of "**Hard Disk**".

Click the **Next** button.



Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

Hardware: Hard Disk

Explanation: Add a hard disk.

In the next box, accept the default selection of "**Create a new virtual disk**".

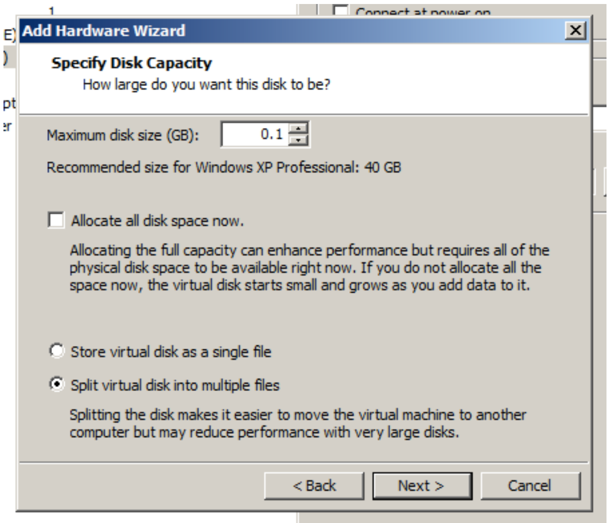
Click the **Next** button.

In the next screen, accept the default selection of "**IDE (Recommended)**".

Click the **Next** button.

In the "Specify Disk Capacity" screen, set the Maximum disk size to **0.1** GB, as shown below.

Click the **Next** button.



Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 0.1

Recommended size for Windows XP Professional: 40 GB

☐ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

In the "Specify Disk File" screen, accept the default selection.

Click the **Finish** button.

In the "Virtual Machine Settings" screen, click the **OK** button.

Click the "**Play Virtual Machine**" button.

Forensically Cleaning the Disk

Windows can now access the disk. But there is no reason to assume it is clean--disk space often contains latent data.

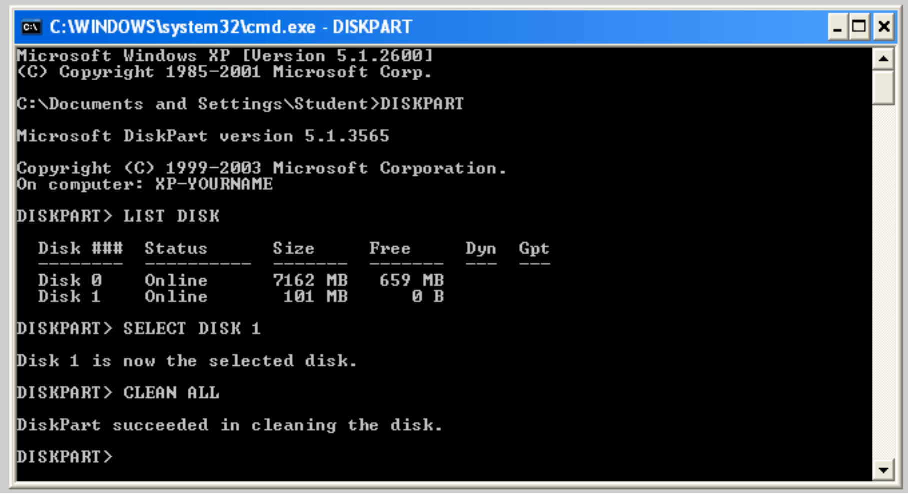
So we'll forensically clean it, writing 00 on every byte.

In your virtual machine, click **Start**, **Run**.

In the Run box, type **CMD** and press Enter to open a Command Prompt.

In the Command Prompt window, type these commands, pressing Enter after each one:

```
DISKPART

LIST DISK
```



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Student>DISKPART

Microsoft DiskPart version 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
On computer: XP-YOURNAME

DISKPART> LIST DISK

  Disk ###  Status      Size     Free     Dyn  Gpt
  --------  ----------  -------  -------  ---  ---
  Disk 0    Online      7162 MB   659 MB
  Disk 1    Online       101 MB      0 B

DISKPART> SELECT DISK 1

Disk 1 is now the selected disk.

DISKPART> CLEAN ALL

DiskPart succeeded in cleaning the disk.

DISKPART>
```

Read the output to find the new 101 MB disk you want to clean--when I did it, it was Disk 1. You don't want to erase the wrong disk by accident!

In the Command Prompt window, excute these commands, specifying the correct disk in the first command:

```
SELECT DISK 1

CLEAN ALL
```

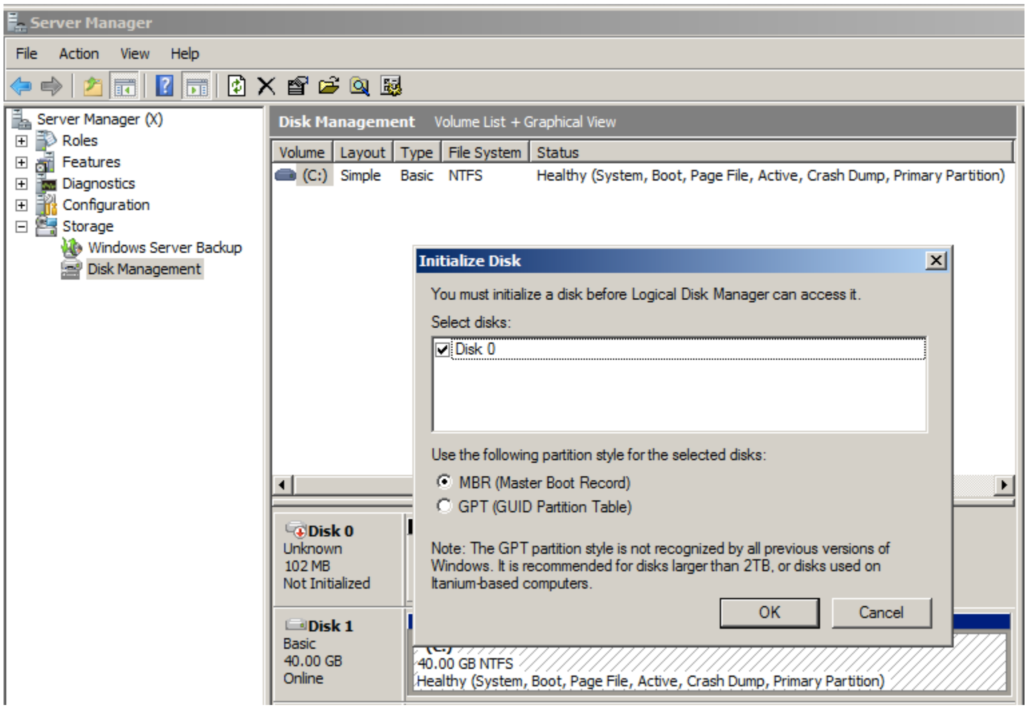
Initializing the New Disk

In your virtual machine, click **Start**.

Right-click "**Computer**" and click **Manage**.

In the left pane of Server Manager, expand **Storage** and click "**Disk Management**".

An "Initialize Disk" box opens, as shown below.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 0

Use the following partition style for the selected disks:

● MBR (Master Boot Record)

○ GPT (GUID Partition Table)

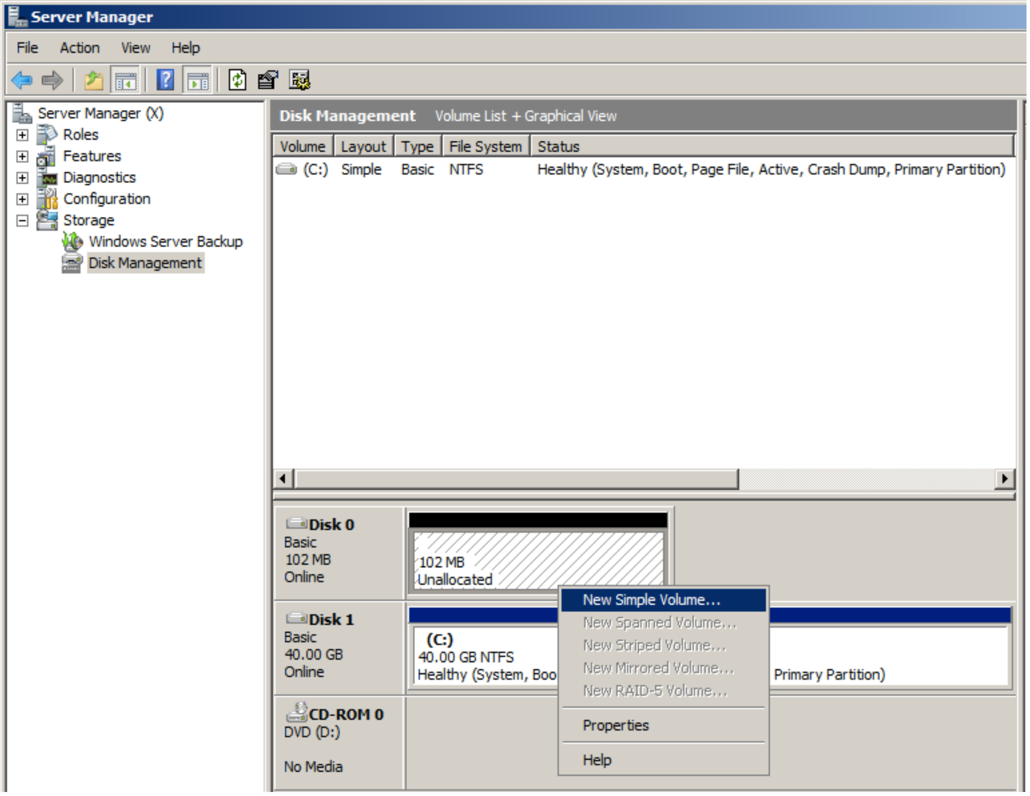
Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.

In the "Initilze Disk" box, accept the default choice of "MBR (Master Boot Record)" and click **OK**.

Parititioning and Formatting the New Drive

In Disk Management, in the lower center, right-click the "Unallocated" space on your new hard disk.

In the context menu, click "**New Simple Volume...**", as shown below.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

Disk 0
Basic
102 MB
Online

102 MB
Unallocated

Disk 1
Basic
40.00 GB
Online

(C:)
40.00 GB NTFS
Healthy (System, Boo ... Primary Partition)

CD-ROM 0
DVD (D:)

No Media

The "New Simple Volume Wizard" opens.

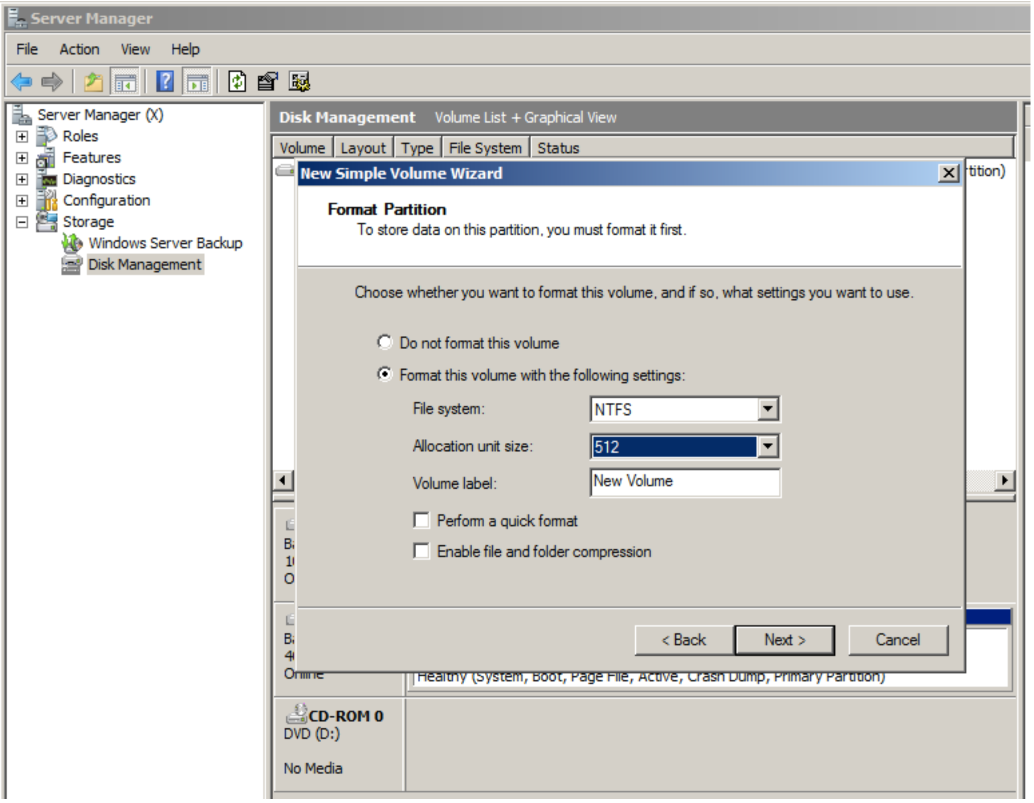
Click **Next**.

In the "Select Volume Size" screen, accept the default size and click **Next**.

In the "Assign Drive Letter or Path" screen, accept the default selection and click **Next**.

In the "Format Partition" screen, set the "Allocation unit size" to **512**, as shown below, and click **Next**.

This size makes each cluster equal to a sector, which is how floppy disks work. It's inefficient for large disks, but OK for this small disk and it simplifies the project.



Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: NTFS

Allocation unit size: 512

Volume label: New Volume

□ Perform a quick format

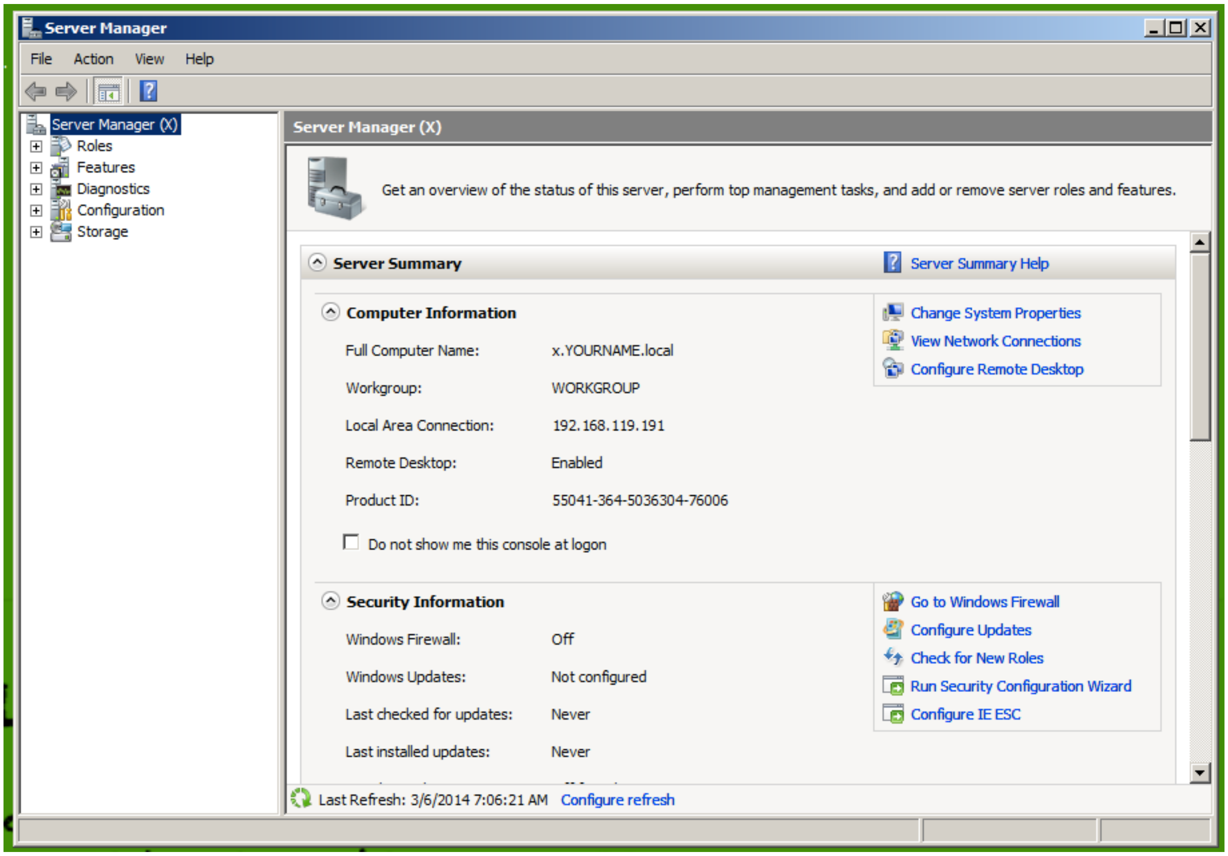
□ Enable file and folder compression

In the "Completing the New Simple Volume Wizard" screen, click **Finish**.

Turning Off Internet Explorer Enhanced Security Configuration

This is an annoyance that only happens on Server versions of windows. It's intended to deter people from surfing the Internet on a server.

In the lower right of Server Manager, in the "Security Information" section, click the "**Configure IE ESC**" link, as shown below.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Computer Information

Full Computer Name: x.YOURNAME.local

Workgroup: WORKGROUP

Local Area Connection: 192.168.119.191

Remote Desktop: Enabled

Product ID: 55041-364-5036304-76006

☐ Do not show me this console at logon

Security Information

Windows Firewall: Off

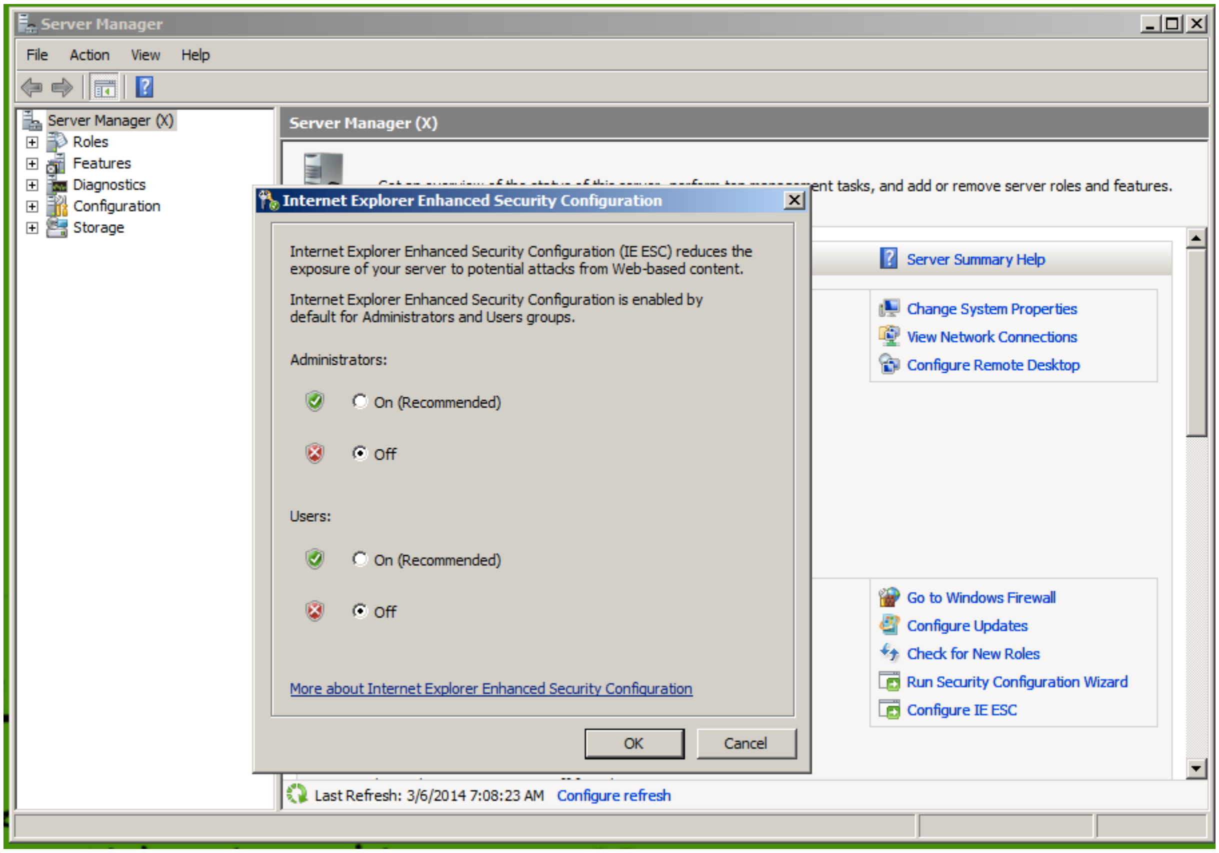
Windows Updates: Not configured

Last checked for updates: Never

Last installed updates: Never

Last Refresh: 3/6/2014 7:06:21 AM

Click both **Off** buttons, as shown below. Then click **OK**.



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

○ On (Recommended)

● Off

Last Refresh: 3/6/2014 7:08:23 AM

Downloading the Test Files

In your virtual machine, open Internet Explorer and open this page of instructions.

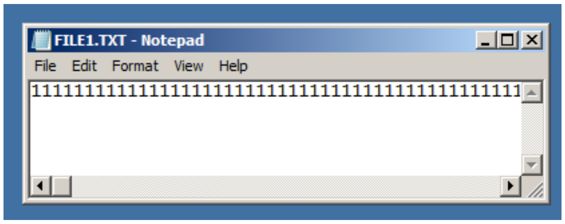
Right-click the FILE1.TXT link below and save the file on your desktop.

Repeat the process for FILE2.TXT.

FILE1.TXT
FILE2.TXT

On your desktop, double-click **FILE1.TXT** to open it in Notepad.

As you can see, this file contains 1000 "1" characters on a single line.



```
11111111111111111111111111111111111111111111111
```

Open FILE2.TXT to see what it contains--1000 "2" characters.

Close all Notepad windows.

Copying The Test Files to the New Partition

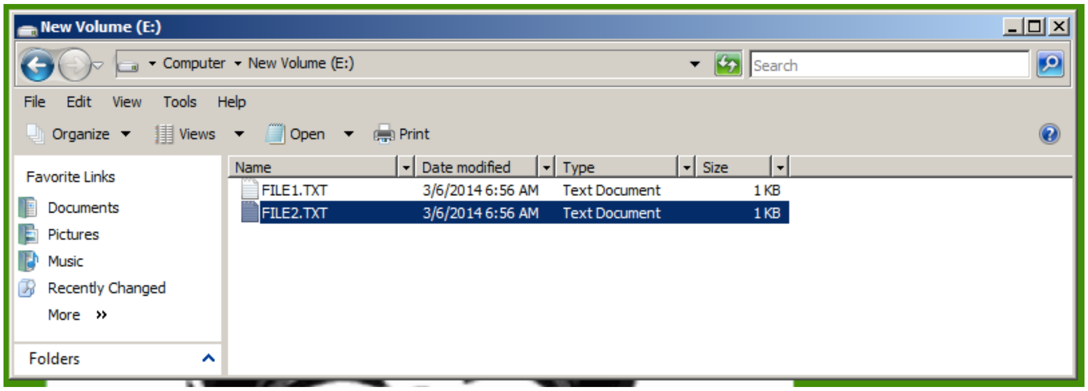
Click **Start**, "**Computer**".

Double-click the "**New Volume**" icon.

Drag the **FILE1.TXT** file from your desktop into the "New Volume" window and drop it there.

Drag the **FILE2.TXT** file from your desktop into the "New Volume" window and drop it there.

The two files should be visible on the new drive, as shown below.



Name	Date modified	Type	Size
FILE1.TXT	3/6/2014 6:56 AM	Text Document	1 KB
FILE2.TXT	3/6/2014 6:56 AM	Text Document	1 KB

Getting WinHex

Open a browser and go to

http://winhex.com

In the center of the page, click **WinHex**

In the left center portion of the window, click **Download**. Save the file on your desktop.

On your desktop, right-click the **winhex.zip** file and click "**Extract All...**".

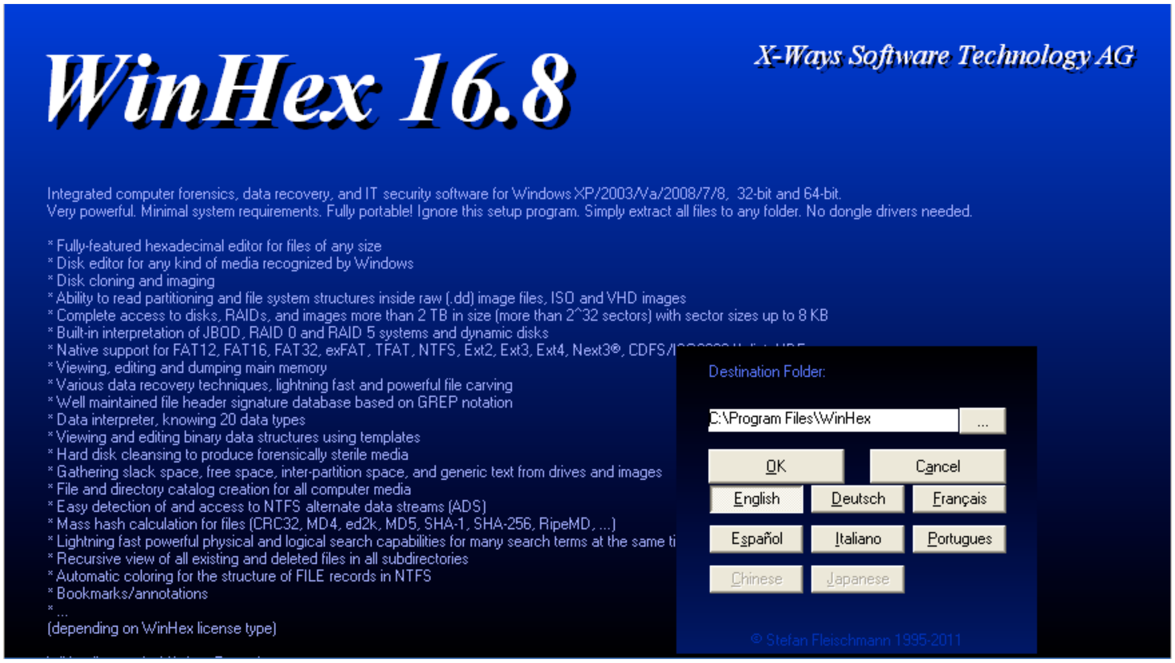
In the "Extract Compressed (zipped) Folders" box, click **Extract**.

A folder with several files opens. Double-click the **setup.exe** file.

If a pop-up box, asks whether you want to run the file, click **Run**.

In the "WinHex 16.8" screen, in the lower right, as shown below, click the **English** button.

Then click the **OK** button.



WinHex 16.8

X-Ways Software Technology AG

Integrated computer forensics, data recovery, and IT security software for Windows XP/2003/Va/2008/7/8, 32-bit and 64-bit.
Very powerful. Minimal system requirements. Fully portable! Ignore this setup program. Simply extract all files to any folder. No dongle drivers needed.

* Fully-featured hexadecimal editor for files of any size
* Disk editor for any kind of media recognized by Windows
* Disk cloning and imaging
* Ability to read partitioning and file system structures inside raw (.dd) image files, ISO and VHD images
* Complete access to disks, RAIDs, and images more than 2 TB in size (more than 2^32 sectors) with sector sizes up to 8 KB
* Built-in interpretation of JBOD, RAID 0 and RAID 5 systems and dynamic disks
* Native support for FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/I
* Viewing, editing and dumping main memory
* Various data recovery techniques, lightning fast and powerful file carving
* Well maintained file header signature database based on GREP notation
* Data interpreter, knowing 20 data types
* Viewing and editing binary data structures using templates
* Hard disk cleansing to produce forensically sterile media
* Gathering slack space, free space, inter-partition space, and generic text from drives and images
* File and directory catalog creation for all computer media
* Easy detection of and access to NTFS alternate data streams (ADS)
* Mass hash calculation for files (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...)
* Lightning fast powerful physical and logical search capabilities for many search terms at the same ti
* Recursive view of all existing and deleted files in all subdirectories
* Automatic coloring for the structure of FILE records in NTFS
* Bookmarks/annotations
* ...
(depending on WinHex license type)

Destination Folder: C:\Program Files\WinHex

A pop-up box, asks whether you want to "Install into C:\Program Files\Winhex". Click **Yes**.

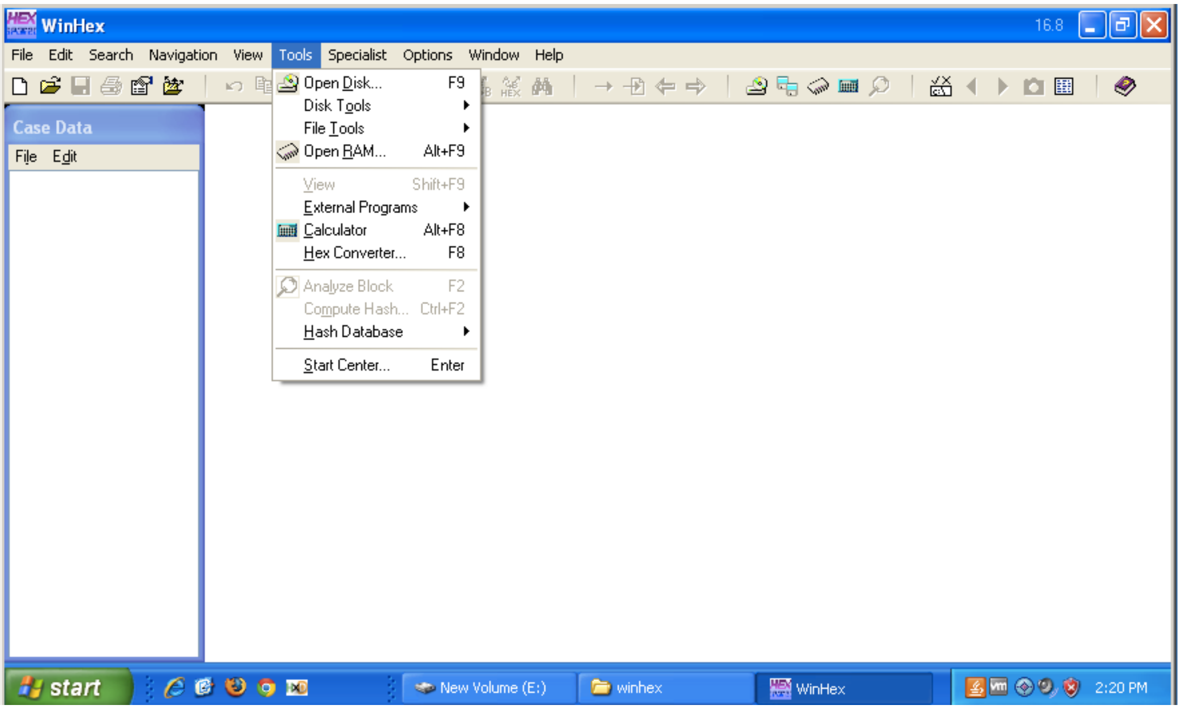
A pop-up box, asks whether you want to "Create program shortcut". Click **Yes**.

A pop-up box, asks whether you want to "Run program". Click **Yes**.

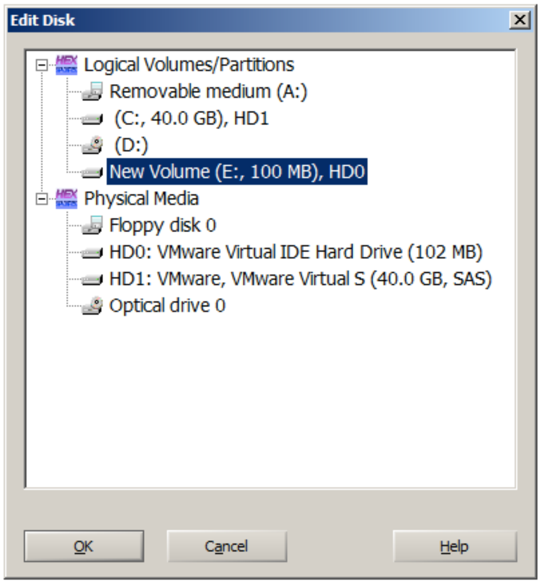
WinHex opens, as shown below.

Viewing the Data in WinHex

From the WinHex menu bar, click **Tools**, "**Open Disk...**".



In the "Edit Disk" box, click "New Volume", as shown below, and then click the **OK** button.

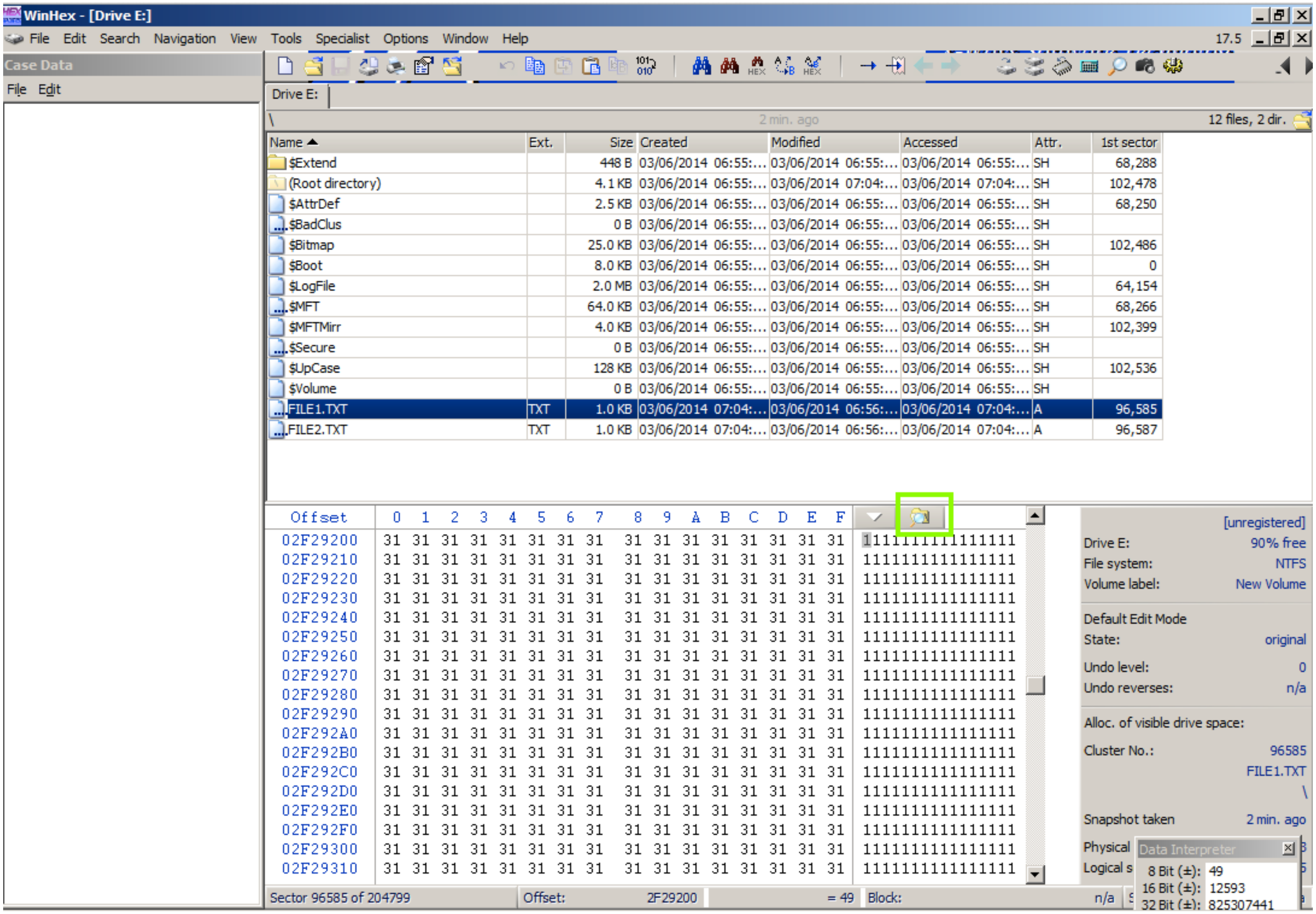


- Logical Volumes/Partitions
  - Removable medium (A:)
  - (C:, 40.0 GB), HD1
  - (D:)
  - New Volume (E:, 100 MB), HD0
- Physical Media
  - Floppy disk 0
  - HD0: VMware Virtual IDE Hard Drive (102 MB)
  - HD1: VMware, VMware Virtual S (40.0 GB, SAS)
  - Optical drive 0

The Directory Browser pane appears in the upper center of the window.

In the Directory Browser, click **FILE1.TXT**.

The lower pane shows the raw hex data in the first cluster containing data for FILE1.TXT, as shown below. All the bytes are hexadecial 31, or the numeral "1".



\

Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
 02F29200   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29210   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29220   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29230   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29240   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29250   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29260   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29270   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29280   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29290   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292A0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292B0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292C0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292D0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292E0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F292F0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29300   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
 02F29310   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
```

[unregistered]

Drive E:	90% free
File system:	NTFS
Volume label:	New Volume
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	96585
	FILE1.TXT
	\
Snapshot taken	2 min. ago
Physical	
Logical s	

Data Interpreter

8 Bit (±):	49
16 Bit (±):	12593
32 Bit (±):	825307441

Sector 96585 of 204799 | Offset: 2F29200 | = 49 | Block: | n/a

In the figure above, in the center right, find the little icon marked with a green box. (It's a magnifying glass on a folder). This icon toggles the display of Directory Browser.

In your WinHex window, click that icon now.

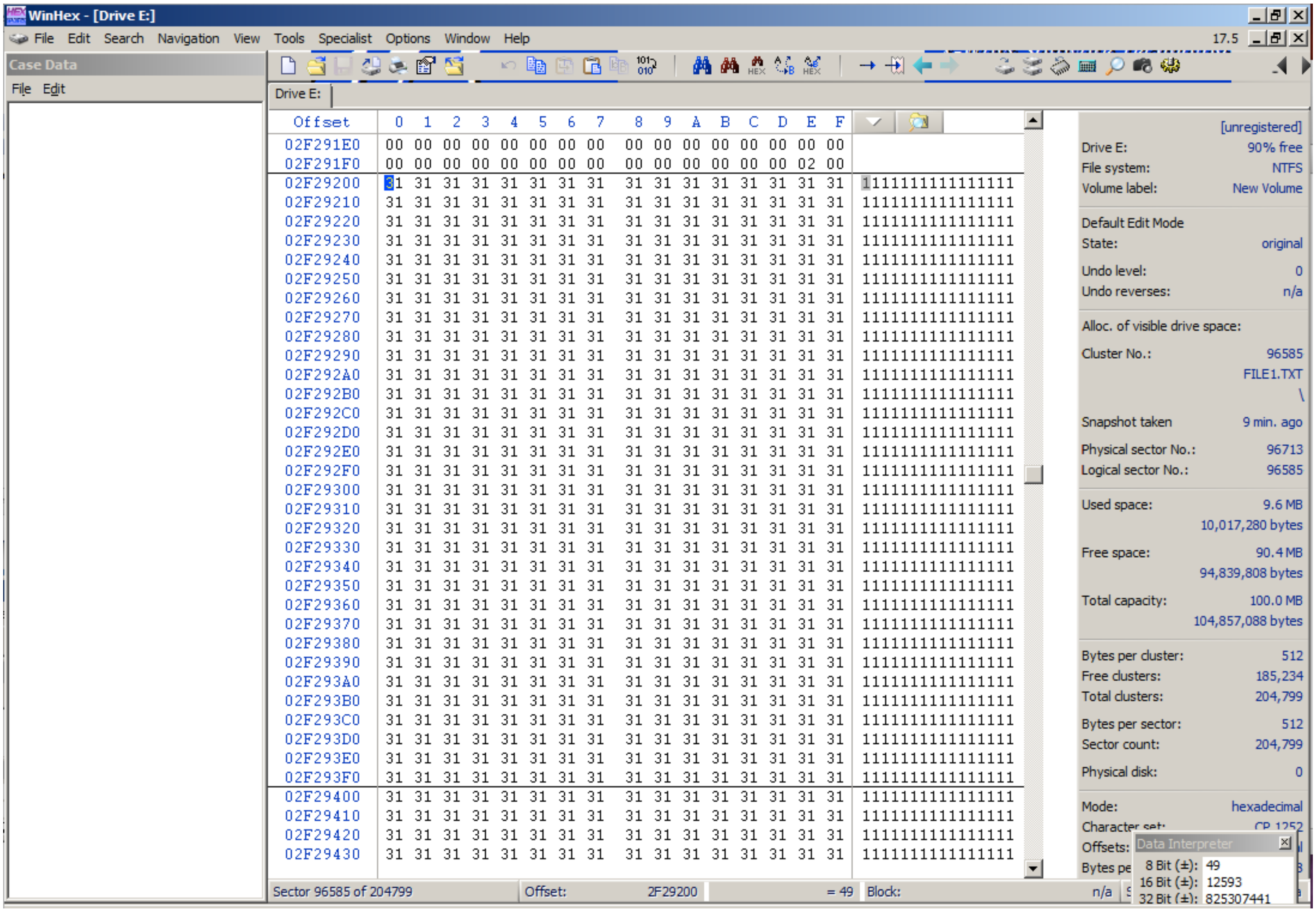
Directory Browser vanishes, so you can see more of the hex view, as shown below.

Scroll up a few rows in the hex view so you can see where the "1" characters start, as shown below.

Click the first "31" to put the cursor there.

Just to the left you can see the hexadecimal address of that disk location--when I did it, the address was 02F29200.

The right side of WinHex shows a gray bar with further details, including the cluster number. When I did it, FILE1 started at cluster number 96585, as shown below.


WinHex - [Drive E:]
File Edit Search Navigation View Tools Specialist Options Window Help
17.5
Case Data
File Edit
Drive E:

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
02F291E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F291F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 02 00
02F29200  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29210  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29220  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29230  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29240  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29250  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29260  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29270  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29280  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29290  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292A0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292B0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292C0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292D0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292E0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F292F0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29300  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29310  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29320  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29330  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29340  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29350  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29360  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29370  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29380  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29390  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293A0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293B0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293C0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293D0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293E0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F293F0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29400  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29410  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29420  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29430  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 96585
FILE1.TXT
\

Snapshot taken 9 min. ago

Physical sector No.: 96713
Logical sector No.: 96585

Used space: 9.6 MB
10,017,280 bytes

Free space: 90.4 MB
94,839,808 bytes

Total capacity: 100.0 MB
104,857,088 bytes

Bytes per cluster: 512
Free clusters: 185,234
Total clusters: 204,799

Bytes per sector: 512
Sector count: 204,799

Physical disk: 0

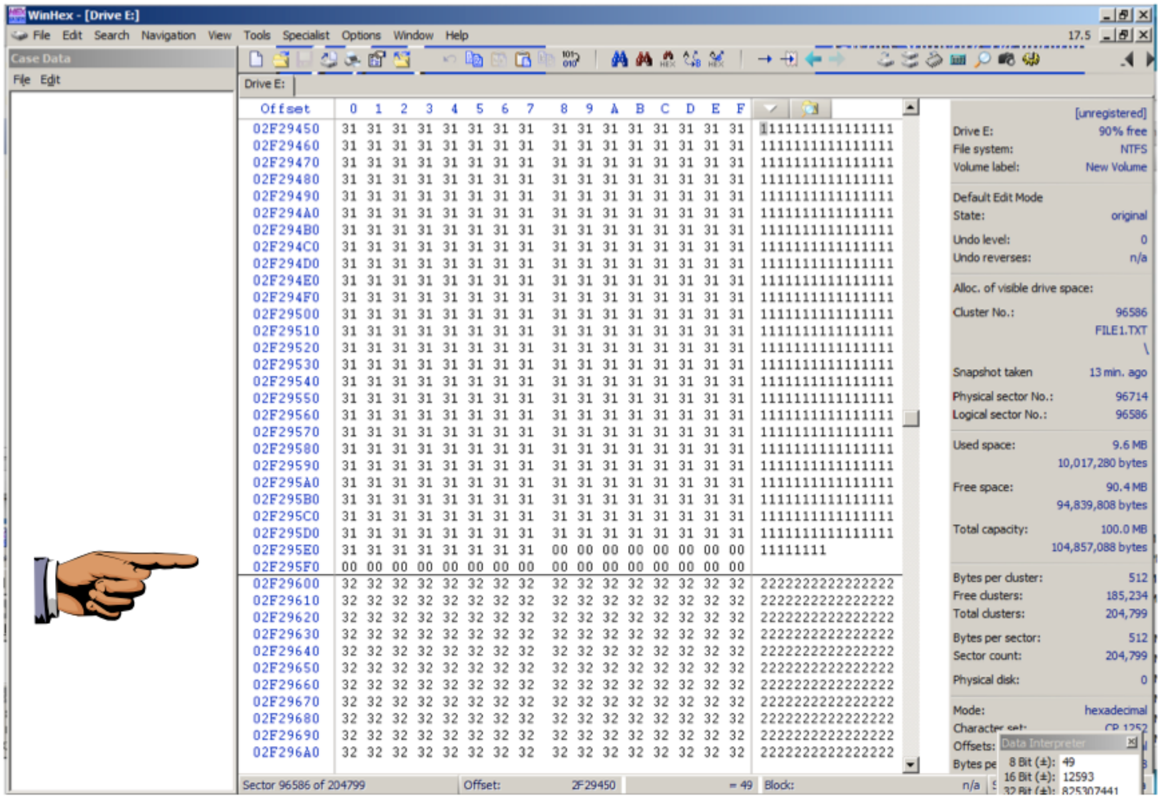
Mode: hexadecimal
Character set: CP 1252
Offsets:
Bytes pe

Data Interpreter
8 Bit (±): 49
16 Bit (±): 12593
32 Bit (±): 825307441

Sector 96585 of 204799 | Offset: 2F29200 | = 49 | Block: n/a

Scroll down in the Hex view until you find the end of the "1" characters.

As shown below, they fill one sector completely, and nearly fill the next sector.


WinHex - [Drive E:]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Drive E:

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
02F29450  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29460  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29470  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29480  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29490  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294A0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294B0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294C0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294D0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294E0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F294F0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29500  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29510  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29520  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29530  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29540  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29550  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29560  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29570  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29580  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F29590  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F295A0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F295B0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F295C0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F295D0  31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31  1111111111111111
02F295E0  31 31 31 31 31 31 31 31  00 00 00 00 00 00 00 00  11111111
02F295F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F29600  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29610  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29620  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29630  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29640  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29650  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29660  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29670  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29680  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F29690  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
02F296A0  32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  2222222222222222
```

```
                       [unregistered]
Drive E:                     90% free
File system:                     NTFS
Volume label:              New Volume

Default Edit Mode
State:                       original
Undo level:                         0
Undo reverses:                    n/a

Alloc. of visible drive space:
Cluster No.:                    96586
                            FILE1.TXT
                                    \
Snapshot taken            13 min. ago
Physical sector No.:            96714
Logical sector No.:             96586

Used space:                    9.6 MB
                     10,017,280 bytes
Free space:                   90.4 MB
                     94,839,808 bytes
Total capacity:              100.0 MB
                    104,857,088 bytes

Bytes per cluster:                512
Free clusters:                185,234
Total clusters:               204,799
Bytes per sector:                 512
Sector count:                 204,799
Physical disk:                      0

Mode:                     hexadecimal
Character set:                CP 1252
Offsets:
Bytes pe

Data Interpreter
8 Bit (±):  49
16 Bit (±): 12593
32 Bit (±): 825307441

Sector 96586 of 204799    Offset:    2F29450    = 49  Block:    n/a
```

Saving a Screen Image

Make sure your screen shows a hex view showing the end of the "1" characters, some zero bytes, and the start of the "2" characters, as shown above.

Sometimes there is a large gap of zeroes between the two files--if that happens, perhaps you forgot to set the cluster size to 512 bytes on your volume.

If the cluster size is correct, and you still see a large gap, use two images to show both the 1s and 2s.

Press the PrintScrn key in the upper-right portion of the keyboard. That will copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE TO GET FULL CREDIT!

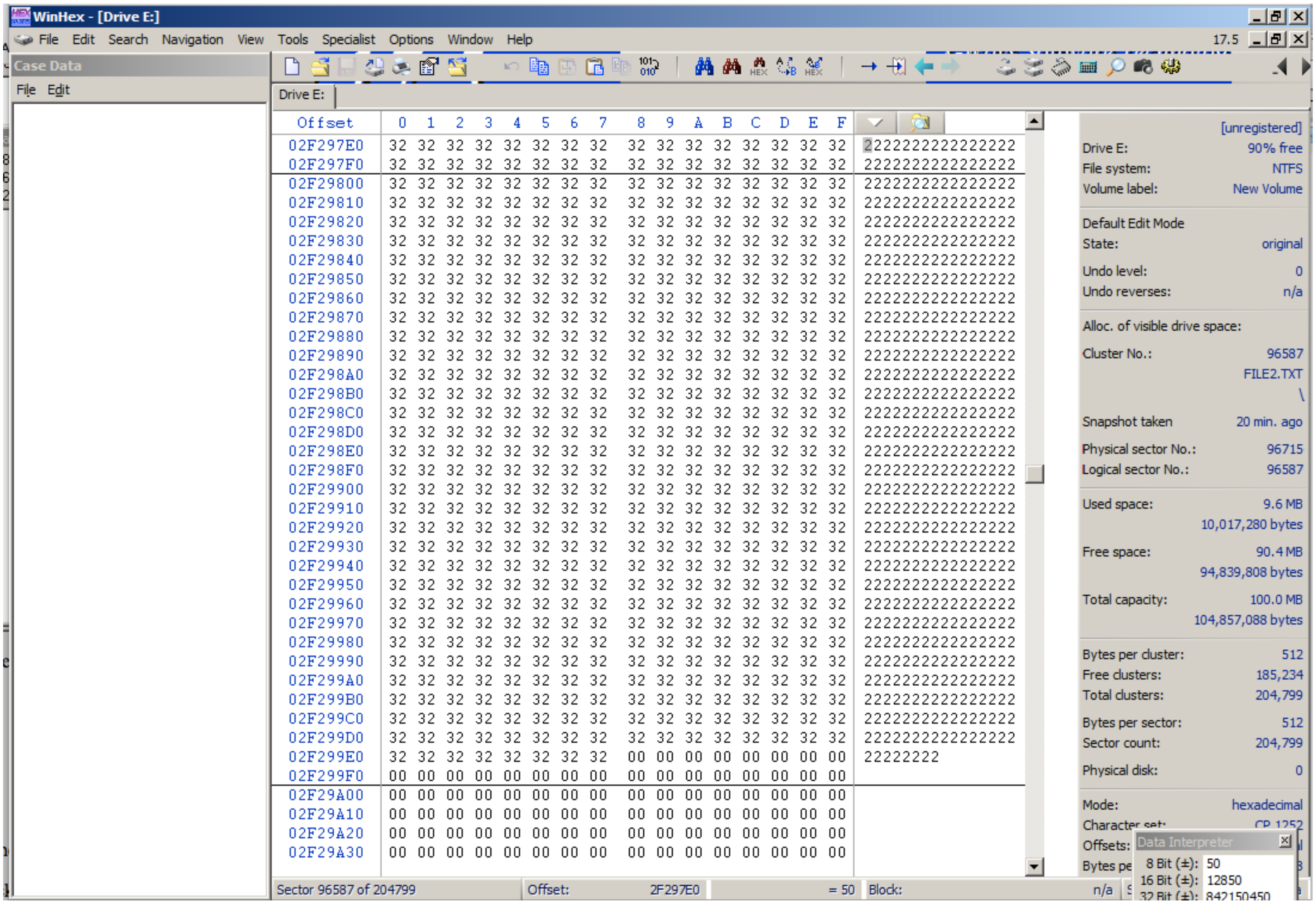
Open Paint and paste in the image.

Save the image with the filename "**Your Name Proj 8a**". Use your real name, not the literal text "Your Name".

Viewing FILE2.TXT in WinHex

Scroll down and see where the "2" characters end.

They should follow the same pattern, filling one sector completely, and nearly filling the next sector, as shown below.


WinHex - [Drive E:]
File Edit Search Navigation View Tools Specialist Options Window Help
17.5
Case Data
File Edit
Drive E:

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
02F297E0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F297F0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29800   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29810   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29820   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29830   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29840   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29850   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29860   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29870   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29880   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29890   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298A0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298B0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298C0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298D0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298E0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F298F0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29900   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29910   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29920   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29930   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29940   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29950   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29960   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29970   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29980   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F29990   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F299A0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F299B0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F299C0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F299D0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32   2222222222222222
02F299E0   32 32 32 32 32 32 32 32  00 00 00 00 00 00 00 00   22222222
02F299F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F29A00   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F29A10   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F29A20   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02F29A30   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

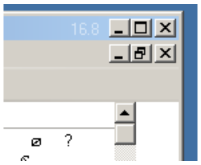
```
                        [unregistered]
Drive E:                      90% free
File system:                      NTFS
Volume label:               New Volume

Default Edit Mode
State:                        original

Undo level:                          0
Undo reverses:                     n/a

Alloc. of visible drive space:
Cluster No.:                     96587
                             FILE2.TXT
                                     \
Snapshot taken              20 min. ago

Physical sector No.:             96715
Logical sector No.:              96587

Used space:                     9.6 MB
                     10,017,280 bytes
Free space:                    90.4 MB
                     94,839,808 bytes
Total capacity:               100.0 MB
                    104,857,088 bytes

Bytes per cluster:                 512
Free clusters:                 185,234
Total clusters:                204,799

Bytes per sector:                  512
Sector count:                  204,799

Physical disk:                       0

Mode:                      hexadecimal
Character set:                 CP 1252
Offsets:
Bytes pe

Data Interpreter
 8 Bit (±): 50
16 Bit (±): 12850
32 Bit (±): 842150450

Sector 96587 of 204799    Offset:    2F297E0    = 50  Block:    n/a
```

Here's a summary of the data layout:

```
Sector   Contents
------   --------
96585       1s
96586    1s and 0s
96587       2s
96588    2s and 0s
```

In the upper right corner of the WinHex window there are two X buttons, as shown below.

Click the lower X button. This closes the "New Volume" drive.



Click the remaining X button. This closes WinHex.

Extending the FILE1.TXT File

In your virtual machine, click **Start**, "**Computer**".

Double-click the "**New Volume**" icon to open the volume.

Double-click the **FILE1.TXT** icon to open the file in Notepad.

Click in the Notepad Window.

Press **Ctrl+A**, **Ctrl+C** to copy the text.

Press **Ctrl+V** five times. This makes the file 5000 bytes long.

Save the file.

Viewing a Fragmented File in WinHex

In your virtual machine, click **Start**, "**All Programs**", **WinHex**.

If an "Open File -- Security Warning" box pops up, click **Run**.

From the WinHex menu bar, click **Tools**, "**Open Disk...**".

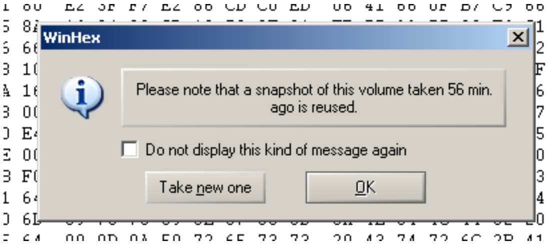
In the "Edit Disk" box, click "New Volume", and then click the **OK** button.

From the WinHex menu bar, click **View**, **Show**, "**Directory Browser**".

A box pops up saying that a snapshot is reused, as shown below. Directory Browser actually works from a copy of the data called a Snapshot, not from the original disk.

We just changed the disk, so an old snapshot won't be accurate.

So click "**Take a new one**".

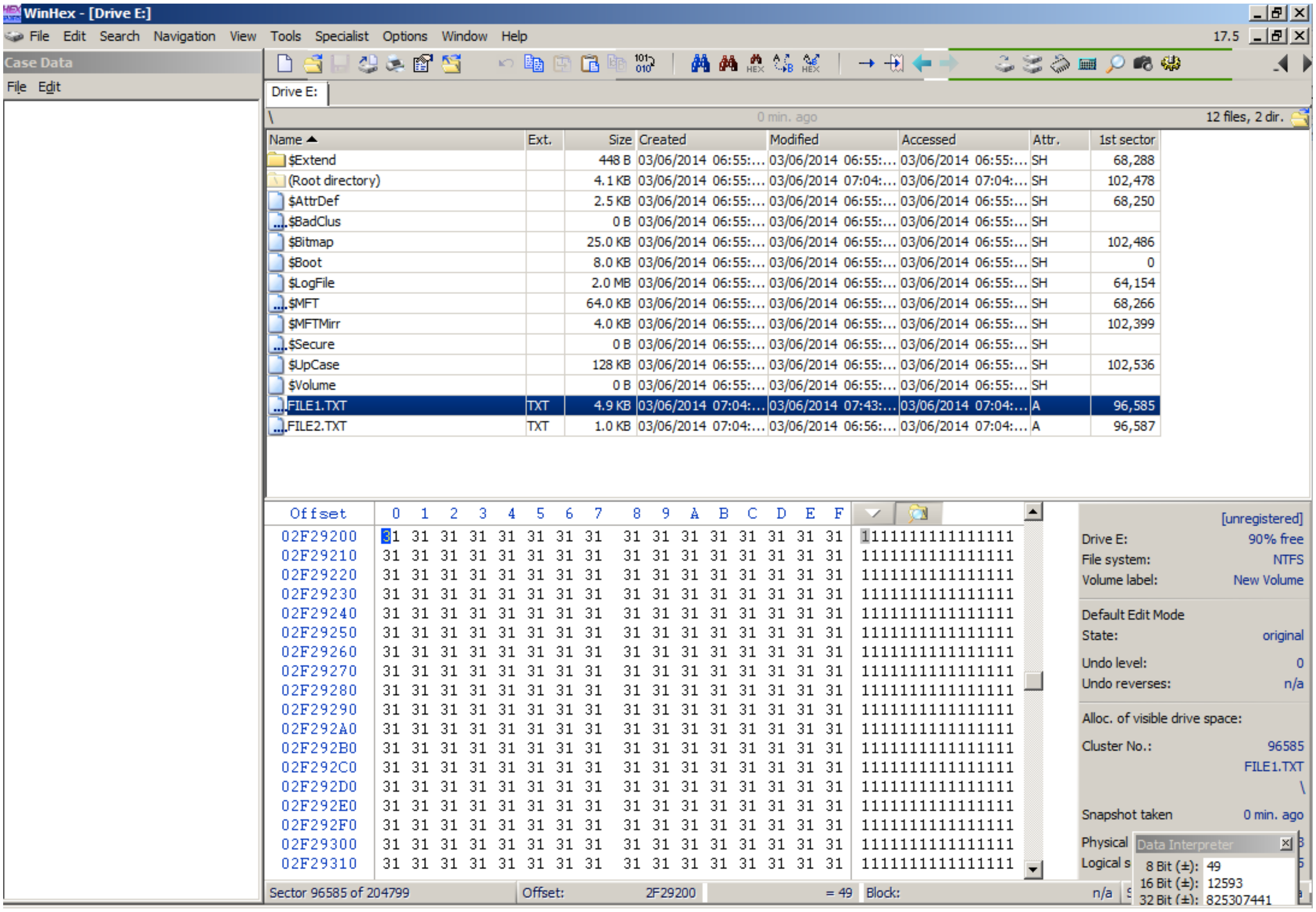


Please note that a snapshot of this volume taken 56 min. ago is reused.

The Directory Browser pane appears in the upper center of the window.

In the Directory Browser, click **FILE1.TXT**.

Notice that FILE1 now has a size of 4.9 KB, as shown below.



Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
02F29200   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29210   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29220   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29230   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29240   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29250   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29260   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29270   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29280   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29290   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292A0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292B0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292C0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292D0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292E0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F292F0   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29300   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
02F29310   31 31 31 31 31 31 31 31  31 31 31 31 31 31 31 31   1111111111111111
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 96585
FILE1.TXT
\

Snapshot taken 0 min. ago

Data Interpreter
8 Bit (±): 49
16 Bit (±): 12593
32 Bit (±): 825307441

Sector 96585 of 204799 Offset: 2F29200 = 49 Block: n/a

Click the yellow icon to hide Directory Browser, as you did before.

Scroll down through the two sectors of "1" characters.

Scroll down through the two sectors of "2" characters.

There should be additional sectors of "1" characters below the "2" characters, as shown below.

Here's a summary of the data layout:

```
Sector  Contents
------  --------
96585      1s
96586   1s and 0s
96587      2s
96588   2s and 0s
96589      1s
96590      1s
  ...      ...
```

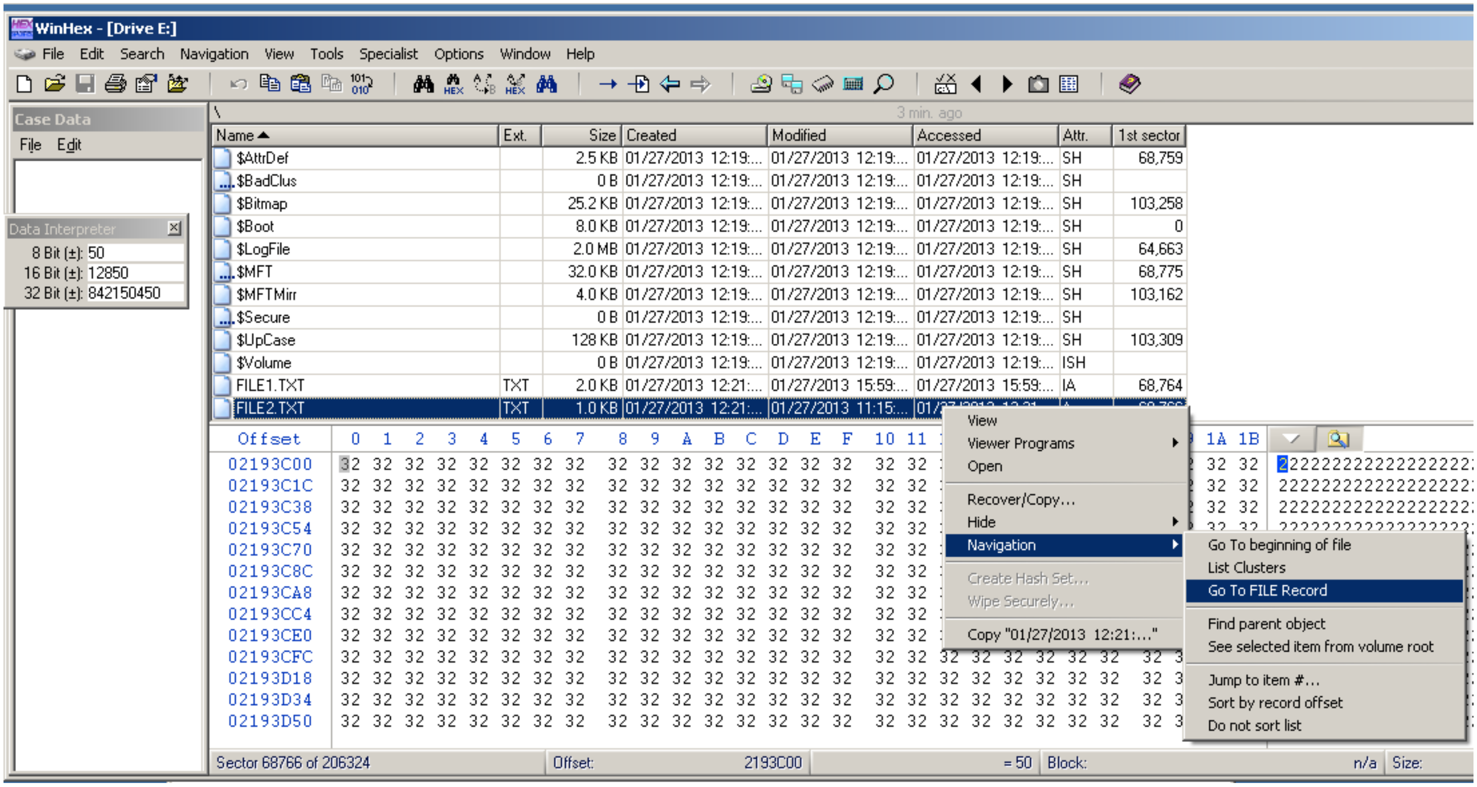
Viewing an MFT Record

Click the little yellow icon to show Directory Browser again.

Scroll to the bottom.

Right-click **FILE2.TXT**.

In the context menu, click **Navigation**, "**Go To FILE Record**", as shown below.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$AttrDef		2.5 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	68,759
$BadClus		0 B	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	
$Bitmap		25.2 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	103,258
$Boot		8.0 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	0
$LogFile		2.0 MB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	64,663
$MFT		32.0 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	68,775
$MFTMirr		4.0 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	103,162
$Secure		0 B	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	
$UpCase		128 KB	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	SH	103,309
$Volume		0 B	01/27/2013 12:19:...	01/27/2013 12:19:...	01/27/2013 12:19:...	ISH	
FILE1.TXT	TXT	2.0 KB	01/27/2013 12:21:...	01/27/2013 15:59:...	01/27/2013 15:59:...	IA	68,764
FILE2.TXT	TXT	1.0 KB	01/27/2013 12:21:...	01/27/2013 11:15:...	01/		

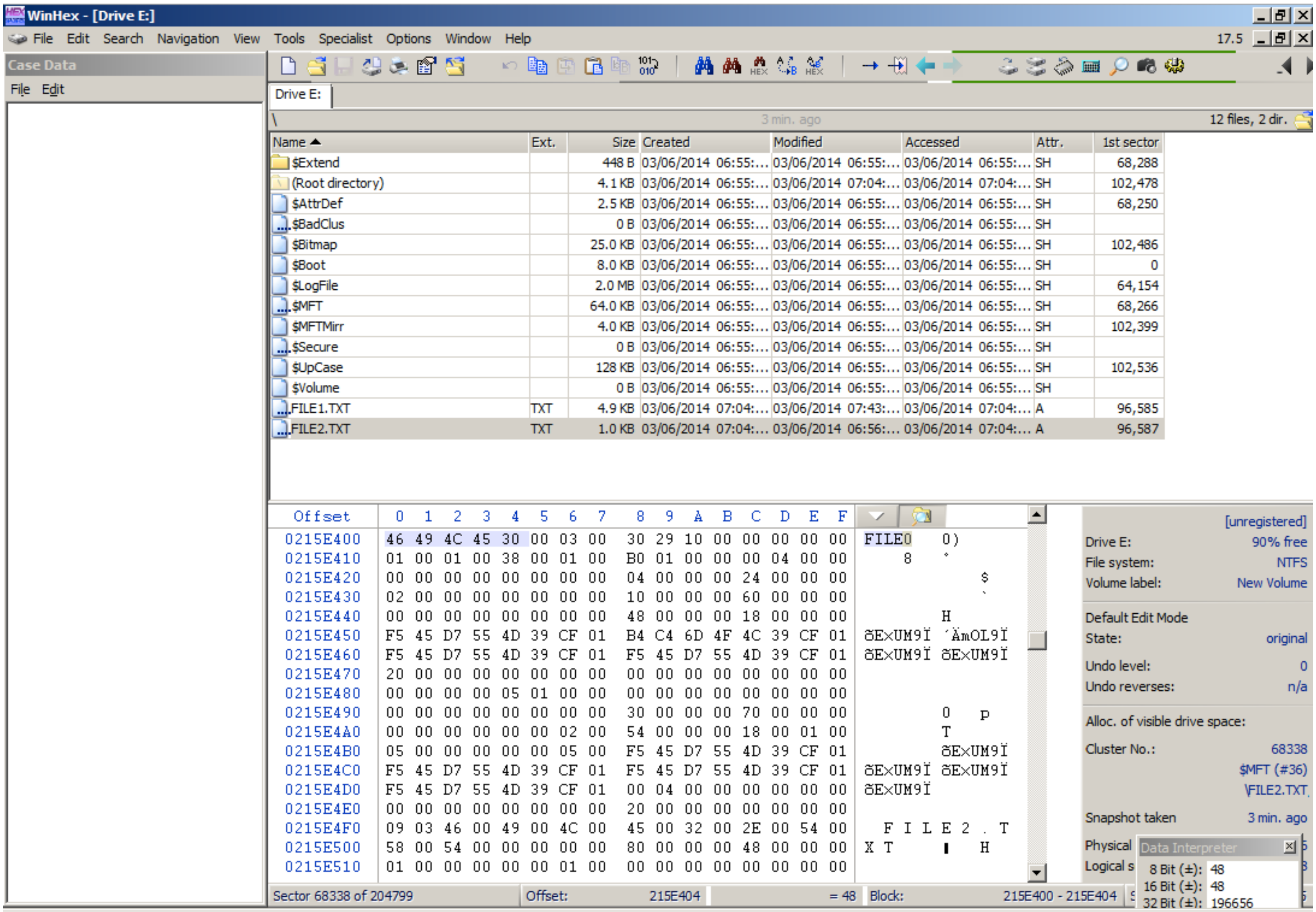
```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   10 11
02193C00   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193C1C   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193C38   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193C54   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193C70   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193C8C   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193CA8   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193CC4   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193CE0   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193CFC   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193D18   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193D34   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
02193D50   32 32 32 32 32 32 32 32  32 32 32 32 32 32 32 32  32 32
```

Sector 68766 of 206324 | Offset: 2193C00 | = 50 | Block: n/a | Size:

This is the Master File Table (MFT) record which contains information about FILE2.TXT.

Each MFT record begins with the ASCII text "FILE0".

Highlight that text, so your screen looks like the image below.


WinHex - [Drive E:]
File Edit Search Navigation View Tools Specialist Options Window Help
17.5
Case Data
File Edit
Drive E:

\ 3 min. ago 12 files, 2 dir.

Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E400   46 49 4C 45 30 00 03 00  30 29 10 00 00 00 00 00   FILE0   0)
0215E410   01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00       8   °
0215E420   00 00 00 00 00 00 00 00  04 00 00 00 24 00 00 00               $
0215E430   02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00               `
0215E440   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00           H
0215E450   F5 45 D7 55 4D 39 CF 01  B4 C4 6D 4F 4C 39 CF 01   õE×UM9Ï ´ÄmOL9Ï
0215E460   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E470   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E480   00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
0215E490   00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00           0   p
0215E4A0   00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00           T
0215E4B0   05 00 00 00 00 00 05 00  F5 45 D7 55 4D 39 CF 01           õE×UM9Ï
0215E4C0   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E4D0   F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00   õE×UM9Ï
0215E4E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E4F0   09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00     F I L E 2 . T
0215E500   58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00   X T     €   H
0215E510   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

Snapshot taken 3 min. ago
Physical
Logical s

Data Interpreter
8 Bit (±): 48
16 Bit (±): 48
32 Bit (±): 196656

Sector 68338 of 204799 Offset: 215E404 = 48 Block: 215E400 - 215E404

MFT Record Header

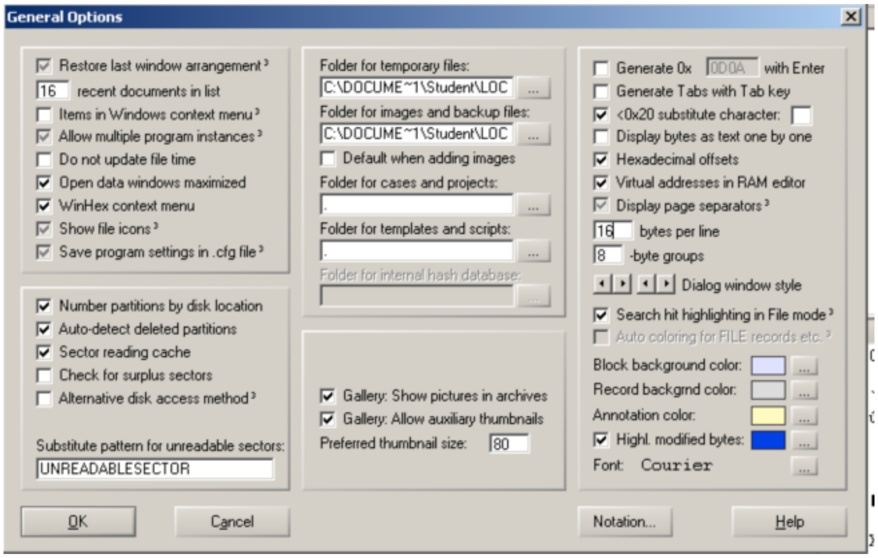
The MFT Record begins with a 56-byte header.

We need to count 56 bytes from this point. That will be a lot easier with only 16 bytes per row.

From the WinHex menu bar, click **Options**, **General**.

On the right side, in the center, verify that it is set to **16** in the "bytes per line" box, as shown below.

Click **OK**.



☑ Restore last window arrangement³
16 recent documents in list
☐ Items in Windows context menu³
☑ Allow multiple program instances³
☐ Do not update file time
☑ Open data windows maximized
☑ WinHex context menu
☑ Show file icons³
☑ Save program settings in .cfg file³

☑ Number partitions by disk location
☑ Auto-detect deleted partitions
☑ Sector reading cache
☐ Check for surplus sectors
☐ Alternative disk access method³

Substitute pattern for unreadable sectors: UNREADABLESECTOR

Folder for temporary files: C:\DOCUME~1\Student\LOC
Folder for images and backup files: C:\DOCUME~1\Student\LOC
☐ Default when adding images
Folder for cases and projects: .
Folder for templates and scripts: .
Folder for internal hash database:

☑ Gallery: Show pictures in archives
☑ Gallery: Allow auxiliary thumbnails
Preferred thumbnail size: 80

☐ Generate 0x 0D0A with Enter
☐ Generate Tabs with Tab key
☑ <0x20 substitute character:
☐ Display bytes as text one by one
☑ Hexadecimal offsets
☑ Virtual addresses in RAM editor
☑ Display page separators³
16 bytes per line
8 -byte groups
Dialog window style
☑ Search hit highlighting in File mode³
☐ Auto coloring for FILE records etc.³
Block background color:
Record backgrnd color:
Annotation color:
☑ Highl. modified bytes:
Font: Courier

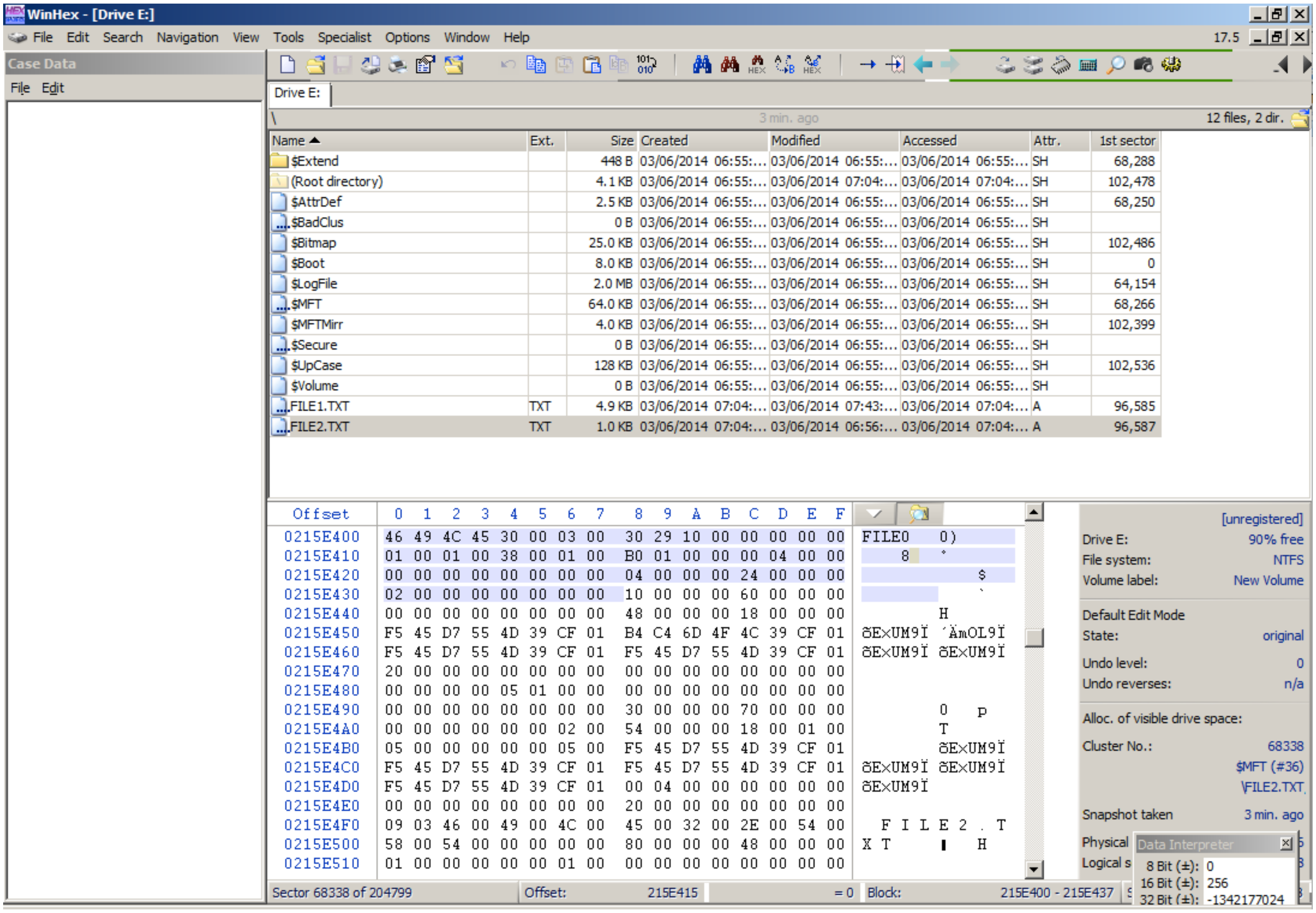
WinHex now has only 16 bytes per line, labelled 0 though F in the "Offset" line at the top of the display, as shown below.

Click on the first byte, with the value: **46**.

Hold down the Shift key and press the down-arrow on the keyboard three times. This selects three lines of 16 bytes for a total of 48 bytes.

Now, holding down the Shift key, press the right-arrow key until you have selected bytes 0 through 7 in that row.

This selects the entire 56 bytes of the MFT record header, as shown below.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
 0215E400  46 49 4C 45 30 00 03 00  30 29 10 00 00 00 00 00  FILE0   0)
 0215E410  01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00      8   °
 0215E420  00 00 00 00 00 00 00 00  04 00 00 00 24 00 00 00              $
 0215E430  02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              `
 0215E440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
 0215E450  F5 45 D7 55 4D 39 CF 01  B4 C4 6D 4F 4C 39 CF 01  õE×UM9Ï ´ÄmOL9Ï
 0215E460  F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01  õE×UM9Ï õE×UM9Ï
 0215E470  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 0215E480  00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
 0215E490  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00          0   p
 0215E4A0  00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00          T
 0215E4B0  05 00 00 00 00 00 05 00  F5 45 D7 55 4D 39 CF 01          õE×UM9Ï
 0215E4C0  F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01  õE×UM9Ï õE×UM9Ï
 0215E4D0  F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00  õE×UM9Ï
 0215E4E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
 0215E4F0  09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00    F I L E 2 . T
 0215E500  58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00  X T     ▌   H
 0215E510  01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
```

	[unregistered]
Drive E:	90% free
File system:	NTFS
Volume label:	New Volume
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	68338
	$MFT (#36)
	\FILE2.TXT
Snapshot taken	3 min. ago

Data Interpreter

8 Bit (±):	0
16 Bit (±):	256
32 Bit (±):	-1342177024

Sector 68338 of 204799 | Offset: 215E415 | = 0 | Block: 215E400 - 215E437

Standard Information (10 00 00 00)

The next secton is the "Standard Information" section.

Each section of the MFT begins with a four-byte identifier--in this case 10 00 00 00.

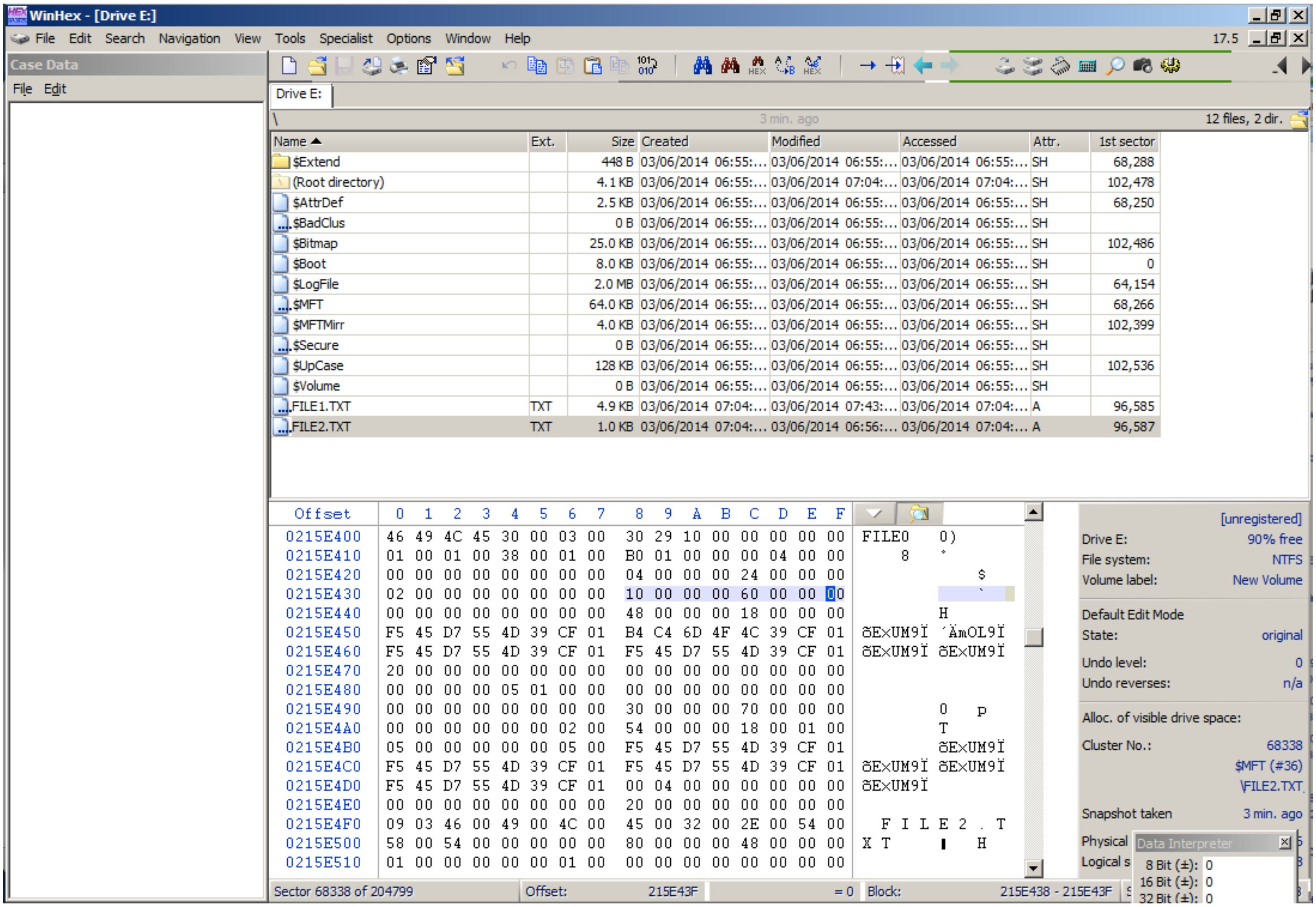
Here is a chart of the MFT attribute types, from http://grayscale-research.org/new/pdfs/NTFS%20forensics.pdf

Figure 2.7 MFT Record Attribute Type Table

Attribute Name	Hexidecimal Value
Unused	0x00
Standard Information	0x10
File Name	0x30
Object ID	0x40
Security Descriptor	0x50
Volume Name	0x60
Volume Information	0x70
Data	0x80
Index Root	0x90
Index Allocation	0xa0
Bitmap	0xb0
Reparse Point	0xc0
EA Information	0xd0
EA	0xe0
Property Set	0xf0
Logged Utility Stream	0x100

The next four bytes indicate the length of the section, in hexadecimal, with the least significant byte first.

So the eight bytes highlighted below indicate that the Standard Information section is 60 bytes long.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E400   46 49 4C 45 30 00 03 00  30 29 10 00 00 00 00 00   FILE0   0)
0215E410   01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00      8   °
0215E420   00 00 00 00 00 00 00 00  04 00 00 00 24 00 00 00             $
0215E430   02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00             `
0215E440   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0215E450   F5 45 D7 55 4D 39 CF 01  B4 C4 6D 4F 4C 39 CF 01   õE×UM9Ï ´ÄmOL9Ï
0215E460   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E470   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E480   00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
0215E490   00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00          0   p
0215E4A0   00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00          T
0215E4B0   05 00 00 00 00 00 05 00  F5 45 D7 55 4D 39 CF 01          õE×UM9Ï
0215E4C0   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E4D0   F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00   õE×UM9Ï
0215E4E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E4F0   09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00     F I L E 2 . T
0215E500   58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00   X T     ▮   H
0215E510   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

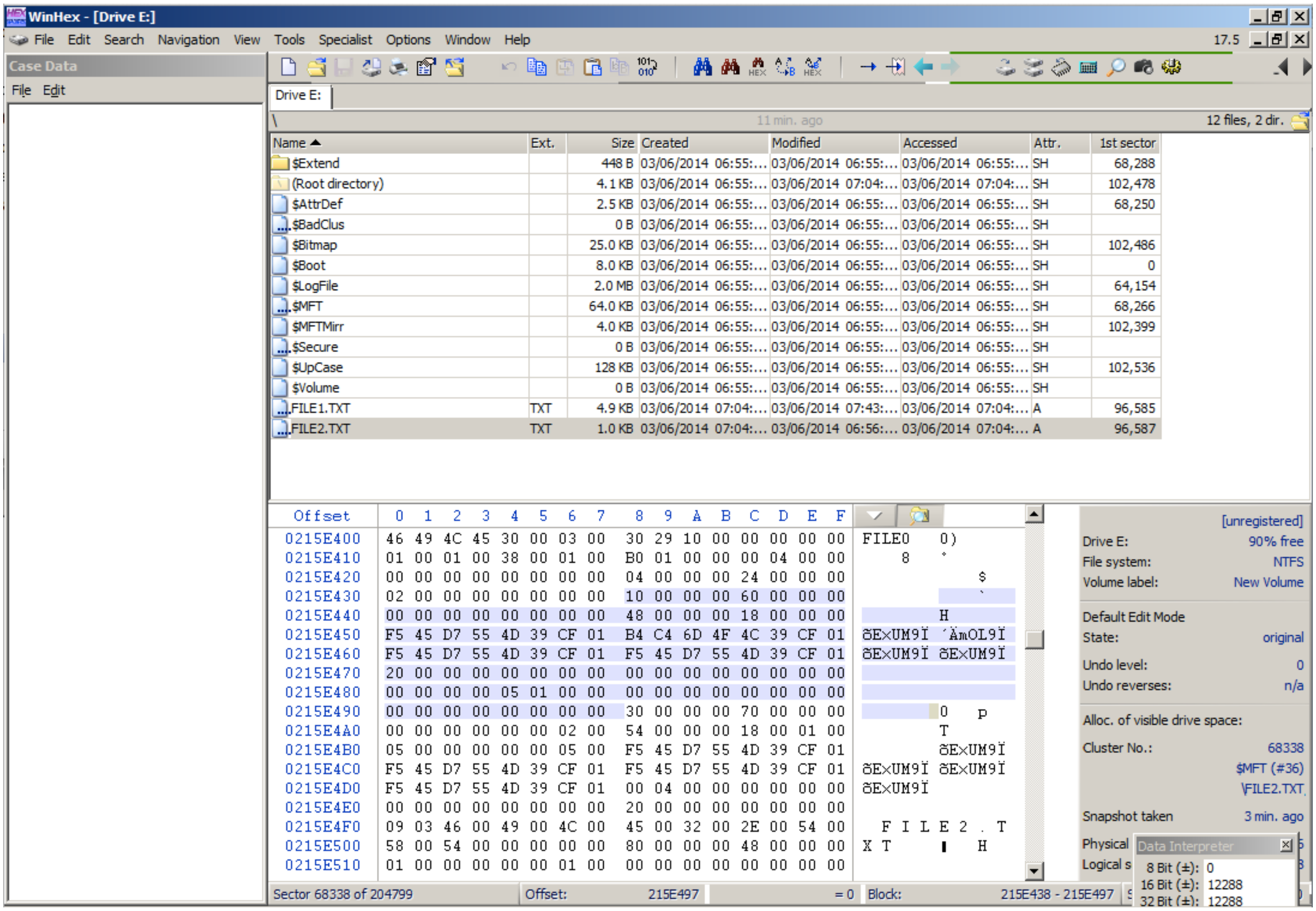
Snapshot taken 3 min. ago

Physical
Logical s

Data Interpreter
8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 0

Sector 68338 of 204799 | Offset: 215E43F | = 0 | Block: 215E438 - 215E43F

Highlight the entire Standard Information section. It will be six entire rows of 16 bytes, as shown below.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E400   46 49 4C 45 30 00 03 00  30 29 10 00 00 00 00 00   FILE0   0)
0215E410   01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00       8   °
0215E420   00 00 00 00 00 00 00 00  04 00 00 00 24 00 00 00             $
0215E430   02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00             `
0215E440   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00           H
0215E450   F5 45 D7 55 4D 39 CF 01  B4 C4 6D 4F 4C 39 CF 01   õE×UM9Ï ´ÄmOL9Ï
0215E460   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E470   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E480   00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
0215E490   00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00           0   p
0215E4A0   00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00           T
0215E4B0   05 00 00 00 00 00 05 00  F5 45 D7 55 4D 39 CF 01           õE×UM9Ï
0215E4C0   F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01   õE×UM9Ï õE×UM9Ï
0215E4D0   F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00   õE×UM9Ï
0215E4E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E4F0   09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00     F I L E 2 . T
0215E500   58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00   X T     ▮   H
0215E510   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
```

Sector 68338 of 204799 | Offset: 215E497 | = 0 | Block: 215E438 - 215E497

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:

Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

Snapshot taken 3 min. ago

Physical
Logical s

Data Interpreter
8 Bit (±): 0
16 Bit (±): 12288
32 Bit (±): 12288

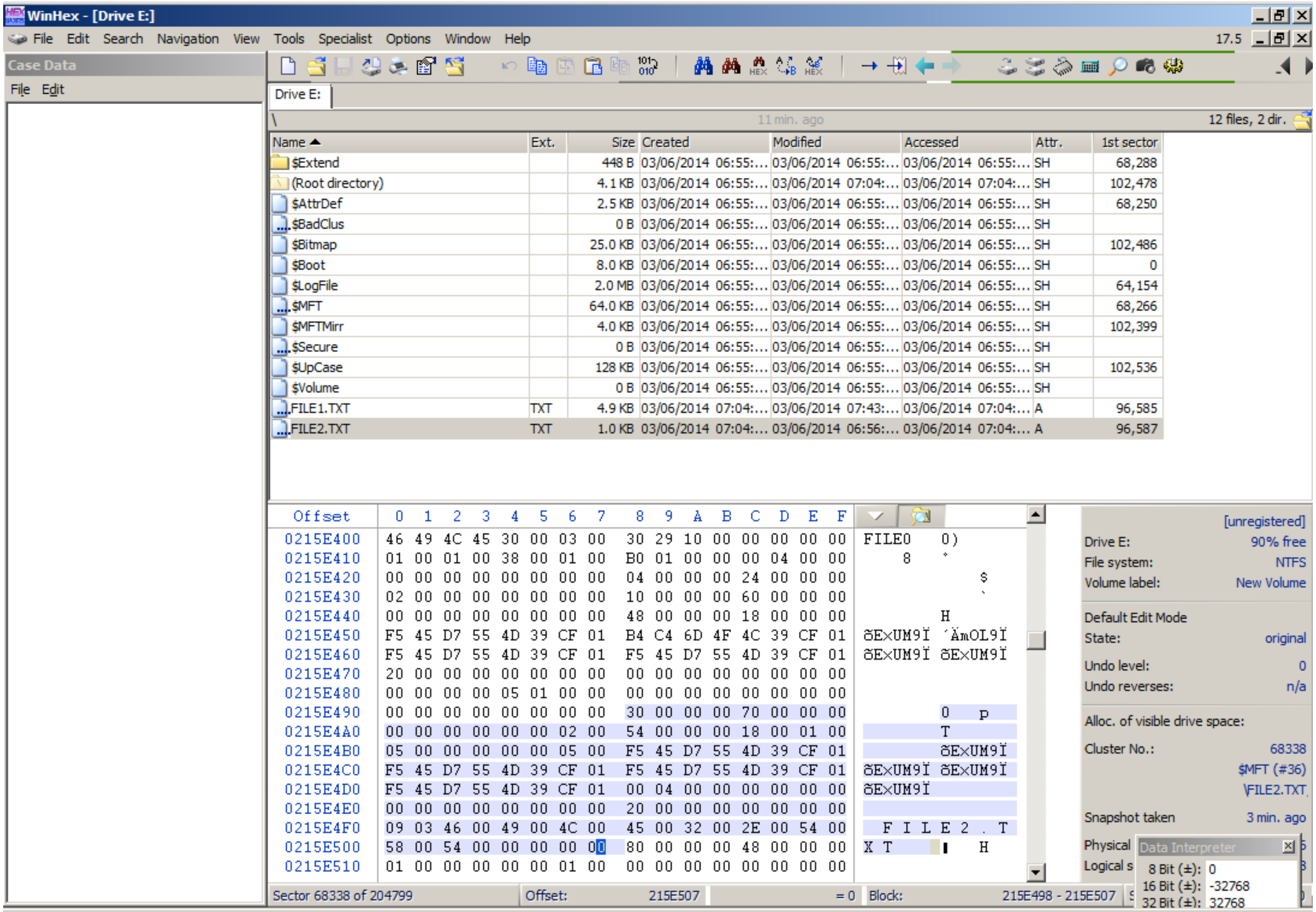
File Name section

The next section begins with 30 00 00 00 and is 70 bytes long, as shown below.

Highlight the section.

Notice the readable file name near the end of this section: FILE2.TXT.

It's in Unicode, so there's a 00 byte after each readable character.


WinHex - [Drive E:]
File Edit Search Navigation View Tools Specialist Options Window Help
17.5
Case Data
File Edit
Drive E:
11 min. ago

\ 12 files, 2 dir.

Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E400  46 49 4C 45 30 00 03 00  30 29 10 00 00 00 00 00  FILE0   0)
0215E410  01 00 01 00 38 00 01 00  B0 01 00 00 00 04 00 00      8   °
0215E420  00 00 00 00 00 00 00 00  04 00 00 00 24 00 00 00              $
0215E430  02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              `
0215E440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0215E450  F5 45 D7 55 4D 39 CF 01  B4 C4 6D 4F 4C 39 CF 01  õE×UM9Ï ´ÄmOL9Ï
0215E460  F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01  õE×UM9Ï õE×UM9Ï
0215E470  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E480  00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
0215E490  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00          0   p
0215E4A0  00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00          T
0215E4B0  05 00 00 00 00 00 05 00  F5 45 D7 55 4D 39 CF 01          õE×UM9Ï
0215E4C0  F5 45 D7 55 4D 39 CF 01  F5 45 D7 55 4D 39 CF 01  õE×UM9Ï õE×UM9Ï
0215E4D0  F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00  õE×UM9Ï
0215E4E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E4F0  09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00   F I L E 2 . T
0215E500  58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00  X T      ▮   H
0215E510  01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
```

Sector 68338 of 204799 | Offset: 215E507 | = 0 | Block: 215E498 - 215E507

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

Snapshot taken 3 min. ago

Physical
Logical s

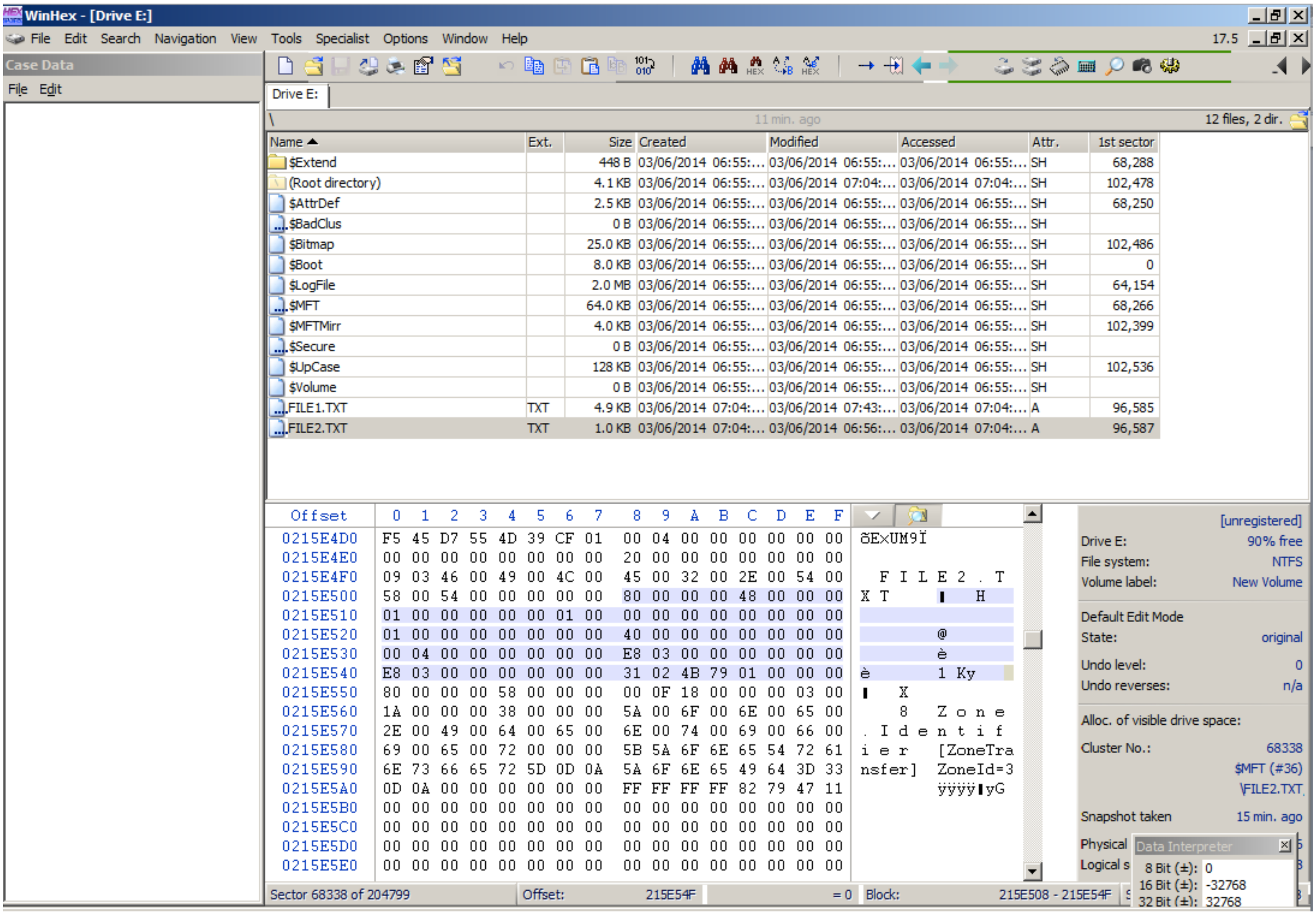
Data Interpreter
8 Bit (±): 0
16 Bit (±): -32768
32 Bit (±): 32768

Data Section

The next section begins with 80 00 00 00 and is 48 bytes long, as shown below.

This section indicates where the data is actually stored on the disk.

Highlight the section.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
 0215E4D0   F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00  õE×UM9Ï
 0215E4E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
 0215E4F0   09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00    F I L E 2 . T
 0215E500   58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00  X T     ▮   H
 0215E510   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
 0215E520   01 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00          @
 0215E530   00 04 00 00 00 00 00 00  E8 03 00 00 00 00 00 00          è
 0215E540   E8 03 00 00 00 00 00 00  31 02 4B 79 01 00 00 00  è        1 Ky
 0215E550   80 00 00 00 58 00 00 00  00 0F 18 00 00 00 03 00  ▮   X
 0215E560   1A 00 00 00 38 00 00 00  5A 00 6F 00 6E 00 65 00      8   Z o n e
 0215E570   2E 00 49 00 64 00 65 00  6E 00 74 00 69 00 66 00  . I d e n t i f
 0215E580   69 00 65 00 72 00 00 00  5B 5A 6F 6E 65 54 72 61  i e r   [ZoneTra
 0215E590   6E 73 66 65 72 5D 0D 0A  5A 6F 6E 65 49 64 3D 33  nsfer]  ZoneId=3
 0215E5A0   0D 0A 00 00 00 00 00 00  FF FF FF FF 82 79 47 11          ÿÿÿÿ▮yG
 0215E5B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 0215E5C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 0215E5D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
 0215E5E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

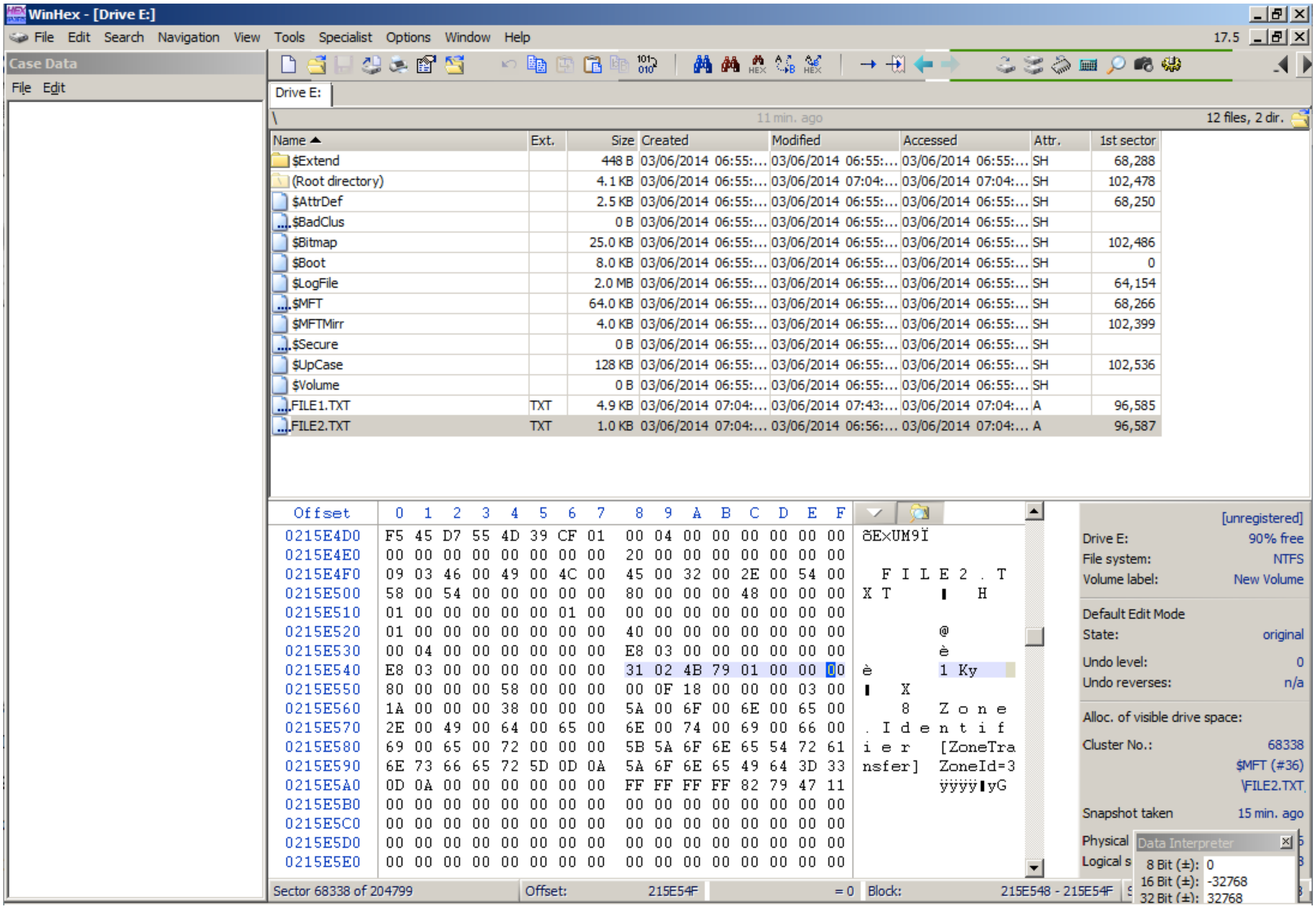
Alloc. of visible drive space:
Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

Snapshot taken 15 min. ago
Physical
Logical s

Data Interpreter
8 Bit (±): 0
16 Bit (±): -32768
32 Bit (±): 32768

Sector 68338 of 204799 Offset: 215E54F = 0 Block: 215E508 - 215E54F

The last eight bytes of this section contain the "Data Run", as highlighted below.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E4D0   F5 45 D7 55 4D 39 CF 01  00 04 00 00 00 00 00 00   õE×UM9Ï
0215E4E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E4F0   09 03 46 00 49 00 4C 00  45 00 32 00 2E 00 54 00     F I L E 2 . T
0215E500   58 00 54 00 00 00 00 00  80 00 00 00 48 00 00 00   X T     ▮   H
0215E510   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
0215E520   01 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00           @
0215E530   00 04 00 00 00 00 00 00  E8 03 00 00 00 00 00 00           è
0215E540   E8 03 00 00 00 00 00 00  31 02 4B 79 01 00 00 00   è       1 Ky
0215E550   80 00 00 00 58 00 00 00  00 0F 18 00 00 00 03 00   ▮   X
0215E560   1A 00 00 00 38 00 00 00  5A 00 6F 00 6E 00 65 00       8   Z o n e
0215E570   2E 00 49 00 64 00 65 00  6E 00 74 00 69 00 66 00   . I d e n t i f
0215E580   69 00 65 00 72 00 00 00  5B 5A 6F 6E 65 54 72 61   i e r   [ZoneTra
0215E590   6E 73 66 65 72 5D 0D 0A  5A 6F 6E 65 49 64 3D 33   nsfer]  ZoneId=3
0215E5A0   0D 0A 00 00 00 00 00 00  FF FF FF FF 82 79 47 11           ÿÿÿÿ▮yG
0215E5B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E5C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E5D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0215E5E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

```
Sector 68338 of 204799   Offset:   215E54F   = 0   Block:   215E548 - 215E54F
```

[unregistered]
Drive E: 90% free
File system: NTFS
Volume label: New Volume

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:
Cluster No.: 68338
$MFT (#36)
\FILE2.TXT

Snapshot taken 15 min. ago

8 Bit (±): 0
16 Bit (±): -32768
32 Bit (±): 32768

In this case, the Data Run is

```
31 02 4B 79 01
```

The first byte should be read as two individual hexadecimal values:

3: the last 3 bytes contain the starting cluster number

1: The first 1 byte contains the length of this portion of the file, in clusters.

So there are 2 clusters in a row here, at cluster # 4B 79 01.

The cluster # bytes are in "Little Endian" notation, so they must be reversed in order, resulting in Cluster number 01 79 4B.

This means 1x65536 + 7x4096+ 9x256 + 4x16 + 11 = 96587.

Look in the Directory Browser pane in WinHex, and you can see on the right side that FILE2.TXT does indeed start at that cluster number.

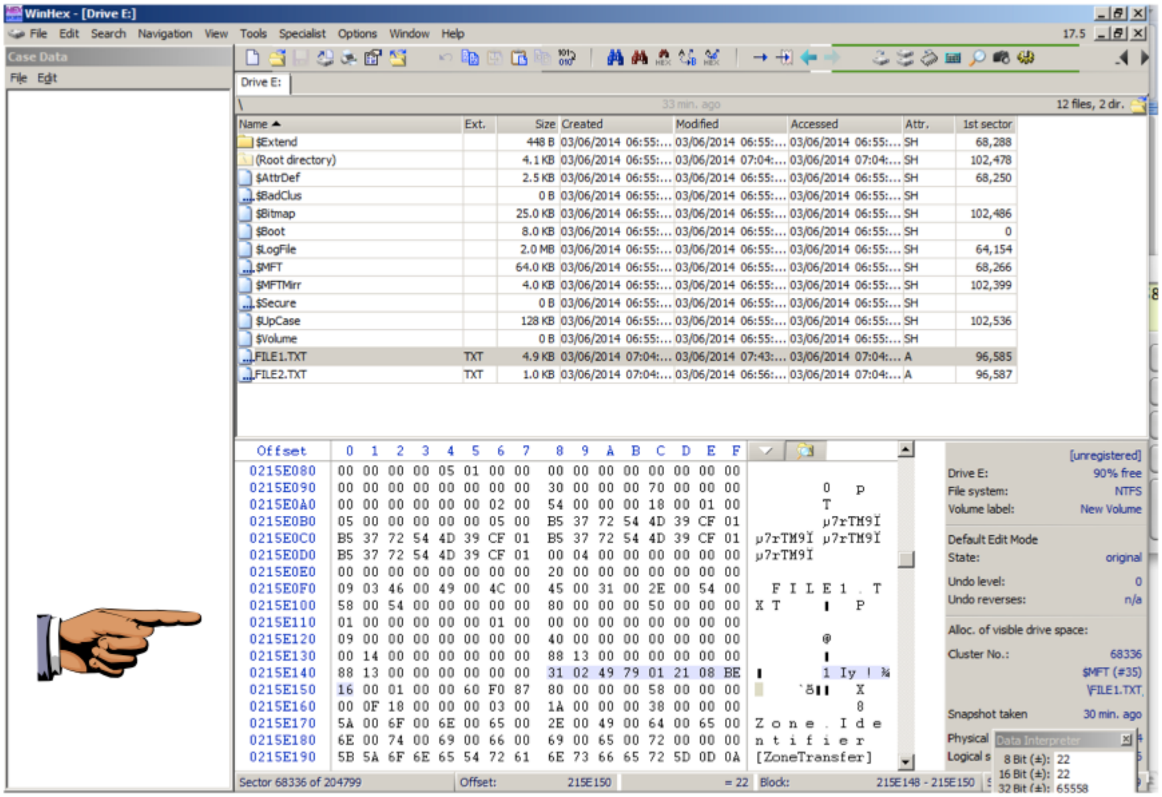
Data Run for FILE1.TXT

In the Directory Browser, right-click **FILE1.TXT**.

In the context menu, click **Navigation**, "**Go To FILE Record**".

Walk through the MFT record as you did before, to find the Data section and the File Run, which starts with 31, as shown below.

Highlight the Data Run, including eight bytes, as shown below.



Name ▲	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,288
(Root directory)		4.1 KB	03/06/2014 06:55:...	03/06/2014 07:04:...	03/06/2014 07:04:...	SH	102,478
$AttrDef		2.5 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,250
$BadClus		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$Bitmap		25.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,486
$Boot		8.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	0
$LogFile		2.0 MB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	64,154
$MFT		64.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	68,266
$MFTMirr		4.0 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,399
$Secure		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
$UpCase		128 KB	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	102,536
$Volume		0 B	03/06/2014 06:55:...	03/06/2014 06:55:...	03/06/2014 06:55:...	SH	
FILE1.TXT	TXT	4.9 KB	03/06/2014 07:04:...	03/06/2014 07:43:...	03/06/2014 07:04:...	A	96,585
FILE2.TXT	TXT	1.0 KB	03/06/2014 07:04:...	03/06/2014 06:56:...	03/06/2014 07:04:...	A	96,587

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0215E080   00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
0215E090   00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00          0   p
0215E0A0   00 00 00 00 00 00 02 00  54 00 00 00 18 00 01 00          T
0215E0B0   05 00 00 00 00 00 05 00  B5 37 72 54 4D 39 CF 01          µ7rTM9Ï
0215E0C0   B5 37 72 54 4D 39 CF 01  B5 37 72 54 4D 39 CF 01  µ7rTM9Ï µ7rTM9Ï
0215E0D0   B5 37 72 54 4D 39 CF 01  00 04 00 00 00 00 00 00  µ7rTM9Ï
0215E0E0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0215E0F0   09 03 46 00 49 00 4C 00  45 00 31 00 2E 00 54 00    F I L E 1 . T
0215E100   58 00 54 00 00 00 00 00  80 00 00 00 50 00 00 00  X T         P
0215E110   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
0215E120   09 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00          @
0215E130   00 14 00 00 00 00 00 00  88 13 00 00 00 00 00 00
0215E140   88 13 00 00 00 00 00 00  31 02 49 79 01 21 08 BE          1 Iy ! ¾
0215E150   16 00 01 00 00 60 F0 87  80 00 00 00 58 00 00 00       `ð      X
0215E160   00 0F 18 00 00 00 03 00  1A 00 00 00 38 00 00 00              8
0215E170   5A 00 6F 00 6E 00 65 00  2E 00 49 00 64 00 65 00  Z o n e . I d e
0215E180   6E 00 74 00 69 00 66 00  69 00 65 00 72 00 00 00  n t i f i e r
0215E190   5B 5A 6F 6E 65 54 72 61  6E 73 66 65 72 5D 0D 0A  [ZoneTransfer]
```

	[unregistered]
Drive E:	90% free
File system:	NTFS
Volume label:	New Volume
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	68336
	$MFT (#35)
	\FILE1.TXT
Snapshot taken	30 min. ago

Data Interpreter
8 Bit (±): 22
16 Bit (±): 22
32 Bit (±): 65558

Sector 68336 of 204799 Offset: 215E150 = 22 Block: 215E148 - 215E150

Saving a Screen Image

Make sure your screen shows eight highlighted bytes, with the first byte **31**.

Press the PrintScrn key in the upper-right portion of the keyboard. That will copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE TO GET FULL CREDIT!

Open Paint and paste in the image.

Save the image with the filename "**Your Name Proj 8b**". Use your real name, not the literal text "Your Name".

Turning in your Project

Email the image to me as an attachment to an e-mail message.

Send it to: **cnit.121@gmail.com** with a subject line of "**Proj 8 From Your Name**", replacing "Your Name" with your own first and last name.

Send a Cc to yourself.

Sources

http://www.epyxforensics.com/node/37

http://stam.blogs.com/8bits/2009/10/lab-ftk-imager-file-carving-using-the-mft-.html

http://grayscale-research.org/new/pdfs/NTFS%20forensics.pdf

Last modified: 3-6-14 8:21 am