IMPORTANT: Please disable your windows defender or Anti-Malware software before conducting this exercise as they will determine the files as malware. I recommend you to create a Windows VM and do this exercise in it like I did in class.

1. This exercise will walk you through the IDA pro demo. First, download the zip file named '469\_malware\_demo.zip'

2. The file contains 4 binaries --- 469, PEiD, upx, and installer for IDA pro 5.

As I demonstrated in class, PEiD is used to read signatures in PE files and to determine whether the file is obfuscated using a packer.

3. '469.exe' is a program with encrypted criminal's bank account information. It is your job to retrieve them.

Let's first run it and see what it does.

	Win	17 [Running] - Oracle VM Virtua	lBox				
						- F	<b>X</b>
😋 💽 🗢 퉬 « Users 🕨	sefcom ► Downloads ► Malw	are_demo	<b>- - - + + + + + + + + + +</b>	Search Malv	vare_demo		٩
Organize 👻 🛛 Include i	n library 👻 Share with 👻	New folder			:== :==	-	0
🔆 Favorites	Name	Date	modified	Туре	Size		
🥅 Desktop	<b>469</b>	4/2/	2019 10:42 PM	Application		7 KB	
鷆 Downloads	🔛 PEiD	4/2/	919 10:42 PM	Application		214 KB	
🖳 Recent Places	💷 upx	4/2/	2019 10:42 PM	Application		277 KB	
□ Doc       □ C: \Users\:         □ Mu       □ Vid         □ Pict       □ Directory         □ Vid       □ Directory         □ Vid       □ Pict         □ Vid       □ Pict         □ Vid       □ Pict         □ Vid       □ 04/02/2011         □ 4/02/2011       □ 04/02/2011         □ Alter       □ C: \Users\:         □ Pict       □ C: \Users\:         □ Pict       □ C: \Users\:         □ Pict       □ Pict         □ Pict       □ 04/02/2011         □ Pict       □ 04/02/2011	Weisylenb2(cmlaxe sefcom\Downloads\Malwar h drive C has no label. srial Number is B41B-E6 y of C:\Users\sefcom\Do ) 10:45 PM	e_demo>dir D4 wnloads\Malware_ - 7,168 469.exe 19,136 PEiD.exe 83,648 upx.exe 509,952 bytes 075,840 bytes fr e_demo>469.exe e_demo>469.exe e_demo>	.demo ree				

I tried two different passwords, 'hello' and 'openSesame', but they are both wrong passwords.

4. Before we disassemble the executable and reveal the hidden information, let's use PEiD to check the file.

organize • 🔄 oper	Name		Date modified	Type	Size		
<ul> <li>Favorites</li> <li>Desktop</li> <li>Downloads</li> <li>Recent Places</li> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> </ul>	ei 469 We PEiD ei upx	File:       C:\Users\sefcom\Down         Entrypoint:       00006A10         File Offset:       00000E10         Linker Info:       10.0	nloads\Malware_demo\4 EP Se First E Subsy	ction: UPX1 sytes: 60,8E,00,60 rstem: Win32 console		5 KB 214 KB 277 KB	
Videos		Multi Scan Task Viewe	r Options	About Ex	it		

5. Unlike the unpacked binary (i.e., '.text' or '.rdata'), the EP Section indicates that it is packed by a program called **UPX**. It is a well-known packer for PE files that uses compression.

Let's unpack it using the 'upx.exe' included in the folder.



6. Finally, disassemble the binary using IDA pro. Install IDA Pro using the installer included, or you can download the latest free version of IDA Pro from https://www.hex-rays.com/products/ida/



The interactive disassembler	
File Edit Jump Search View Debugger Options Windows Help	
😂 🖬   ← ▾ → ▾   🏘 🍓   Փ   Ͻ   Text 🚽 🔽 🔽 🔽 🔽 🚽	2 ==
] 🖹 📾 ♠ ] 📓 🗛   ½ 💥 🏔 🚑 🖌 🗖 👘 🛤 🗎 🐚 🐨 ] 🗣 🎞 📔 🖿 📑 🚟 📲	
<u> 改 En</u> 800 801 121 181 ▼ * N × 911 ▼ # ▼ 'x' S H K /→ ~ / : ; 燕 學 Ц h L 聶 燕 撃	<b>盘</b> 蒸
📰 🖻 🗢 🛛 🕾 🗟 🦷 New disassembly database	
PDAs/Handhelds/Phones Consoles Embedded Various files	
Windows DOS Unix Mac Java .NET Various OS's	
Library Activ Device Driver Object File	
COFF/DMF Static Library	
UK Cancel	
Auto Down Disk	

7. When it starts, select 'PE Executables' from the options under the 'Windows' tab as shown in the picture above.

Unless you want certain options only, run the analysis by clicking 'Next' buttons.

IDA - C:\Users\sefcom\Downloads\469-Malware\469-Malware\469.exe	
ile Edit Jump Search View Debugger Options Windows Help	
🚘 🖬 │ ← ▼ → ▼ │ 🏘 🍇 │ 🚯 │ 1 │ Text 🔹 🔹 │ 🖉 │ =	+× 680(₽≡
🖹 🖼 🔷   📓 🗛   🥨 💥 🏡 🥔 🥓 🎟 🛛 🛛 🏚 📾 🖪 🍖 🐨   🐢 🔽	- 🖹 🗏 🐂
🐧 En   0001 0001 0001 0001 "s" ▼ ★ N 🗙   955 ▼ ₩ ▼ 'x' S H K /→ ~ Ø   = ; क़ 學	ᄔᅆᇄ 🛛 🚠 🏯 🛣 🏯
🖹 IDA View-A 🔛 Hex View-A   🖽 Exports   🕮 Imports   N Names   🖅 Functions   "" Strings   🔉 Structures	En Enums
Find the start and the start a	Name
100.00% /26.41) /461.145) 000007C0 004012C0.+5+	Graph overview 🛛
ompiling file 'C:\Program Files\IDA Free\idc\ida.idc' xecuting function 'main' ompiling file 'C:\Program Files\IDA Free\idc\onload.idc' pais analysing the input file DA is analysing the input file ou may start to explore the input file right now. an not set debug privilege! ropagating type information unction argument information is propagated he initial autoanalysis has been finished. U: idle Down Disk:40GB	

8. You will see a screen like the picture above.

You can see various items from each window. For example:

**Names window**: lists all known named locations in the program. F is a function, C is code/instruction, A is a string, D is defined data, etc.

Strings window: lists a list of embedded strings in the program.

**IDA View Window**: is a disassembly window that shows the program in assembly. It supports graphical view and text view modes. You can toggle between the two modes using the Space key.

Hex View Window: dumps the binary into hex.

Move to the beginning of the program by clicking the leftmost blue portion of the bar indicated in the picture above.

```
45
var CC= dword ptr -OCCh
var_4= dword ptr -4
push
       ebp
mov
       ebp, esp
       esp, OCCh
sub
       eax, dword 403000
mov
xor
       eax, ebp
mov
       [ebp+var 4], eax
push
       esi
mov
       esi, ds:printf
       offset aPleaseInputPas ; "Please input password:\n"
push
call
       esi ; printf
       eax, [ebp+var_CC]
lea
push
       eax
                      ; "%s"
       offset aS
push
call
       ds:scanf
       esp, OCh
add
       ecx, offset a Ftere ; "^&) {)+fTERE"
mov
(004) (0052 010)
```

9. You can see the first few instructions of the program.

As you can see the plain text "Please input password:\n" stored in the variable "aPleaseInputPas" from the picture, this part of the program is the portion simply loads the program to the stack and asks the user for a password.

Assembly instruction shown by IDA pro follows "intel" syntax:

<instruction> <dst>, <src>: <instruction> is an operator, while <dst> and <src> are operands.

(e.g.) **mov ebp, esp**: move the value (or address) stored in current stack pointer (esp) to base pointer (ebp).

Both esp and ebp are *registers*. Registers are tiny, internal memory of CPU. CPU utilizes registers to speed up the operations, instead of obtaining data from external memory through the control bus.

(e.g.) **cmp eax, [ebp + var]**: compare the value of [ebp + var] (the value of 'var' added to that of 'ebp) and the value of eax (accumulator register, which is used in arithmetic operation).

Another example is:

Following C code:

```
int x = 1;
int y = 2;
if(x == y) {
    printf("x equals y.\n");
}else{
    printf("x is not equal to y.\n");
}
```

Can be disassembled as follows:

00401006 0040100D 00401014	mov mov	<pre>[ebp+var_4], 1 [ebp+var_8], 2 eax. [ebp+var_4]</pre>	
00401017	cmp	eax, [ebp+var_8]	; if x=y, the cmp will set the ZF to 1
0040101A	jnz	short loc_40102B	; jump if ZF not set (if x!=y)
0040101C	push	offset aXEqualsY_	; "x equals y.\n"
00401021	call	printf	
00401026	add	esp, 4	
00401029	jmp	short loc_401038	
0040102B	loc_40102B:		
0040102B	push	offset aXIsNotEqualToY	; "x is not equal to y.\n"
00401030	call	printf	

For more tutorials on assembly and IDA pro, please refer to the following links:

http://www-

verimag.imag.fr/~mounier/Enseignement/Software\_Security/BH\_Eagle\_ida\_pro.pdf

https://www.felixcloutier.com/x86/

https://www.tutorialspoint.com/assembly\_programming/index.htm

Please stop following the instructions of this document and play around with IDA pro and try to understand the assembly and have fun (3)



9. If you scroll down the assembly view window, you will find the branch that determines which location of the program the control should jump to. It is determined by the two lines in the top box --- "**test** eax, eax" and '**jnz** short loc 4010C2".

	Loc_401066	: x, eax iort loc_4010C2
	*	
mov eax, offs	et aKmmy ; "Kmmy"	
call sub_4010E mov eax, offs	ប et aNknoW ; "Nkno*W"	push offset aWrongPassword h"
call sub_4010E	0 at ablenabl 0 : "blenash"	call esi; printf
call sub_4010E	0	add esp, 4

10. jnz instruction means "*jump if not zero*". If the *Zero Flag (ZF)* is set to zero, it jumps to the left block, which prints the hidden information, while the block on the right prints out "Wrong password" and exits the program as we saw earlier.

Click or select the instruction "jnz" and it will show the byte offset and the hex code of the instruction in the "Hex View" window.

💮 IDA	- C:\	Jsers	sefo	:om\	Dow	nloa	ds\4	69-N	1alw	are\4	I69-Ⅳ	1alwai	re\46	9.exe	e - [H	ex V	iew-A	A]		
File	Edi	t Ju	imp	Se	arch	Vi	ew	Deb	ugg	er	Optic	ons	Wind	lows	H	elp				_ B ×
🗃 🕻	3	÷ -				i M		<b> </b>	<b>%</b>	ļ	Te:	xt				-	75			-   🌽   - + ×   6 8 0   2 =
	si 🔶			<u>م</u>	100	ж.	Α	<b>a</b>	×					<b>1</b> 1	s.	N	<b>*</b> []	nn	-	
Å E	<b>n</b>     ;	0101 0 COD D	101 0 AT 2	Ŝ <sup>1</sup>	"s" 🔻	- 36	N	$\times$		Off dat	- #	<del>ب</del> »	2 5	5 H	ГК		į ~	8		:; 赤翠 山屿 晶燕寶蟲素
	8) <b>(</b> )	l é	7 9	<b>R</b> 9	3	F	ĥ	Æ												
		1.		•																
D/	4 View	A	а н	lex V	′iew-∆	- 1	۵E>	ports		š Im	ports	N	Name	s N	🗿 Fu	Ini				gs 🔏 Structures En Enums
.text	:004	01 02	0	Dő	8D	85	34	FF	FF	FF	50	68	E8	20	40	.d ឲម	ata:U	15	A4	+ìà4 PhF@.§ñ 🔺
.text	:004	01 03	0	20	40	00	83	C4	0C	B9	ΕØ	30	40	90	8D	85	34	FF	FF	@.â-∎¦a0@.ìà4
.text	:004	0104	0	FF	<b>8</b> A	10	3A	11	75	18	84	D2	74	12	<b>8</b> A	50	01	3A	51	è∔:∢u→ä-tièP :Q
.text	: 004	01 05	0	U1	75	UE	83	CU	02	83	C1		84	D2	75	E4	33	CU	EB	ula+1a-1a-n23+q
.text	: 004	<b>UT UC</b>	0	05	18	00	83	08	FF	85	00	15	28	88	F 8	31	40	50	E8	++a+ a+ UN+*10.F
.text	. 004	0107 0400	0	00	00	00	00	88	60	32	40	00	18	02	00	00	00	88	88	1++2@.FD+e
.text	. 004	9193 0400	10	33	40	40	Eð	20	60	00	00	88	20	34	40	60	Eð	4E	00	30.FA+F40.FN.
.text	.004	0109 0400	0	40	00	99	F 8	31	40	00	FF ZO	50	00	60	32	40	00	69	DO Ch	@. +  +2@. + bô90
.text	. 004	9 I 98 94 90	10	10	99	00	40	00		EC	99	20	54	40	00	66	00	00	54	194^2Mp9_Ep %c
toyt	- 004	0 1 00 0 1 0 C	0	ED	60	60	EC	20	1.0	60	EE	00	00	100	EC	00	C.h.	60	22	
toyt	- 004	0 1 00 0 1 00	10	20	22	00	55	20	69		66		00	55	ED	60	0.4	04	00	
tovt	- 004	0 1 0D 0 1 0E	0	50	RÓ	28	00	00	00	80	JLΩ	FF	9D 9J	60	7.5	86	80	FQ	80	01 AH 3+t_CT
tovt	- 004	01 OF	0	22	70	FF	80	0.2	84	CO	7.5	85	80	FO	80	22	0.0	80	JIQ	ан <u>алс-у</u> т ан <u>алс-у</u> т
tovt	- 004	0110	10	Q-1	81	60	7.5	86	20	FO	80	88	78	Q-1	80	1.8	62	<u>ө</u> л	C0	S+t_CT6H_6H_S+
text	. 004	0111	ß	74	86	80	FQ	86	88	48	62	80	40	03	84	60	74	86	80	t_CTÊH_ÈHLÄ+t_C
text	- 004	0112	a	FO	80	88	18	03	83	CO	85	40	75	RR	63	38	an	66	30	
text	: 004	0113	ด	40	66	75	62	F3	63	FO	98	62	<b>6</b> 6	66	68	<b>ØF</b>	16	40	66	a.u.=+Tiihe.a.
		0110				•••		•••												
•											111									4
0000046	8	00401	068:	sub	401	000+	68													
Compil	ing	file	'C	: \ P	roar	am I	Eile		DA P	ree	-\ide	\ida	. ide							
All idle		Do	wn	Diel	- 400	SB														
Ao. Ture	-	- 00	witt	D/151	. 400	10			_		10					10			r	

11. Assembly Window and Hex View Window are by default synced, so the instruction you selected in the Assembly Window should be highlighted in the Hex View Window, along with the byte offset in hex of the selected instruction at the bottom left corner (see the picture above).

The hex code for assembly 'jnz' is **75**.

Let's change it to "**nop**" instruction (**No Operation**) so it never jump to the part printing out "Wrong password".

$\leftrightarrow$	C 🕜	🛈 🔒 ht	tps://hexed.it							• ©	0 T	3			$\overline{\mathbf{A}}$	lii\	₫	כ	≡
New file	Open file	C Reload	Export	Und	0			A Redo			> Too	<b>\$</b> ols		s	<b>¢</b> etting	s		He	<b>?</b> ⊧lp
ent Address	0x00000469	Memo	-Untitled- 🗙	469.	exe	×													
Address	OWOODOT BEE		0000042	D6	8D	85	34	FF	FF	FF	50	68	E8	20	40	00	FF	15	A4
- duices	0.450		00000430	20	40	00	83	C4	0C	<b>B</b> 9	E0	30	40	00	8D	85	34	FF	FF
D	0X468		00000440	FF	8A	10	3A	11	75	1A	84	D2	74	12	8A	50	01	ЗA	51
	Search		: 00000450	01	75	ΘE	83	CO	02	83	Cl	02	84	D2	75	E4	33	C0	EB
			00000460	05	1B	CO	83	D8	FF	85	CÐ	90	. 8	B8	F8	31	40	00	E8
ch for	CB		00000470	6C	00	00	00	<b>B</b> 8	CO	32	40	00	28	62	00	00	00	<b>B8</b>	88
Туре	✓ 8-bit Integer		00000480	33	40	00	E8	58	00	00	00	<b>B</b> 8	50	34	40	00	E8	4E	00
	16 hit Integer		00000490	00	00	68	F8	31	40	00	FF	D6	68	CO	32	40	00	FF	D6
	V To-bit Integer		000004A0	68	88	33	40	00	FF	D6	68	50	34	40	00	FF	D6	83	C4
	✓ 24-bit Integer		000004B0	10	33	CO	5E	8B	4D	FC	33	CD	E8	6E	00	00	00	8B	E5
	✓ 32-bit Integer		000004C0	5D	C3	68	EC	20	40	00	FF	D6	8B	4D	FC	83	C4	04	33
	. 64-bit Integer		000004D0	CD	33	CO	5E	E8	53	00	00	00	8B	E5	5D	C3	CC	cc	CC
	v of bit integer		000004E0	40	BA	28	00	00	00	8A	48	FF	84	C9	74	06	80	E9	ΘA
	16-bit Floating	g Point	000004F0	88	48	FF	8A	08	84	C9	74	05	80	E9	ΘA	88	08	8A	48
	32-bit Floating	g Point	00000500	01	84	C9	74	06	80	E9	ΘA	88	48	01	8A	48	02	84	C9
	64-bit Floating	Point	00000510	74	06	80	E9	ΘA	88	48	02	8A	48	03	84	C9	74	06	80
			00000520	E9	ΘA	88	48	03	83	CO	05	4A	75	BB	C3	3B	OD	00	30
	<ul> <li>Hexadecimal</li> </ul>	values	00000530	40	00	75	02	F.3	C.3	F9	98	02	00	00	68	ΘF	16	40	00
hexed.it: Clos	e												_						

12. Open the "469.exe" in <u>https://hexed.it</u> to modify. Change the instruction code of "jnz" (75) at byte offset 0x468 to "nop" (**90**).

Organize        Open       Include in library        Share with        New folder       BIE        Image: Control of the state o		🗼 « Local Di	sk (C:) ▶ Users ▶ sef	com 🕨 De	ownloads 🕨	-	<b>4</b> 9	Search Down	loads			53
Year       Name       Date modified       Type       Size         Desktop       # 469-Malware       4/2/2019 11:19 AM       File folder         Downloads       demend:22:x86       A/1 (2010 6:16 DM       File folder         Dade Murphy 1/1/2012 \$5000       \$0       \$5000       \$3500         Dade Murphy 1/1/2012 \$5000       \$0       \$5000       \$         Dade Murphy 1/1/2012 \$0       \$5000       \$3500       \$         C:\Users\sefcom\Downloads>469.       'tops: is not recognized as an internal or external command, onerable, program or hatch file.       \$         C:\Users\sefcom\Downloads>469.exe       Please input password:       \$       \$         Dade Murphy 1/1/2012 \$5000       \$       \$       \$         Mccount       Date       Credit Debit       Balance         Account       Date	Organize 🔻	- 🔚 Oper	n Include in library	▼ Sh	are with 🔻	New folder			3	= <b>-</b>		•
Desktop       469-Malware       4/2/2019 11:19 AM       File folder         Mumploadt       demendr22 x85       4/1/2010 6:16 DM       Eile folder         Mumploadt       File folder       File folder         Mumploat       File folder       File folder         Mumploat       File folder       File folder         Mumploat       File folder       File folder         File folder       File folder       File folder	🔆 Favorit	tes	Name	~		Date modifie	ed	Туре		Size		
Councleads   C:\Windows\system32\cmd.exe   Dade Murphy 1/2/2012 \$5000 \$0   Dade Murphy 1/2/2012 \$0   Dade Murphy 1/2/2012 \$0   Dade Murphy 1/2/2012 \$0   Stop   C:\Users\sefcom\Downloads>469.   '469.'   I:   C:\Users\sefcom\Downloads>469.exe   Please input password:   hello   Account   Dade Murphy 1/2/2012 \$5000 \$0   Stop   Dade Murphy 1/2/2012 \$5000 \$0   Stop   I:   C:\Users\sefcom\Downloads>469.exe   Please input password:   hello   Dade Murphy 1/2/2012 \$5000 \$0   Stop   Dade Murphy 1/2/2012 \$5000 \$0   Stop   I:   C:   Users\sefcom\Downloads>469.exe   Please input password:   hello   Dade Murphy 1/2/2012 \$5000 \$0   Stop   Dade Murphy 1/2/2012 \$5000 \$0   Stop   Stop   Bade Murphy 1/2/2012 \$5000 \$0   Stop   Bade Murphy 1/2/2012 \$5000 \$0   Stop   Bade Murphy 1/2/2012 \$5000 \$0   Stop   Balance   Dade Murphy 1/2/2012 \$5000 \$0   Stop   Balance   Balance   C:   Users\sefcom\Downloads>469.exe   Please input password:   Bade Murphy 1/2/2012 \$5000 \$0   Balance   Account   Dade Murphy 1/2/2012 \$5000 \$0   Bade Murphy 1/2/2012 \$5000 \$0   Bade	Deskt	top	469-Malware			4/2/2019 11:	19 AM	File folder				
Dade Murphy 1/1/2012 \$5000 \$0 \$5000   Dade Murphy 1/2/2012 \$0 \$1000 \$4000   Dade Murphy 1/2/2012 \$0 \$5000 \$3500   Dade Murphy 1/4/2012 \$0 \$5000 \$3500   C:\Users\sefcom\Downloads>469.   '469.' is not recognized as an internal or external command,   onerable nrogram or batch file.   C:\Users\sefcom\Downloads>469.exe   Please input password:   hello   Account Date Credit Debit Balance   Dade Murphy 1/2/2012 \$0   Dade Murphy 1/2/2012 \$0   \$1000 \$4000   Dade Murphy 1/2/2012 \$0   Stone   C:\Users\sefcom\Downloads>469.exe   Please input password:   hello   Account Date Credit Debit Balance   Dade Murphy 1/2/2012 \$0   Stone   C:\Users\sefcom\Downloads>469.exe   Please input password:   openSesame   Account Date Credit Debit Balance   Dade Murphy 1/2/2012 \$0   Stone   Stone   Account Date Credit Debit Balance   Dade Murphy 1/2/2012 \$0   Stone   Bade Murphy 1/2		nloads C:\Windows\	system32\cmd.exe			4/1/2019 6-1	5 DM	File folder				
<pre>/469.' is not recognized as an internal or external command, onerable program or batch file. C:\Users\sefcom\Downloads&gt;469.exe Please input password: hello Account Date Credit Debit Balance Dade Murphy 1/1/2012 \$5000 \$0 Dade Murphy 1/2/2012 \$0 Please input password: openSesame Account Date Credit Debit Balance Please input password: openSesame Account Date Credit Debit Balance Dade Murphy 1/1/2012 \$5000 \$0 Dade Murphy 1/1/2012 \$5000 \$0 Source State Credit Debit Balance Account Date Murphy 1/2/2012 \$0 S1000 \$4000 Bade Murphy 1/4/2012 \$0 S1000 \$4000 Bade Murphy 1/4</pre>	Da Da Da Da Da Ca	ade Murphy ade Murphy ade Murphy :\Users\se	1/1/2012 \$5000 1/2/2012 \$0 1/4/2012 \$0 fcom\Downloads>4	\$0 \$1000 \$500	\$5000 \$4000 \$3500	×						
Image: C:\Users\sefcom\Downloads>469.exe       KB         Image: Please input password:       KB         hello       Account Date Credit Debit Balance       KB         Dade Murphy 1/1/2012 \$5000 \$0       \$5000       KB         Dade Murphy 1/2/2012 \$0       \$1000 \$4000       KB         Dade Murphy 1/4/2012 \$0       \$500       KB         Image: C:\Users\sefcom\Downloads>469.exe       KB         Please input password:       KB         openSesame       Account Date Credit Debit Balance         Account Date Credit Debit Balance       KB         Dade Murphy 1/1/2012 \$5000 \$0       \$500         Dade Murphy 1/2/2012 \$0       \$1000 \$4000         C:\Users\sefcom\Downloads>       KB	J 1	469.' is n	ot recognized as	an int	ernal or	external com	mand,				KE	3
hello       Account       Date       Credit       Debit       Balance       \$5000       \$5000       \$5000       \$6000       \$5000       \$6000       \$5000       \$60000       \$6000       \$6000		:\Users\se: lease inpu	fcom\Downloads>4 t_password:	69.exe							KE	3   B
Co       Dade Hurphy 1/1/2012 \$0       \$1000       \$4000       \$4000       \$4000         Dade Hurphy 1/2/2012 \$0       \$1000       \$3500       \$600       \$4000       \$600         Dade Murphy 1/2/2012 \$0       \$500       \$3500       \$600       \$600       \$600       \$600         Ne       C:\Users\sefcom\Downloads>469.exe       \$600       \$5000       \$600 <th>he Ac</th> <td>ello ccount</td> <td>Date Credit</td> <td>Debit</td> <td>Balance</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>KE</td> <td>в</td>	he Ac	ello ccount	Date Credit	Debit	Balance						KE	в
Image: Second Down Loads > 469.exe       KB         Please input password:       KB         openSesame       KB         Account       Date         Credit Debit       Balance         Dade Murphy 1/1/2012       \$5000         Dade Murphy 1/2/2012       \$1000         State       \$3500         C:\Users\sefcom\DownLoads>	Co Da Da	ade Murphy ade Murphy ade Murphy	1/1/2012 \$5000 1/2/2012 \$0 1/4/2012 \$0	\$1000 \$500	\$4000 \$3500 \$3500						KE	3 R
Piease input password:       KB         openSesame       Account       Date       Credit       Debit       Balance       KB         Dade Murphy 1/1/2012 \$5000       \$0       \$5000       \$600       KB       KB         Dade Murphy 1/2/2012 \$0       \$1000       \$4000       KB       KB         C:\Users\sefcom\Downloads>       KB       KB       KB	🗣 Ne 😋	Users\se	fcom\Downloads>4	69.exe							KE	в
Dade Murphy 1/1/2012 \$5000 \$0 \$5000         \$60 \$5000 <td< th=""><th></th><th>rease inpu penSesame ccount</th><th>t password: Date Credit</th><th>Debit</th><th>Balance</th><th></th><th></th><th></th><th></th><th></th><th>KE</th><th>3</th></td<>		rease inpu penSesame ccount	t password: Date Credit	Debit	Balance						KE	3
C:\Users\sefcom\Downloads>	Da Da	ade Murphy ade Murphy	1/1/2012 \$5000 1/2/2012 \$0	\$0 \$1000	\$5000 \$4000						KE	8
	Da C:	NUsers\se	1/4/2012 \$0	\$500	\$3500						+ KE	в
				1 4 (1 (201	0.6.10.014						KE	3

13. Download the modified program and run it.

I used the same passwords ("hello" and "openSesame") again and the program shows me the account information!

There are at least two more ways to get the hidden information by modifying the binary:

- 1. You can change the very first instruction of the program to jump to the location of the hidden information so the program does not even ask you for the password.
- 2. Change the "cmp" instructions that checks the password to "nop" so the program does not check the password.

Please try various methods to achieve the same goal.