EnCase exam screenshot showing a file's name in MFT (master file table) of the NTFS file system:

🕐 New 🚰 Open 🔛 Save 🎒 Print 🦢 Add I		able 🗇 Descut 🛄 Callana, 🖓 Timeline 🔿 Diala 🔶 C	- d -					
Cases		able 🔄 Report 📰 Gallery 🧭 Timeline 🖉 Disk 🥳 C	ode		cil- Al	ed.	ei-	1
🗠 Home 🎏 Entries 🔟 Bookmarks 🔍 Se (Name	Filter	Report	Ext	Type	Category	
👍 Home 😡 File Extents 🔒 Permissions 👍	54	SAM						
or 5- Entries	55	system						
	0.56	System There						
	00	L \$191F1						
	57	docucments and settings						
	58	🛅 \$Extend						
	59	Lost Files						
	60	Volume Slack						
⊕−D── ── Documents and Settings	Documents and Settings							
⊕-D Cownloads	01							
🖶 – D 🖂 🔂 Drivers								
률 🕞 🦳 HD-win2000-bkup								
FHD C Choli 1200								
Detpub Detpu								
Detpub Difference Diffe								
Inetpub Inetpub Inetpub Init init Ininit Init Init Init Init Init Init Inin	<	- THI						~
Inetpub Inetpub Initian I	Console	© Details □ Lock □ 0/171643		1 4 3	EnScripts	∛ Filters ((≘ Co	nditions 🐙 Queries	× *
	console	Details Lock 0/171643 0 00 00 00 18 00 01 00 E4 31 00 00	•-Z••••• <u>a1</u> •••	× •••	EnScripts	∀ Filters (t≘ Co	nditions 🥡 Queries	× * *
Textpub Textpub Textpub Textpub Maxtor9 MBACK622 MSOCache Text Hex Picture Report C S129986 00 00 00 00 2 15 81 02 AF	Console	Details □ Lock □ 0/171643 00 00 18 00 01 00 E4 31 00 00 00 00 12 AI 5 81 02 AF 52 C6 01 2A 15*.□.	• Z••••• šl•• Ræ• • • Ræ• •	× + **	EnScripts EnScripts	ず Filters [(≝ Co	nditions 🥥 Queries	× *
Text Hex Picture Report Text Hex Picture Report Text Area on the second of the second	Console 00 5A (52 C6 (02 AF 5	Details Lock 0/171643 00 00 18 00 10 Bt 4 31 00 00 01 2A 15 81 02 AF 52 C6 01 2A 15 51 02 AF 52 C6 01 00	••Z••••• <u>ä1</u> •• P£•••]•—R£•••		EnScripts EnScripts Exampl	▼ Filters ({≘ Co	nditions 🥡 Queries	× *
Text Text	Console 0 00 5A (52 C6 (02 AF 5 00 00 (Details Lock 0/171643 00 00 00 18 00 01 2A 15 81 02 AF 52 C6 01 2A 15 81 02 AF 52 C6 01 00	- Z äl RÆ - * - □ - RÆ - * . J - RÆ		EnScripts EnScripts Texample	☆ Filters 【(클 Co es	nditions 🤯 Queries	× * *
Text Text Maxtor9 MBACK622 MSOCache Text Hex Pcture Report C 0 0 00 00 00 00 00 00 00 S1 129930 81 02 AF 52 06 11 2A 15 81 S1212952 00 00 00 00 00 00 00 00 S12129574 53 00 54 00 45 00 4D 00 7E	Console 00 5A (52 C6 (02 AF 9 00 00 (00 32 (Details Lock 0/171643 00 00 12 15 0.1 12 15 81 02 AF 52 C6 01 2A 15 0.0 00	· Z· · · · ši· · PÆ- *- 0- PÆ- *- J- PÆ- · · · · · · - S· Y· - 2· . · D· L· L· n·		EnScripts EnScripts EXampi Include	∵ Filters (ł≣ Co es	nditions 🤯 Queries	
Textpub T	onsole 0 52 C6 (00 32 (00 00 (00 32 (00 00 (Image: Details Lock 0/171643 00 00 00 18 00 10 84 31 00 00 00 10 84 31 00 00 00 12 15 81 02 AF 52 C6 01 2A 15 52 C6 01 2A 15 00 </td <td>· Z · · · · · · <u>ä</u>l · · · - RZ · · · · · · RZ · · · · · - RZ · · · · · · · · · · · · · · · · · · ·</td> <td></td> <td>EnScripts EnScripts EXampi Tinclude</td> <td>¶ Filters [t≘ Co es</td> <td>nditions 🥡 Queries</td> <td>> </td>	· Z · · · · · · <u>ä</u> l · · · - RZ · · · · · · RZ · · · · · - RZ · · · · · · · · · · · · · · · · · · ·		EnScripts EnScripts EXampi Tinclude	¶ Filters [t≘ Co es	nditions 🥡 Queries	>
Text I Hex I Picture Report C C C C C C C C C C C C C C C C C	console i 00 5A 0 52 C6 0 00 00 00 00 00 00 00 32 0 00 00 0 00 00 0 15 81 0	Image: Control of the state of the	• Z • • • • • • • • • • • • • • • • • •		EnScripts EnScripts	₹Filters (t≣ Co es File n	nditions @Queries	× > ₹4►
Text Text	Console 00 5A 0 52 C6 0 00 3Z 0 00 00 0 00 00 0 00 00 0 15 81 0 00 00 0	Details Lock 0/171643 00 00 00 18 00 00 00 12 15 20 00 00 18 00 01 00 12 15 102 AF 52 C6 12 15 100 00	· Z · · · · · · · · · · · · · · · · · ·		EnScripts EnScripts	₹Filters (ﷺ Co es File n	nditions @Queries	₩
Text Text	Console 0 00 5A (52 C6 (02 AF 5 00 00 (00 32 (00 00 (00 00 (15 81 (00 00 (00 00 (Image Image <th< td=""><td>- Zšil - RgS.Y. - Rg - S.Y. - 2D.L.L.n. </td><td></td><td>EnScripts EnScripts Exampi Include</td><td>₹^{Filters} (ﷺ Co es File n</td><td>nditions @Queries ame in</td><td>× * *</td></th<>	- Zšil - RgS.Y. - Rg - S.Y. - 2D.L.L.n. 		EnScripts EnScripts Exampi Include	₹ ^{Filters} (ﷺ Co es File n	nditions @Queries ame in	× * *
Text Text	Console 0 00 5A (52 C6 (02 AF 3 00 00 (00 32 (00 00 (00 00 (00 00 (00 00 (00 00 (00 00 (00 0 0 (00 0 73 (00 0 73 (Details Lock 0/171643 00 00 18 00 10 84 31 00 00 12 12 15 81 02 AF 52 C6 01 2A 15 1	Zši. - RE. *. 0 RE. *. RE. - S.Y. - 2D.L.L.n. *. 0 RE. *. 0 R		EnScripts EnScripts	^{™ Filters} (ﷺ ^{Co} es File n Unico	nditions @Queries ame in de:	×
Text Hex MBACK622 MAxtor9 MBACK622 MSOCache Text Hex Picture Report X X	Console 00 5A (52 C6 (00 00 (00 67 (0)	Image: Constraint of the state of	- Z		EnScripts EnScripts Exampl	₹Filers (t≅ Co es File n Unico	nditions @Queries ame in de:	× * *
Text Hex Hex Polute Text Hex Polute Report Text Hex Polute Report Text Hex Polute Report Text Hex Polute Report Text Text	console 0 00 SA 0 52 C6 0 02 AF 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 67 0 00 00 0	Image: Constraint of the state of	· Z · · · · · · · · · · · · · · · · · ·		EnScripts EnScripts Exampl	₹ ^{Filters} (ﷺ co es File n Unico "Syste	nditions @Queries ame in de: am Dra	
Text Text	Console 0 00 5A (52 C6 (00 02 AF 3 00 00 (00 00 (00 00 (00 07 (00 07 (00 07 (00 07 (00 07 (00 00 (00 0 00 (00 0 0 (00 0 (0 0 (00 0 (0 0	Image: Second	· Z · · · · · · · · · · · · · · · · · ·		EnScripts EnScripts Example	₹ ^{Filters} (ﷺ co es File n Unico "Syste	nditions @Queries ame in de: em.Dra	awir
	Console 00 5A (52 C6 (00 3Z (00 00 (00 00 (00 00 (00 67 (00 67 (00 67 (00 67 (00 60 (00 00 (00 0 (0 0 (Image: Second	-Zail -RE.+RE.+ -RE -Y		EnScripts EnScripts Exampl	₹ File n Unico "Syste	nditions @Queries ame in de: em.Dra	awir
Text Hex Hex Hex Picture Report MSOCache MSOCache MSOCache MSOCache MSOCache Text Hex Picture Report Text Text Text Hex Picture Report Text	Console Consol	Image: Second	- Z		EnScripts EnScripts Exampl	^{☞ Filers} (ﷺ co es File n Unico "Syste Desig	nditions @Queries ame in de: em.Dra n.dll"	awir

Number system:

- <u>decimal system</u>: e.g., $123 = 1 * 10^2 + 2 * 10^1 + 3 * 10^0$
- <u>binary system</u>: e.g., $1101 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 13$ (in decimal)
- <u>hexadecimal system</u>: a base-16 system as an abbreviation for binary system by grouping 4 bits into a hex digit (0 - 9, A - F), e.g., $4C2E = 4*16^3 + 12*16^2 + 2*16^1 + 14*16^0 = 19502$ (in decimal, converted using Windows calculator pad)

	PowerPoint - ESCompliterFollingations in	
	Calculator	
	Edit View Help	
		422E
	⊙ Hex ODec OOct OBin OQu	vord O Dword O Word O Byte (2) Enter hex value
(1) Check	Inv Hyp	Backspace CE C
hex	SF FE () MC (8 9 / Mod And
	Ave dms Exp In MR 4	5 6 * Or Xor
(3)	Sum sin x^y log MS 1	2 3 - Lsh Not
Convert to	s cos x^3 n! M+ C	+/ + = Int
decimal	Dat tan x^2 1/x pi 4	

Example. An IDE hard disk of size 60 GB (i.e., 60 billion bytes), which has a single partition of size 57207.9 MB (Megabytes). Why is the difference in size? **Answer**: 1 KB = 1,024 bytes = 2^{10} bytes; 1 MB = 2^{20} bytes = 1048576 bytes. Thus, 57207.9 * 1048576 = 59986830950.4 \approx 60 billion bytes

Representing negative numbers:

• Two common ways of representing negative numbers are <u>sign-</u> <u>magnitude representation</u> and <u>two's-complement</u> notation.

Note: Computers generally use two's-complement notation.

- Sign-magnitude sets the first bit to 1 if it is a negative number (the first bit, then, is not part of the quantity).
- Two's Complement inverts all of the bits and then adds one.

An example of binary arithmetic:

0000 1101 (13 in decimal) 1000 1101 (-13 in signed-magnitude notation)

```
1111 0010 (invert 0's and 1's for 13)
1111 0011 (2's complement representation of -13)
(note that -(-13) = 13, in both representations)
```

Subtraction works by adding the two's complement of a number (and ignore carry out of the most significant place):

```
25 0001 1001
-13 + 1111 0011
12 10000 1100
ignored
```

Organization of Multiple-Byte Non-Negative Numbers:

- Numbers larger than 255 require more than 1 byte to represent. Common sizes are 1-byte, 2-bytes (16-bit), 4-bytes (32-bit), and 8-bytes (64-bit).
- Consider the number 954 :

 $954 = 0000\ 0011\ 1000\ 1010\ (using\ 16\ bits) = 0x03BA\ (in hexadecimal), with the high (more significant) byte 03 and low byte BA,$

 \succ in Big Endian notation, 03 BA (high byte 03 first, then BA), as in Motorola processors, Sun Solaris, and IBM mainframe computers

➤ in Little Endian, BA 03 (low byte first in the lower address), as in Intel processors.