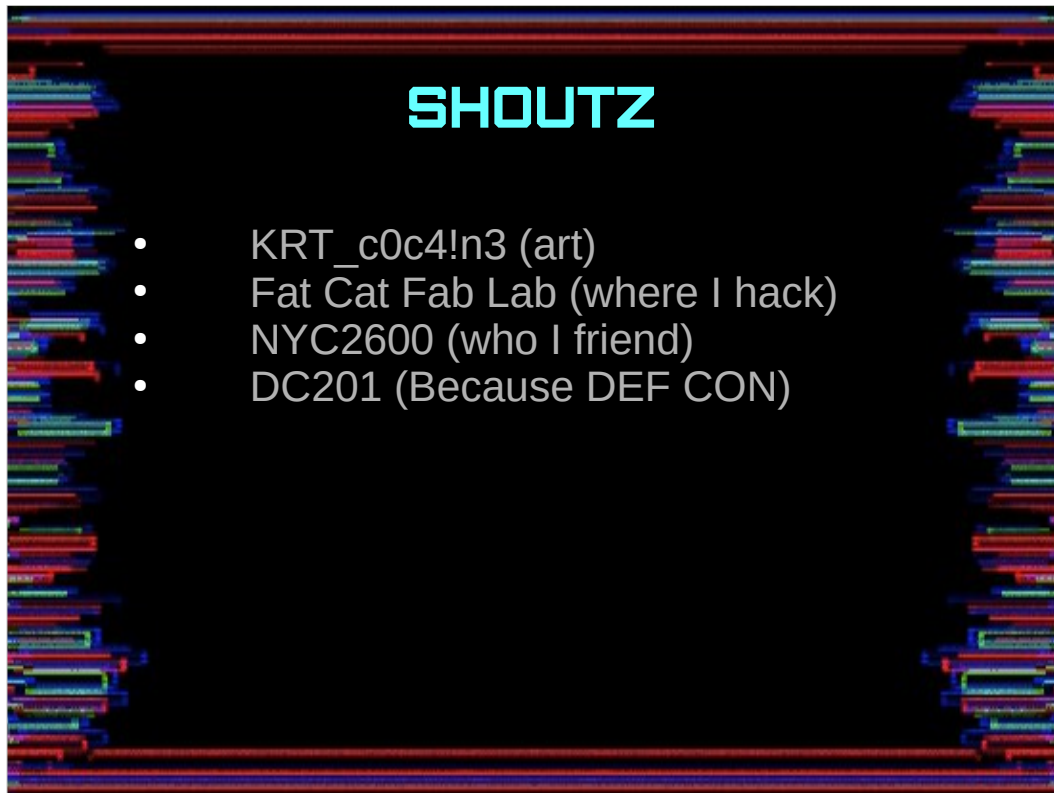


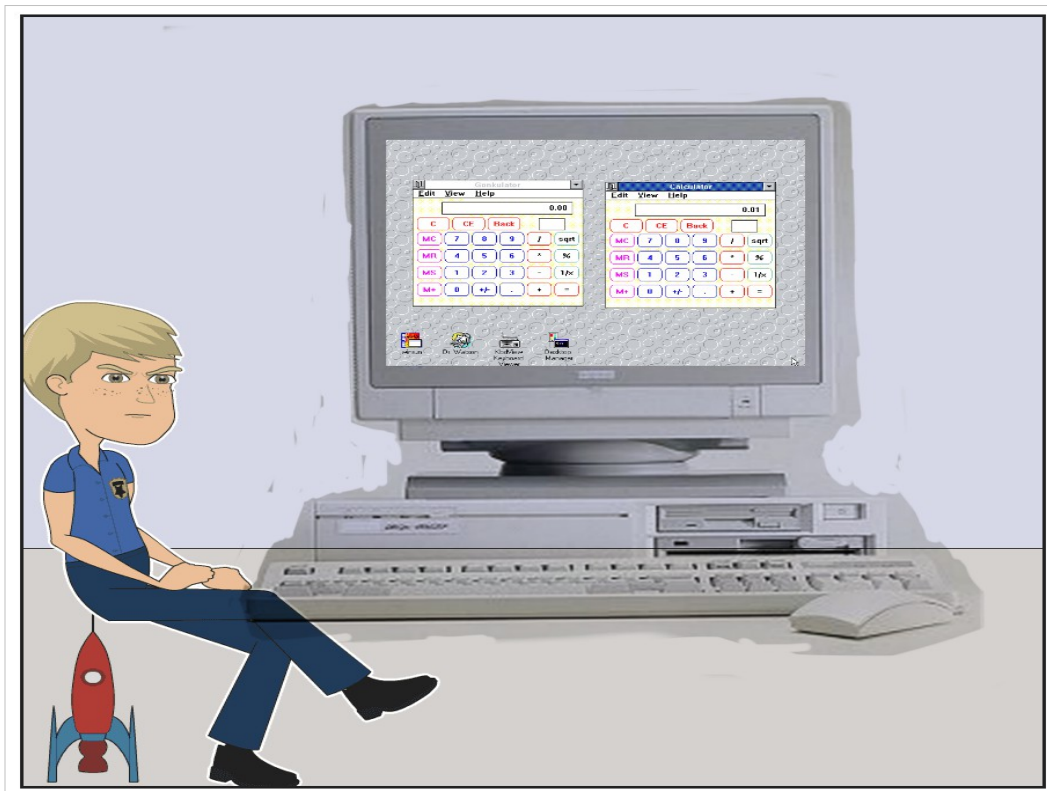
# ASSEMBLY LANGUAGE IS TOO HIGH LEVEL

DEF CON 25  
XlogicX

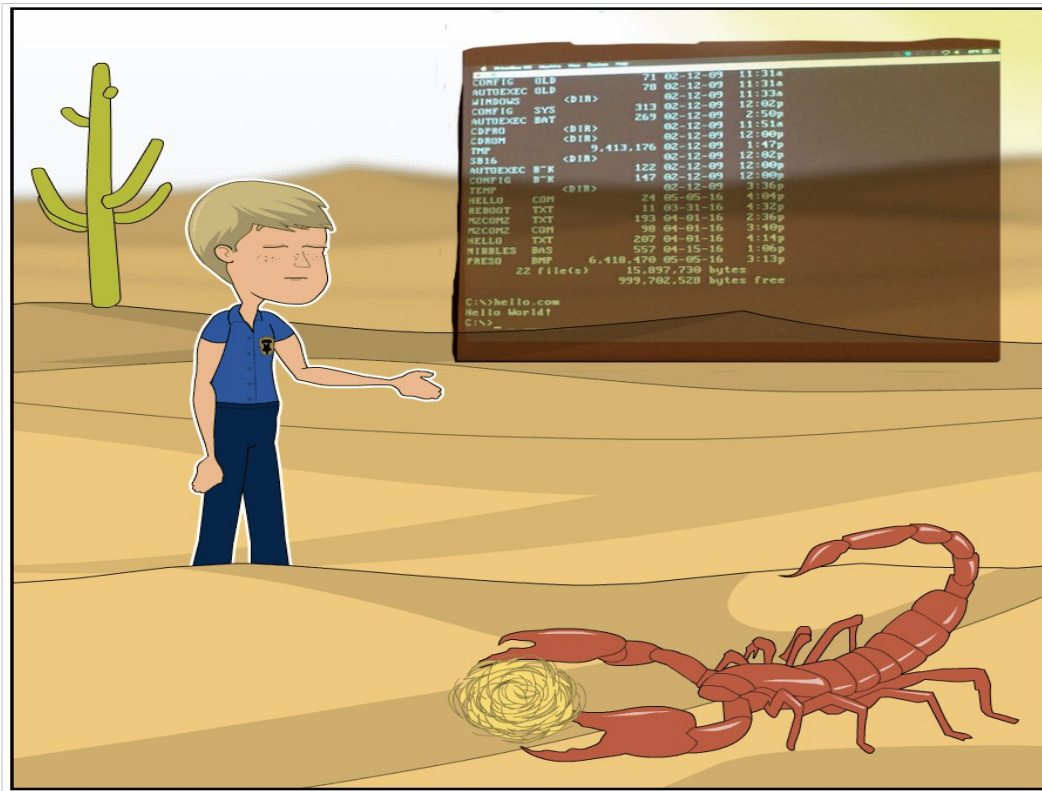
...or the drinking game replaces 'cyber' with 'assembly is too high level'



- My girlfriend KRT\_c0c4!n3 (art director) did a good portion of the art of these slides
- I worked on most of my code and all of these slides from Fat Cat Fab Lab. It's my favorite hackerspace in the NYC area (West Village)
- NYC2600 is my local 2600 community and where I've made most of the friends I have in NYC
- DC201, because it's the closest active DEF CON group in my area

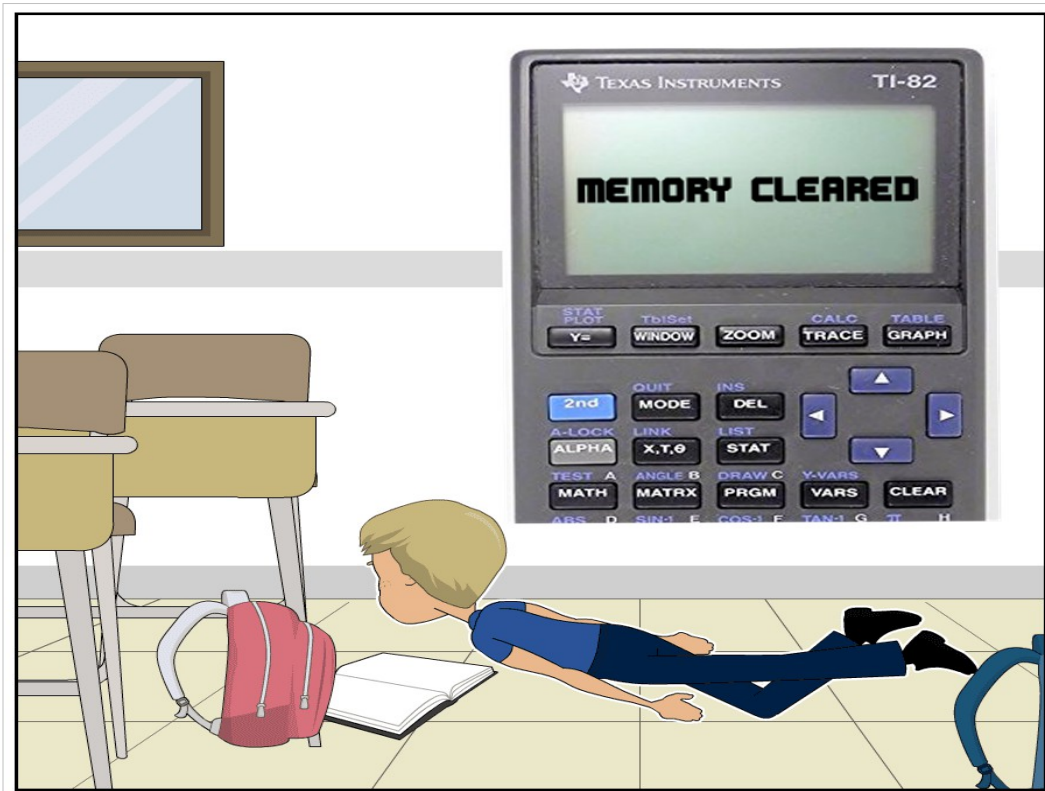


Even as a kid I wanted to do low level programming. I had no access or knowledge of compilers or even major programming languages. I deep down felt like I should be able to type the right binary data into a notepad (or something like it) and run it, but all I had was just some Windows 3.11 and ignorance

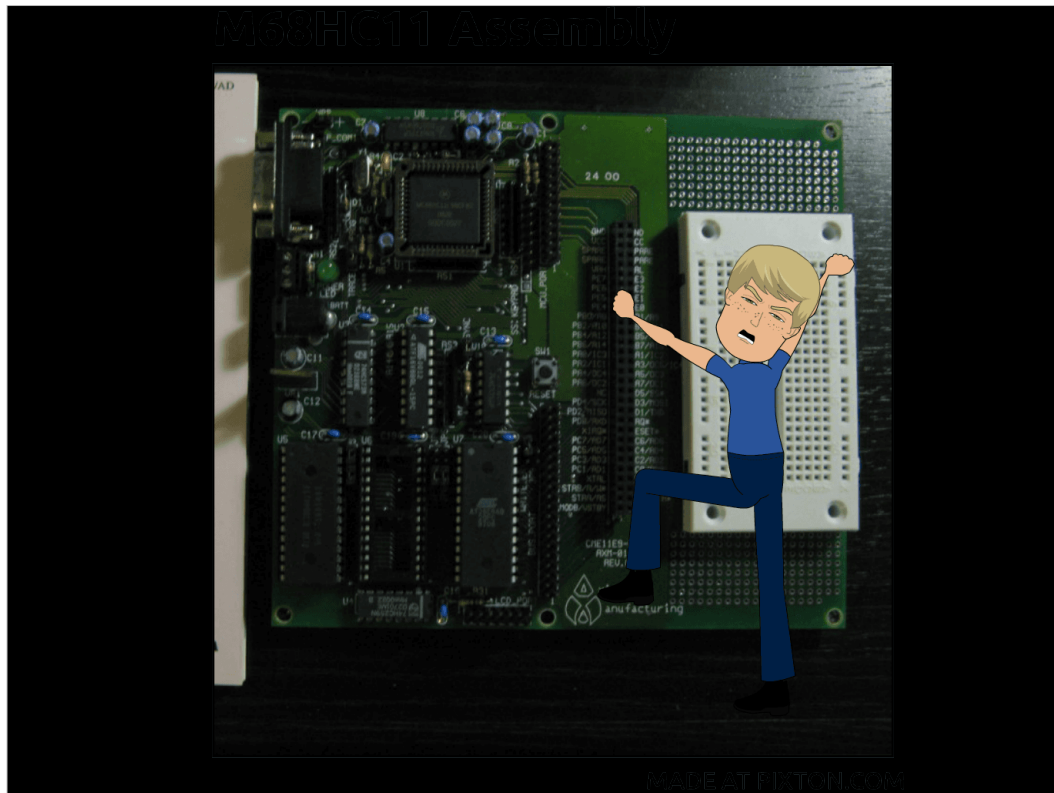


I eventually did end up typing hex into debug (comes with Windows 3.11+) and executed my program live at CactusCon 2016

Deck at <http://xlogicx.net/?p=515>



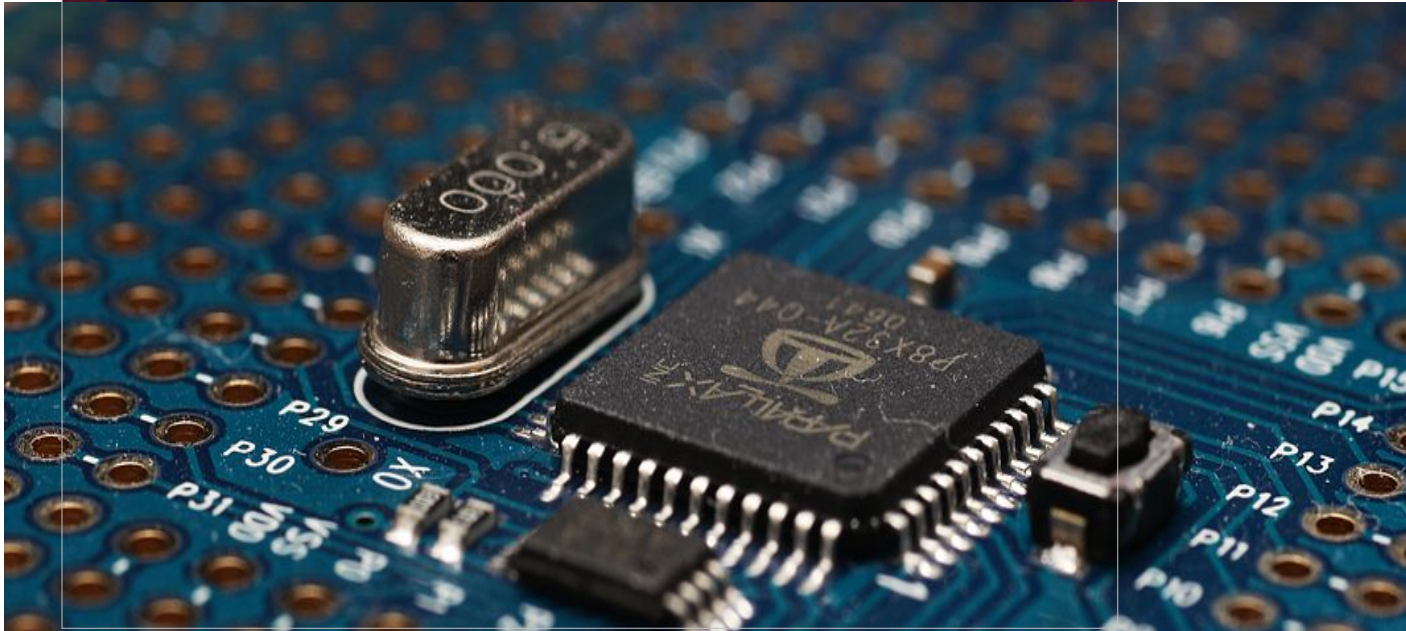
I eventually try to teach myself Z80 assembly. This is because I already had a TI-82 and already tried some sweet games programmed in assembly. The first program I made was an example program that clears the screen. My first attempt to make my own program cleared the memory. This was unintended...



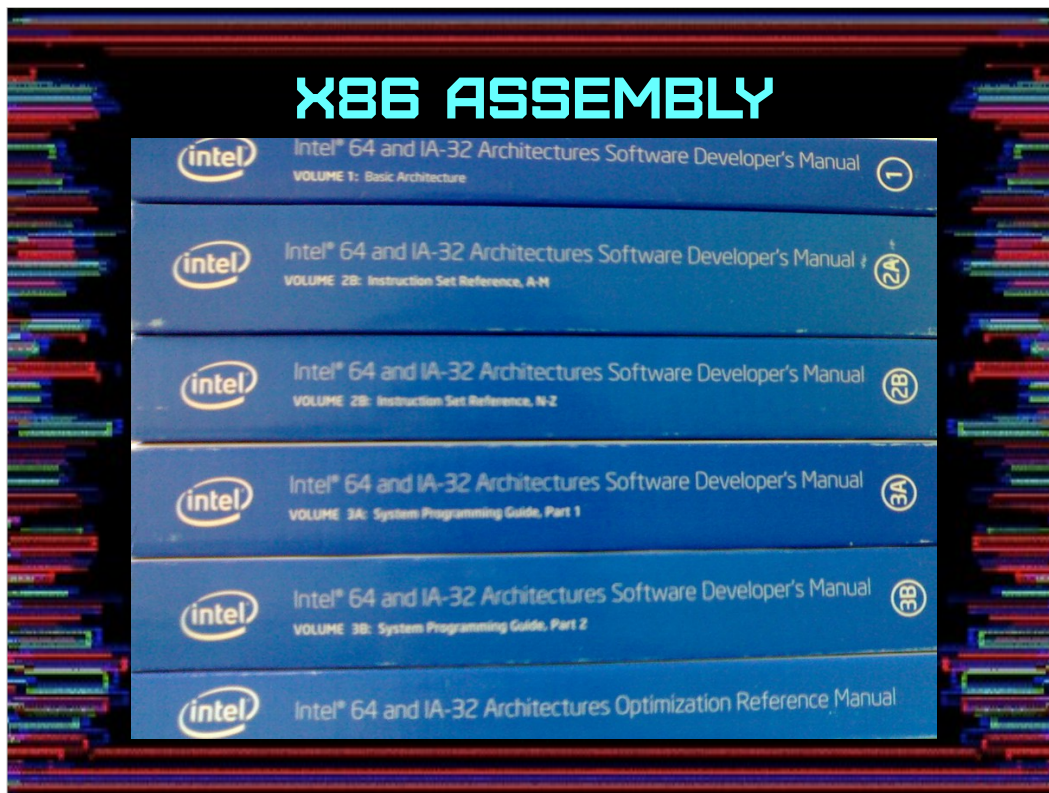
I then formally learn Assembly for the M68HC11 microcontroller in school. I don't even remember if we had a textbook, but we did have the Motorola manual. This manual listed all of the instructions with the machine code next to the instruction. I had a lot of fun with this architecture. Inspired by Godel Escher Bach, I attempted to create a program that replicated itself into the next area of memory and executed itself. I learned the importance of needing to understand the abstraction layer of machine code in order to pull this off. Also, the assembly language and machine code for this architecture was relatively one to one.



## PROPELLER ASSEMBLY



After using various micro-controllers, I start to crave more capabilities and want to find a way to do floating point math in a sane way. LoST eventually convinces me to try this new Propeller micro (well it was new back then in 2006). I ended up not using it for what I had planned, but made an audio driver instead. The performance of this project required the use of Propeller Assembly (instead of the recommended high level language: SPIN). This architecture was pure beauty, and the relationship between the machine-code and assembly language was practically one to one for all intents and purposes. I'm still waiting on Chip Gracey to finish Duke Nukem Forever (...I mean the Propeller II)



Then, a matter of years ago, the company I was working with before voluntold me to take GREM training (GIAC Reverse Engineering Malware). This is the context in which I eventually learned the x86 architecture for assembly language. I learned that the language was the most terrible assembly language I've ever seen up to this point; which made it all that more beautiful.

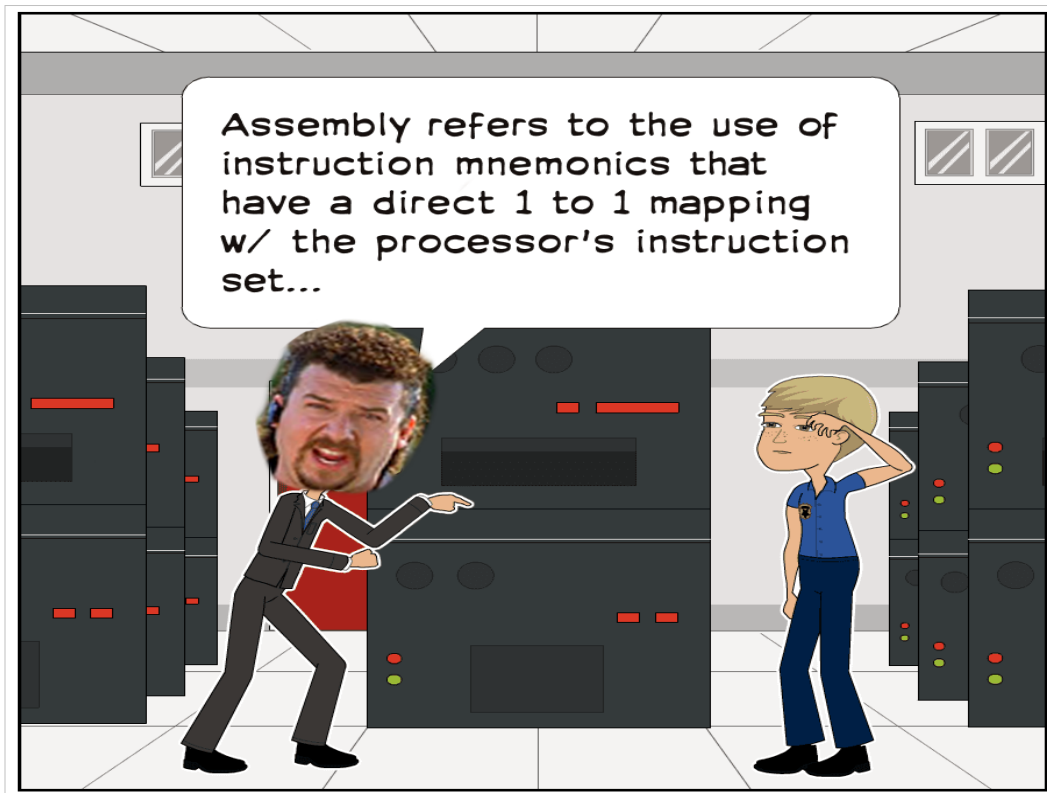
And those manuals in the screenshot, I've read them all, cover to cover.



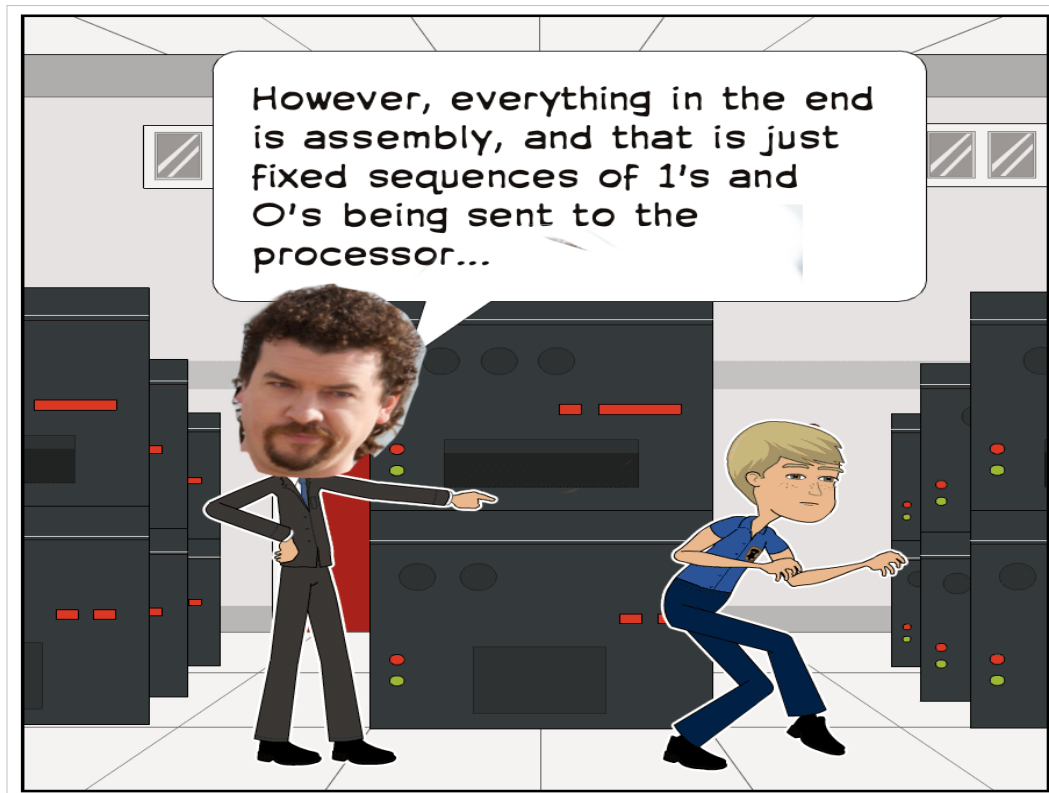
## INTRODUCING: INFOSEC BRO



This is just how I picture most infosec bros; a Kenny Powers like character.



- "Assembly refers to the use of instruction mnemonics that have a direct one-to-one mapping with the processors instruction set"



- "However, everything in the end is assembly, and that is just fixed sequences of ones and zeros being sent to the processor"



- "...that is to say, there are no more layers of abstraction between your code and the processor"





SYNOPSIS®

Copyrighted Material

**IOActive™**  
COMPREHENSIVE COMPUTER SECURITY SERVICES

# Reverse Engineering Code with **IDA Pro**

**Uncover the Good, the Bad, and the Ugly Code with IDA Pro!**

- Master the Most Powerful Disassembler and Debugger for Windows, Linux, or OS X

- Single Step through Code to Understand the Complexities of Worms, Viruses, and Trojans

- Master the Most Powerful Computer Tools Using the IDA Scripting Language

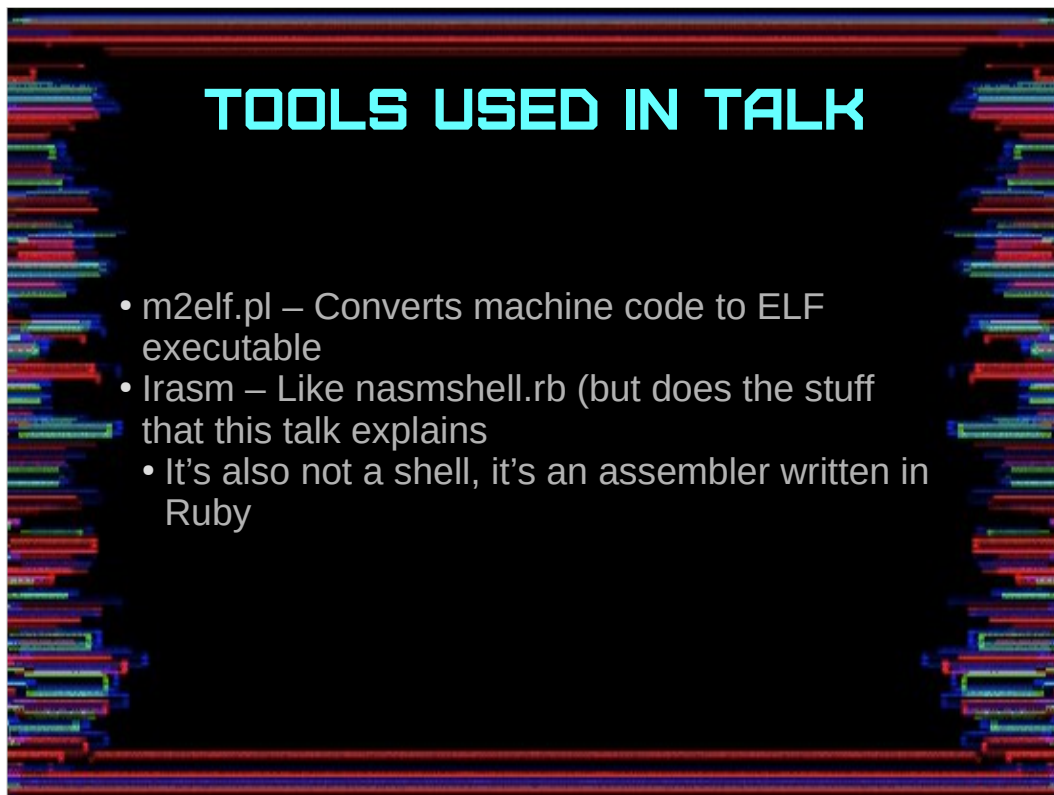
Copyrighted Material

This book had all of the above quotes. This book is also apparently all around terrible in many other ways. But don't just take my word for it...(next slide)



This review was from one of the authors of this book!





I will likely be flying in and out of these tools during this talk. Not as legitimate full demos, just a few seconds here and there to illustrate the points.

M2elf is a tool that I created that takes hex or binary (1's and 0's) in an input file and converts it into a fully ELF executable. For the purposes of this presentation, I will be running it in 'interactive' mode; it takes machine code input and immediately displays the instruction it represents (instruction by instruction)

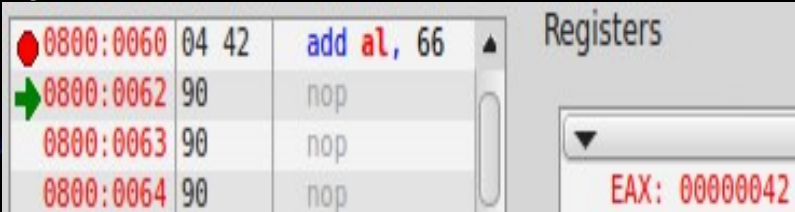
lrasn is like nasmshell.rb, only lrasn is not a shell, it's an assembler. Instead of just displaying official machine code, it outputs a bunch of redundant machine code as well (as discussed in this talk)



## ASSEMBLY ↔ MACHINE CODE

04 ib	ADD AL, imm8	I	Valid	Valid	Add imm8 to AL.
-------	--------------	---	-------	-------	-----------------

- ADD AL, imm8
- Adding an 8-bit value to the 8-bit AL register
- 0x04 is opcode for 'ADD AL' followed by byte to add



The screenshot shows a debugger window with a list of instructions at memory addresses 0800:0060 to 0800:0064. The instruction at 0800:0060 is 'add al, 66' with machine code '04 42'. The other instructions are 'nop' with machine code '90'. To the right, the 'Registers' window shows 'EAX: 00000042'.

Address	Disassembly	Machine Code
0800:0060	add al, 66	04 42
0800:0062	nop	90
0800:0063	nop	90
0800:0064	nop	90

Registers: EAX: 00000042

Let's talk about what people are thinking about when they erroneously say that assembly language and machine code have a one to one relationship.

We can say that if we add the byte of 0x42 to the AL register (ADD AL,0x42). The machine code will be 0x0442 (0x04 for ADD and 0x42 is the byte).

This means that if we wanted to add 0x33 to the AL register, the machine code would be 0x0433

You see the correlation right?

## ASSEMBLY ↔ MACHINE CODE

40+ rd	INC r32	0	N.E.	Valid	Increment doubleword register by 1.
--------	---------	---	------	-------	-------------------------------------

- INC, 32-bit Register
- Increments a 32 bit register
- These registers come in the following order:
- EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI

0800:0060	40	inc eax
0800:0061	41	inc ecx
0800:0062	42	inc edx
0800:0063	43	inc ebx
0800:0064	44	inc esp
0800:0065	45	inc ebp
0800:0066	46	inc esi
0800:0067	47	inc edi
0800:0068	90	nop
0800:0069	90	nop
0800:006a	90	nop
0800:006b	90	nop

Registers

EAX: 00000001

EBX: 00000001

ECX: 00000001

EDX: 00000001

EBP: 00000001

ESP: bff48051

ESI: 00000001

EDI: 00000001

This one is a little more complicated but not that bad. All of this increment (INC) instructions start with a 0x4 nibble, and the next nibble corresponds to the register you want to increment. Since EAX is first, INC EAX is just 0x40.

This is unless we are using a 64 bit processor, then the 0x40 is a prefix byte, different story all together though.

## ASSEMBLY ↔ MACHINE CODE

B0+ rb ib	MOV r8, imm8	OI	Valid	Valid	Move imm8 to r8.
C6 /0 ib	MOV r/m8, imm8	MI	Valid	Valid	Move imm8 to r/m8.

- MOV r8, imm8
- Move a byte into an 8-bit register
- These registers come in the following order:
- AL, CL, DL, BL, AH, CH, DH, BH

Similar to the last two instructions. This is a group of MOV instructions where 0xB is the first nibble representing MOV, and the next nibble represents the register. Finally, the byte that follows is the byte to be moved to said register.

But wait, there's a 0xC6 format that allows us to add a byte to a more complex data structure that includes memory pointers AND also registers (and because this structure supports registers, we find a redundancy here)

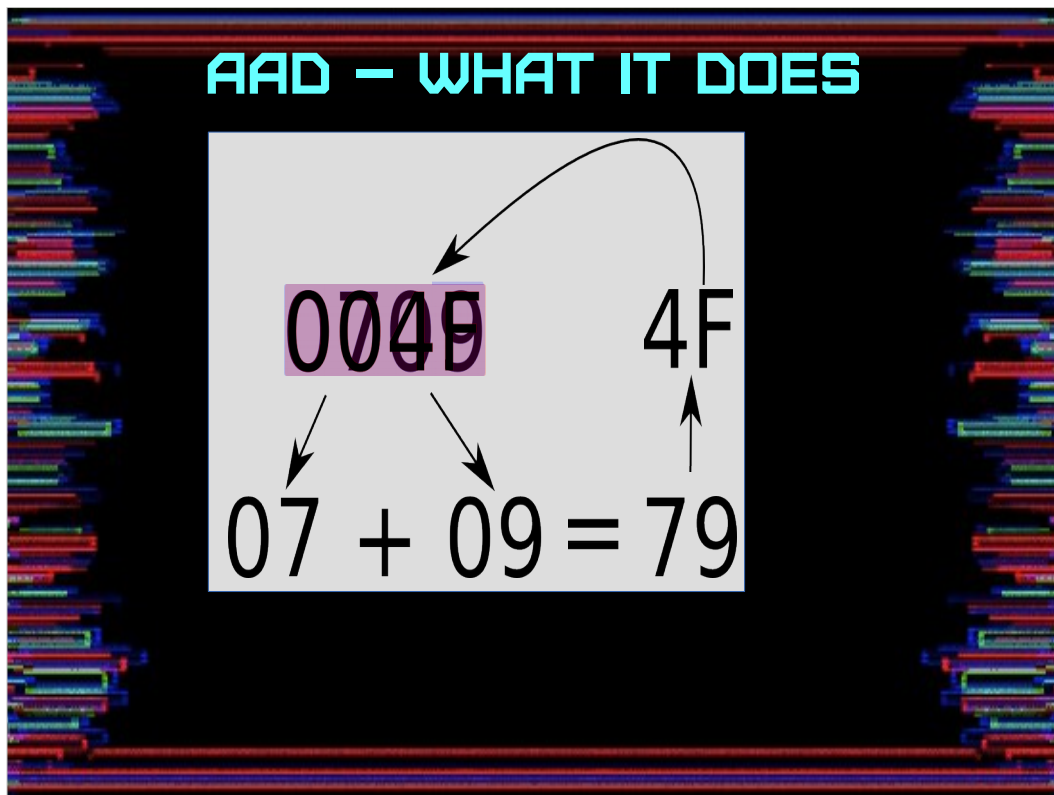
Knowing all of this, if you did: `mov al, 0x44`  
 Your assembler (and nasmshell) would output:  
 0xB042  
 It wouldn't output 0xC6C042  
 But the irasm tool will

## AAD (ASCII ADJUST AX BEFORE DIVISION)

- The assembly for this is too high level
- The machine code is also too high level
- Even the mathematical concept is too high level!
- Or, how to do base1 and base0 math
- Supposed to do Base10 conversion

I love the AAD instruction. It says it does a thing. But the thing it actually does to do the thing it says it does is far more interesting. The next several slides go into depth of these things.





This instruction takes the value of AX (two bytes).

It breaks them out and considers them to be two decimal numbers (base10).

Regardless of the misleading '+' symbol in the slide, it combines the two digits as if the zeros weren't there.

The result is considered a base10 value. It's hexadecimal representation is stored back into AX. This really means that it is stored into AL and AH gets wiped. Because even the largest decimal value of 99 would still fit into AL as hexadecimal.

This style of slides are animated; they will look a little weird in the PDF version.

## AAD – ASSUMPTIONS

0709

- The entire value is 16 bits
- The two halves make up 8 bits (07 and 09)
- Being that the values are converting from base 1
- The two halves need to be from 00-09
- Even though 0A-FF are valid 8 bit values

To think like a hacker for a second, think of the context of what goes wrong when you don't do input validation and the things that could go wrong.

In AX, you're supposed to have a decimal (0-9) value in AH and AL. However, each of these registers could actually be in the range of 0x00-0xFF

## AAD – DEBUGGED

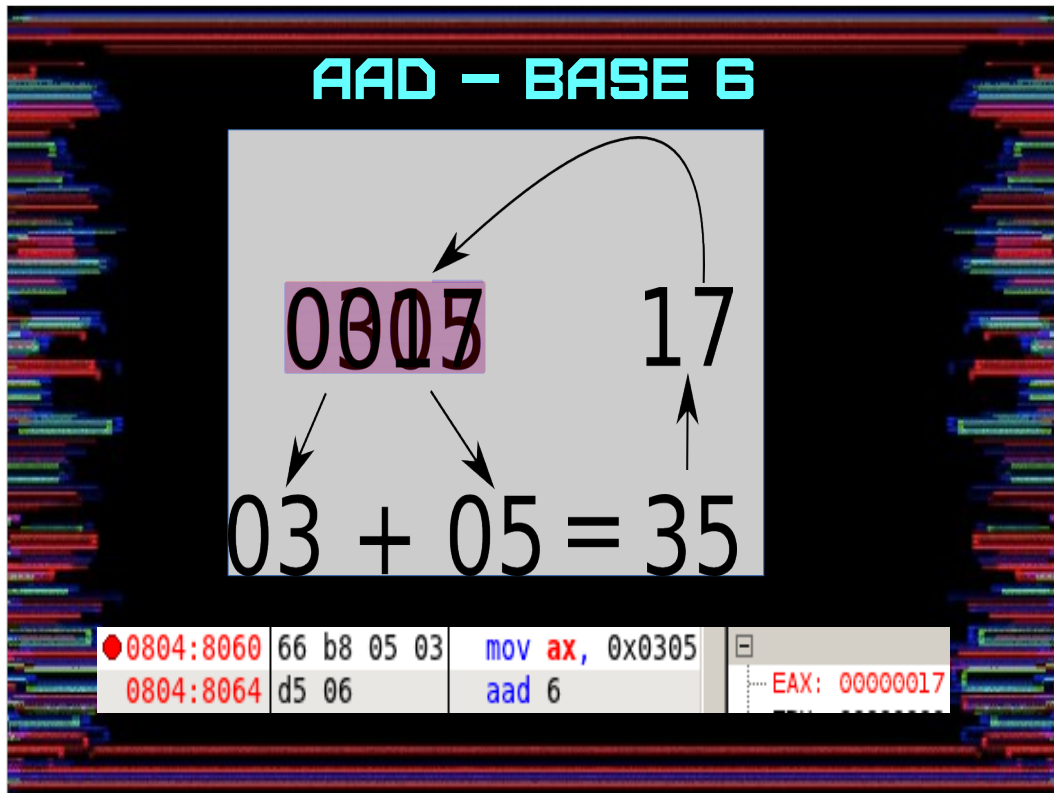
● 0804:8060	66 b8 09 07	mov ax, 0x0709	
0804:8064	d5 0a	aad 10	EAX: 0000004f

- 0709 moved into the 16 bit register (ax)
- AAD performed
- The 'A' (al/ah/ax/eax) register now contains 004f
- The AAD mnemonic is interpreted by all assemblers to mean adjust ASCII (base 10) values. To adjust values in another number base, the instruction must be hand coded in machine code (D5 imm8)

The interesting thing here is that the real machine code for the opcode of AAD is just 0xD5, the next byte is actually not part of the opcode; it's an operand. It just defaults to 0x0A (or 10 in decimal). In assembly, you can only type 'aad'; you can't give it the base you want to use because base10 is assumed.

However, if you write this instruction in directly in machine code though, you can actually choose a different base and the high level mathematical concept works out.

Assembly, it's too high level



This is us working through an example of choosing our own arbitrary base of 6.

Our character set for base6 is from 0-5.

Cramming 3 and 5 together gives us 35.

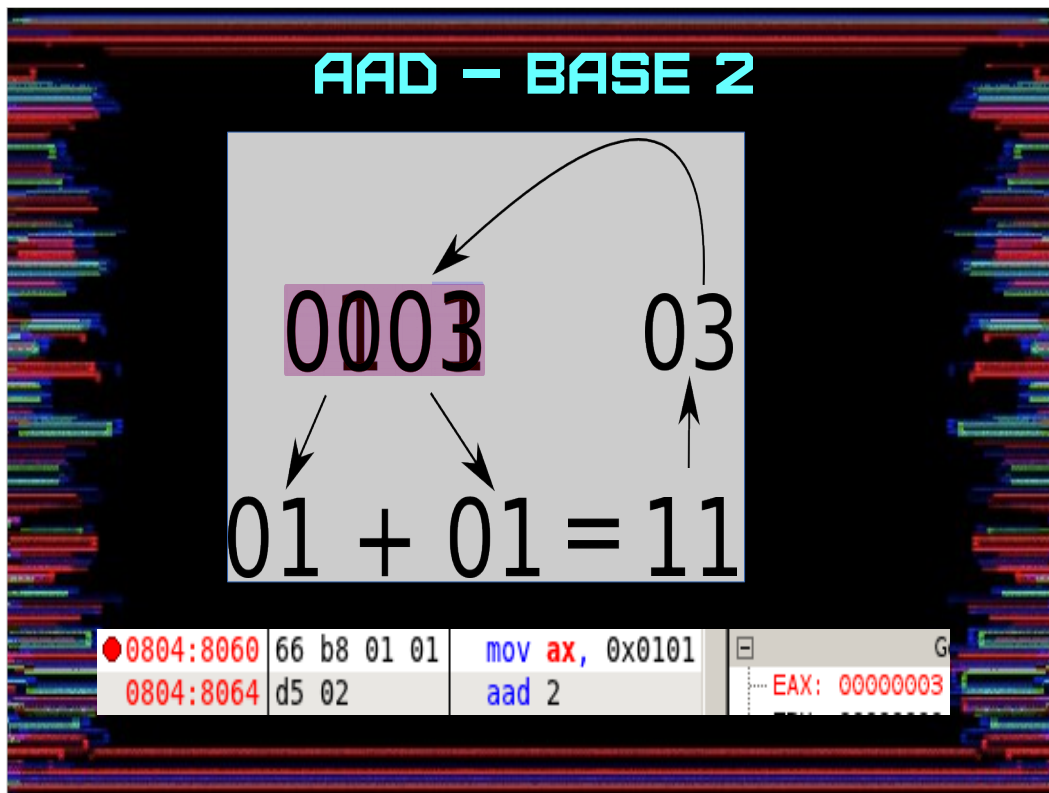
This instruction needs to convert 35 (base6) to a hexadecimal (base16) value.

35 in base10 is actually 23 = ((3 \* 6) + (5 \* 1))

23 in hexadecimal is 0x17

It's amazing, it all works out!



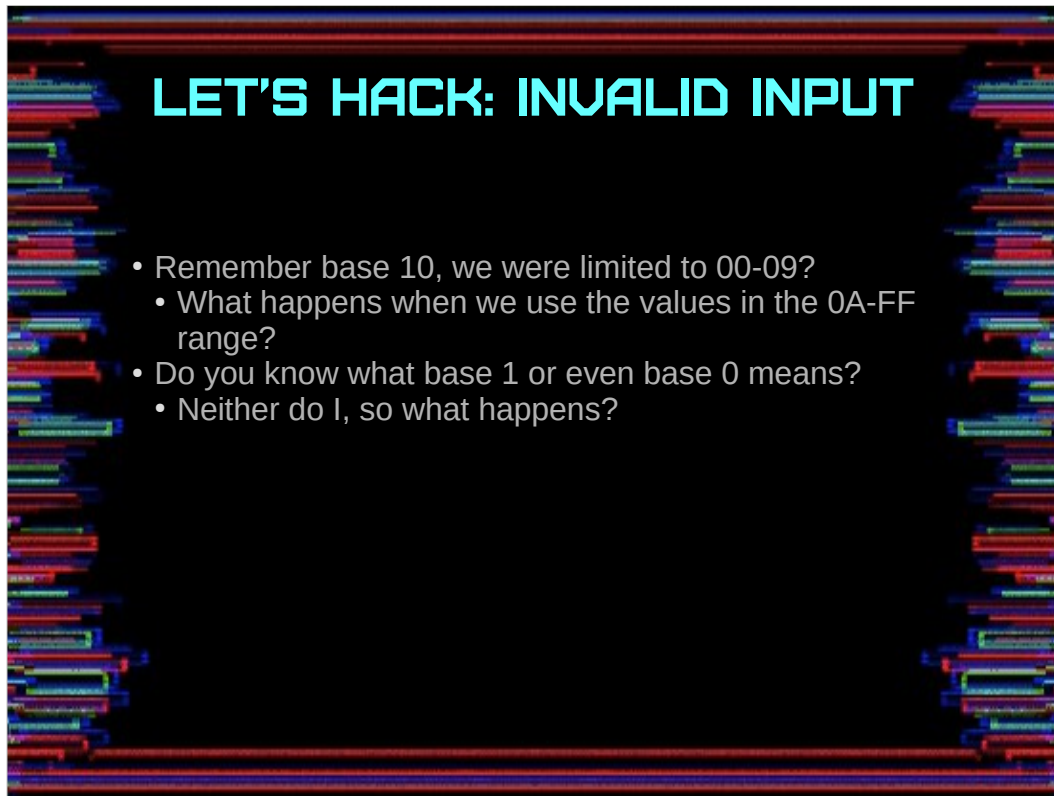


Let's do base2

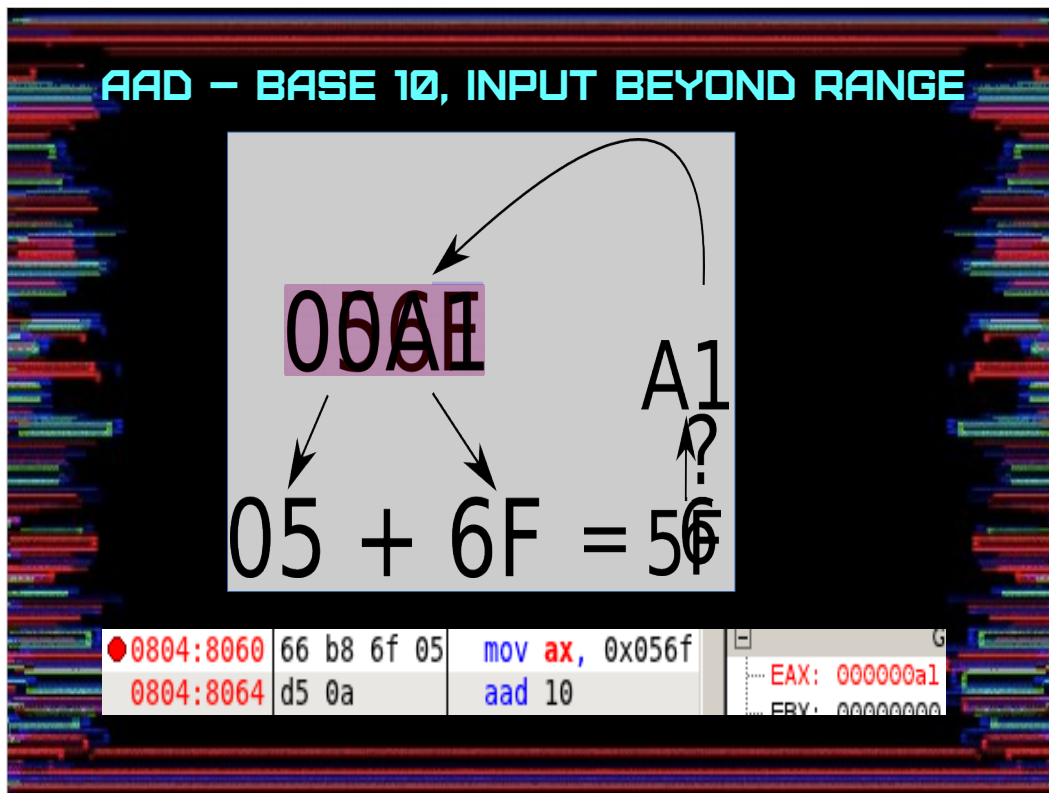
We cram 1 and 1 together and get 11

11 in binary is 3 in decimal which is 0x03 in hexadecimal

So this works too.



This is an introduction slide for us to try some real ignorant things and to attempt to make some meaning out of it

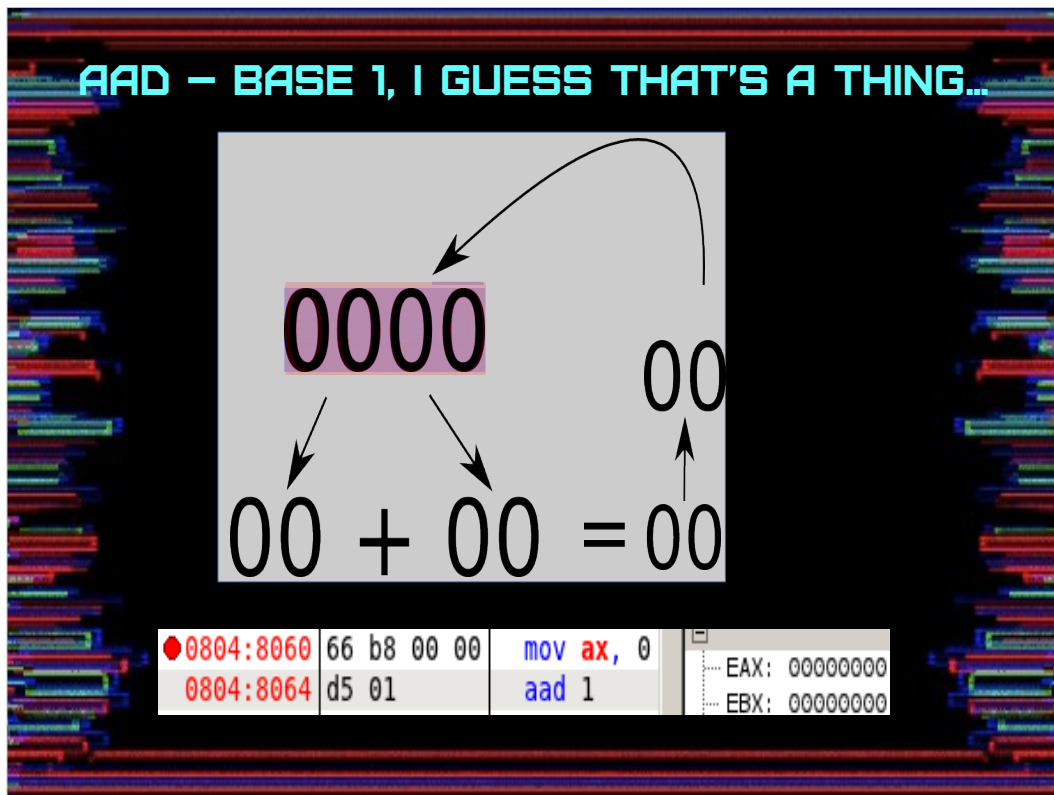


This is us going far above base10 values in AX (AH/AL), but then specifying base10 for the aad instruction.

It's hard to visualize cramming 5 and 6F together, but the slide does it's best to make something of it.

By the process of magic (whatever AAD is actually doing), we get the result of 0xA1.

0xA1 is then stored back into AX

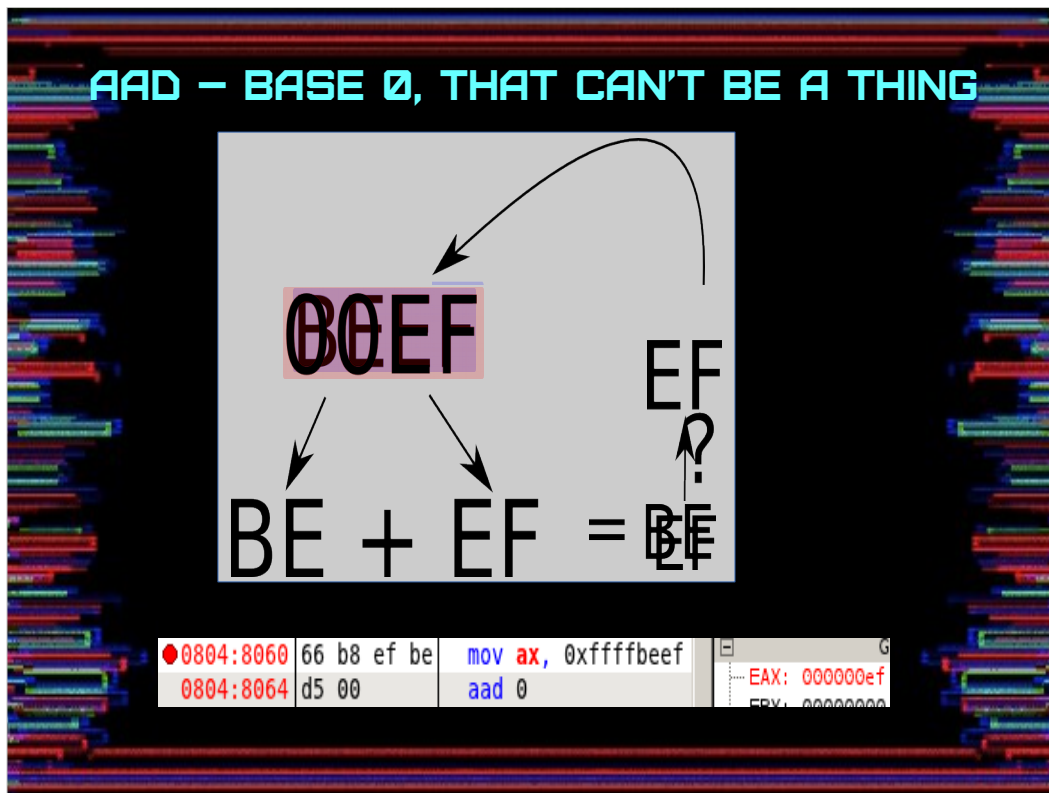


What about base 1?

Well, our only valid character is zero, so:

Cram 0 with 0 to get 0 to convert to 0 and store 0 back into our register that already had 0.

Pointless, but at least it makes sense and we know whats going on here I guess.



Then there's base0. There is really no valid character for this, so I just made AX 0xBEEF.

We cram it together, and by the magical process of AAD we get a result of 0xEF and store it back into AX.





It really is fine though, because microcode

## MACHINE CODE: TOO HIGH LEVEL

- What's actually happening under the Hood?
- Microcode
- Intel's PseudoCode for AAD:

```
IF 64-Bit Mode
THEN
    #UD;
ELSE
    tempAL ← AL;
    tempAH ← AH;
    AL ← (tempAL + (tempAH * imm8)) AND FFH;
    (* imm8 is set to 0AH for the AAD mnemonic.*)
    AH ← 0;
FI;
```

This screenshot from the Intel manual shows what is actually happening under the hood.

It's not literally a base conversion, just some mathematical operations (an 'algorithm') that happen to perform the conversion when you don't feed it garbage.

This is fucking profound. Mathematics is not reality, it's just a model for it sometimes. Don't take math too seriously, math is stupid.

## A MORE SIMPLE FORMULA

- $AL = AL + (AH * \text{base})$
- Where:
  - AL is the last 2 bytes of input
  - AH is the first 2 bytes of input
  - Base defaults to 10 (but we can machine hack that)

This is a better representation of what the Intel pseudo-code is doing. It's actually pretty elegant looking. It's also pretty cool that something so simple can 'convert' 'bases' so easily

## A NEW UNDERSTANDING

- $AL = AL + (AH * \text{base})$
- 0709 (base10):  $09 + (07 * 10) = 4F$  (79 decimal)
- 0305 (base6):  $05 + (03 * 6) = 17$  (23 decimal)
- 0101 (base2):  $01 + (01 * 2) = 3$  (3 decimal)
- 056F (base10):  $6F + (05 * 10) = A1$  (161 decimal)
- 0000 (base1):  $00 + (00 * 1) = 0$  (0 decimal)
- BEEF (base0):  $EF + (BE * 0) = EF$  (239 decimal)

For fun, we use this simple formula to crunch through all of the examples in the previous slides to see that the formula does crunch out the answers that we expect them to.

## HOW IS THIS USEFUL

- We have a new certain way to clear AH
  - Old way number 1: `mov ah, 0`
  - Efficient Compiler way: `xor ah, ah`
  - Our new stupid way: `db 0xd5, 0x00`
    - Or AAD base 0

All kidding aside about clearing the AH register, it's cool to know that we can do conversions in obscure bases with one instruction. It's even cooler that the way to implement it is even more obscure: you have to do it in machine code

...because assembly is too high level



## MODR/M + SIB

- Allows you to do various encodings with registers and memory
- Memory encodings is where it gets interesting (complicated)
- Already complicated enough, even without the redunds

This can be some rough terrain right here. Not having to manually do this encoding should make people appreciate assembly language as a super high level language that makes things easier for the programmer. We will be treading this terrain in the next 30ish something slides!

This encoding is used to allow the programmer to use registers and memory pointers as operands

## MEMORY POINTER FORMAT

- Things you can use in a pointer:
  - Register (base register)
  - Register multiplied by 1, 2, 4, and 8 (scaled)
  - A 8bit or 32 bit offset (displacement)
- All of these are optional
  - Examples:
    - `[eax + ebx * 2]`
    - `[ebx + 0x33]`
    - `[ecx * 8 + 0x11223344]`
    - `[0x33]`

In a memory pointer, you can have a base register, a scaled register, and a displacement. They are all optional, but you at least need to use one of them (otherwise it would be nothing at all)

Of the registers, you have the 8 general purpose ones to choose from (with some major exceptions)

If `eax` is `0x11223344`, `XOR [eax]`, `eax` will XOR the value of `eax` with the value in the address of `0x11223344` and store it at that address

You can also add to the address of that pointer with a displacement. `[eax + 0x42]` would be `[0x11223386]` (considering what `eax` originally had above)

# MODR/M TABLE

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte												
r8(r) r16(r) r32(r) mm(r) xmm(r) (in decimal) /digit (Opcode) (in binary) REG =	AL AX EAX MM0 XMM0 0 000	CL CX ECX MM1 XMM1 1 001	DL DX EDX MM2 XMM2 2 010	BL BX EBX MM3 XMM3 3 011	AH SP ESP MM4 XMM4 4 100	CH BP EBP MM5 XMM5 5 101	DH SI ESI MM6 XMM6 6 110	BH DI EDI MM7 XMM7 7 111				
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)									
[EAX] [ECX] [EDX] [EBX] [J] - 1 disp32 <sup>2</sup> [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F		
[EAX]+disp8 <sup>3</sup> [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [J] - 1+disp8 [EBP]+disp8 [ESI]+disp8 [EDI]+disp8		01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F	
[EAX]+disp32 <sup>2</sup> [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [J] - 1+disp32 [EBP]+disp32 [ESI]+disp32 [EDI]+disp32			10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7				11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	CB CA CC CD CE CF	D0 D1 DA DB DC DD DE DF	DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	EB EC ED EE EF	FB FC FD FE FF

This is the machine encoding table that makes it all happen (well half of it, the other half is the SIB byte when required).

The MODR/M Table allows for encoding operands as a register, a pointer with one base register, a pointer with a base register and a 8 or 32 bit displacement, or just a 32 bit displacement.

If you want to have a scaled register or mix and match the above with a scaled register, then you need the SIB byte (selectable from this table)

As always, there are many exceptions

# XOR EAX, EDX [0X31D0]

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

r8(/r) r16(/r) r32(/r) mm(/r) xmm(/r) (In decimal) /digit (Opcode) (In binary) REG =			AL AX MM0 0	CL CX MM1 1	DL DX MM2 2	BL BX MM3 3	AH SP MM4 4	CH BP MM5 5	DH SI MM6 6	BH DI MM7 7
			000	001	010	011	100	101	110	111
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F
[EAX]+disp8 <sup>3</sup> [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF

In this slide we work through an example, because we like to explore more than just theory.

In most of our examples, we will use the 0x31 machine opcode for XOR (there are exceptions when we cover redundancies). It's the XOR r/m32, r32 encoding (so first operand can be register or pointer and second operand has to be a register, both 32 bit)

In the table, we line up EAX with EDX to get our 0xD0 value for the operand information for our machine code.

# XOR [ECX], EAX [0X3101]

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

r8(r/r) r16(r/r) r32(r/r) mm(r) xmm(r/r) (in decimal) /digit (Opcode) (in binary) REG =			AL AX EAX MM0 0 000	CL CX ECX MM1 1 001	DL DX EDX MM2 2 010	BL BX EBX MM3 3 011	AH SP ESP MM4 4 100	CH BP EBP MM5 5 101	DH SI ESI MM6 6 110	BH DI EDI MM7 7 111
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F
[EAX]+disp8 <sup>3</sup> [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF

Next we do a pointer for the first operand. Note we are still starting with the 0x31 encoding for XOR

We are using the pointer of [ECX] for the first operand and EAX for the second operand. All we have to do is line them up to arrive at the 0x01 byte for the machine code byte to encode this. It's just as straight forward as the last example









**XOR [EBX + ECX \* 4 + 0x42], EAX [0x31448B42]**

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

r8(r) r16(r) r32(r) mm(r) xmm(r) (In decimal) /digit (Opcode) (In binary) REG =										
			AL AX EAX MM0 XMM0 0 000	CL CX ECX MM1 XMM1 1 001	DL DX EDX MM2 XMM2 2 010	BL BX EBX MM3 XMM3 3 011	AH SP ESP MM4 XMM4 4 100	CH BP EBP MM5 XMM5 5 101	DH SI ESI MM6 XMM6 6 110	BH DI EDI MM7 XMM7 7 111
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] [---]1 disp322 [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F
[EAX]+disp83 [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [---]+disp8 [EBP]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [---]+disp32 [EBP]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF

Now we start to get a little crazier; we are going to use a scaled register.

Lining up the second operand of EAX on the chart is easy. To use a scaled register, we need the SIB byte, which is one of the horizontal options using [---][---].

There are 3 different variations of this SIB option, one without a displacement, one with an 8 bit displacement, and another with a 32 bit displacement. In this case, it's just the 8 bit displacement. So we choose 0x44 in this table, and then look next to our SIB table to pick the actual Base and Scaled register

**XOR [EBX + ECX \* 4 + 0X42], EAX [0X31448B42]**

Table 2-3. 32-Bit Addressing Forms with the SIB Byte

r32 (In decimal) Base = (In binary) Base =			EAX 0 000	ECX 1 001	EDX 2 010	EBX 3 011	ESP 4 100	[*] 5 101	ESI 6 110	EDI 7 111
Scaled Index	SS	Index	Value of SIB Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] none [EBP] [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 08 10 18 20 28 30 38	01 09 11 19 21 29 31 39	02 0A 12 1A 22 2A 32 3A	03 0B 13 1B 23 2B 33 3B	04 0C 14 1C 24 2C 34 3C	05 0D 15 1D 25 2D 35 3D	06 0E 16 1F 26 2F 36 3F	07 0F 17 1F 27 2F 37 3F
[EAX*2] [ECX*2] [EDX*2] [EBX*2] none [EBP*2] [ESI*2] [EDI*2]	01	000 001 010 011 100 101 110 111	40 48 50 58 60 68 70 78	41 49 51 59 61 69 71 79	42 4A 52 5A 62 6A 72 7A	43 4B 53 5B 63 6B 73 7B	44 4C 54 5C 64 6C 74 7C	45 4D 55 5D 65 6D 75 7D	46 4E 56 5E 66 6E 76 7E	47 4F 57 5F 67 6F 77 7F
[EAX*4] [ECX*4] [EDX*4] [EBX*4] none [EBP*4] [ESI*4] [EDI*4]	10	000 001 010 011 100 101 110 111	80 88 90 98 A0 A8 B0 B8	81 89 91 99 A1 A9 B1 B9	82 8A 92 9A A2 AA B2 BA	83 8B 93 9B A3 AB B3 BB	84 8C 94 9C A4 AC B4 BC	85 8D 95 9D A5 AD B5 BD	86 8E 96 9F A6 AE B6 BE	87 8F 97 9F A7 AF B7 BF
[EAX*8] [ECX*8] [EDX*8] [EBX*8] none [EBP*8] [ESI*8] [EDI*8]	11	000 001 010 011 100 101 110 111	C0 C8 D0 D8 E0 E8 F0 F8	C1 C9 D1 D9 E1 E9 F1 F9	C2 CA D2 DA E2 EA F2 FA	C3 CB D3 DB E3 EB F3 FB	C4 CC D4 DC E4 EC F4 FC	C5 CD D5 DD E5 ED F5 FD	C6 CE D6 DE E6 EE F6 FE	C7 CF D7 DF E7 EF F7 FF

The Base register will be the vertical line and the Scaled (multiplied register) will be the horizontal line.

Finding EBX (vertical base register) is the easiest.

For the horizontal line, we must find the item that uses ECX and is also \* 4. This is actually not terribly hard to find on the table either.

When you line this up, you get 0x8B for the SIB byte.

Finally, we have the displacement of 0x42 to add to the end of the instruction to get our final result



# XOR [ESP], EAX [0X310424]

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

r8(r) r16(r) r32(r) mm(r) xmm(r) (In decimal) /digit (Opcode) (In binary) REG =			AL AX EAX MM0 XMM0 0 000	CL CX ECX MM1 XMM1 1 001	DL DX EDX MM2 XMM2 2 010	BL BX EBX MM3 XMM3 3 011	AH SP ESP MM4 XMM4 4 100	CH BP EBP MM5 XMM5 5 101	DH SI ESI MM6 XMM6 6 110	BH DI EDI MM7 XMM7 7 111
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] [--][--] disp32 <sup>2</sup> [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F
[EAX]+disp8 <sup>3</sup> [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [BP]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [BP]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF

Now lets dig into some weird exceptions; lets start with using ESP as the base register in a pointer. When looking at the table, ESP isn't an option?

However, we know from the SIB byte that you can choose a Base register, although you have to choose a Scaled register as well. But did you notice from the table on the last slide that 'none' was an option for the Scaled register. That's the hack that assemblers use.

For the MODR/M byte, we line up EAX for the vertical and the [--][--] (SIB) for no displacement. This gives us 0x04 for our MODR/M byte.

Next let's look at what we do with the SIB byte.

# XOR [ESP], EAX [0X310424]

Table 2-3. 32-Bit Addressing Forms with the SIB Byte

r32 (In decimal) Base = (In binary) Base =			EAX 0 000	ECX 1 001	EDX 2 010	EBX 3 011	ESP 4 100	[*] 5 101	ESI 6 110	EDI 7 111
Scaled Index	SS	Index	Value of SIB Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] none [EBP] [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 08 10 18 20 28 30 38	01 09 11 19 21 29 31 39	02 0A 12 1A 22 2A 32 3A	03 0B 13 1B 23 2B 33 3B	04 0C 14 1C 24 2C 34 3C	05 0D 15 1D 25 2D 35 3D	06 0E 16 1E 26 2E 36 3E	07 0F 17 1F 27 2F 37 3F
[EAX*2] [ECX*2] [EDX*2] [EBX*2] none [EBP*2] [ESI*2] [EDI*2]	01	000 001 010 011 100 101 110 111	40 48 50 58 60 68 70 78	41 49 51 59 61 69 71 79	42 4A 52 5A 62 6A 72 7A	43 4B 53 5B 63 6B 73 7B	44 4C 54 5C 64 6C 74 7C	45 4D 55 5D 65 6D 75 7D	46 4E 56 5E 66 6E 76 7E	47 4F 57 5F 67 6F 77 7F
[EAX*4] [ECX*4] [EDX*4] [EBX*4] none [EBP*4] [ESI*4] [EDI*4]	10	000 001 010 011 100 101 110 111	80 88 90 98 A0 A8 B0 B8	81 89 91 99 A1 A9 B1 B9	82 8A 92 9A A2 AA B2 BA	83 8B 93 9B A3 AB B3 BB	84 8C 94 9C A4 AC B4 BC	85 8D 95 9D A5 AD B5 BD	86 8E 96 9E A6 AE B6 BE	87 8F 97 9F A7 AF B7 BF
[EAX*8] [ECX*8] [EDX*8] [EBX*8] none [EBP*8] [ESI*8] [EDI*8]	11	000 001 010 011 100 101 110 111	C0 C8 D0 D8 E0 E8 F0 F8	C1 C9 D1 D9 E1 E9 F1 F9	C2 CA D2 DA E2 EA F2 FA	C3 CB D3 DB E3 EB F3 FB	C4 CC D4 DC E4 EC F4 FC	C5 CD D5 DD E5 ED F5 FD	C6 CE D6 DE E6 EE F6 FE	C7 CF D7 DF E7 EF F7 FF

Since ESP is our Base register, we line that up vertically. We choose the first 'none' horizontal line for the Scaled register to give us 0x24.

So what's the difference between that 'none' and the 3 others. There isn't any in this particular case, hence the next slide

## XOR [ESP], EAX [0X310424], WITH ALL THE 'NONES'

0800:0060	31 04 24	xor dword ptr [esp], eax
0800:0063	31 04 64	xor dword ptr [esp], eax
0800:0066	31 04 a4	xor dword ptr [esp], eax
0800:0069	31 04 e4	xor dword ptr [esp], eax

In this slide we see the PoC of using all 4 of the 'none' options in the SIB byte. This is to note that the assembly is the same for any of these

## USING SIB WHEN YOU DON'T NEED TO

Table 2-3. 32-Bit Addressing Forms with the SIB Byte

r32 (In decimal) Base = (In binary) Base =			EAX 0 000	ECX 1 001	EDX 2 010	EBX 3 011	ESP 4 100	[*] 5 101	ESI 6 110	EDI 7 111
Scaled Index	SS	Index	Value of SIB Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] none [EBP] [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 08 10 18 20 28 30 38	01 09 11 19 21 29 31 39	02 0A 12 1A 22 2A 32 3A	03 0B 13 1B 23 2B 33 3B	04 0C 14 1C 24 2C 34 3C	05 0D 15 1D 25 2D 35 3D	06 0E 16 1E 26 2E 36 3E	07 0F 17 1F 27 2F 37 3F
[EAX*2] [ECX*2] [EDX*2] [EBX*2] none [EBP*2] [ESI*2] [EDI*2]	01	000 001 010 011 100 101 110 111	40 48 50 58 60 68 70 78	41 49 51 59 61 69 71 79	42 4A 52 5A 62 6A 72 7A	43 4B 53 5B 63 6B 73 7B	44 4C 54 5C 64 6C 74 7C	45 4D 55 5D 65 6D 75 7D	46 4E 56 5E 66 6E 76 7E	47 4F 57 5F 67 6F 77 7F
[EAX*4] [ECX*4] [EDX*4] [EBX*4] none [EBP*4] [ESI*4] [EDI*4]	10	000 001 010 011 100 101 110 111	80 88 90 98 A0 A8 B0 B8	81 89 91 99 A1 A9 B1 B9	82 8A 92 9A A2 AA BA	83 8B 93 9B A3 AB BB	84 8C 94 9C A4 AC BC	85 8D 95 9D A5 AD BD	86 8E 96 9E A6 AE BE	87 8F 97 9F A7 AF BF
[EAX*8] [ECX*8] [EDX*8] [EBX*8] none [EBP*8] [ESI*8] [EDI*8]	11	000 001 010 011 100 101 110 111	C0 C8 D0 D8 E0 E8 F0 F8	C1 C9 D1 D9 E1 E9 F1 F9	C2 CA D2 DA EA FA	C3 CB D3 DB EB FB	C4 CC D4 DC EC FC	C5 CD D5 DD ED FD	C6 CE D6 DE EE FE	C7 CF D7 DF EF FF

In the last example, we needed to use the 'none' field in the SIB byte because ESP wasn't an option for the base register. However, we can still use this ignorance when the base register is already an option in the MODR/M table.

In this slide, we are showing that we are using this encoding with EAX. Keep in mind that we can still use any of the 4 'none' bytes

## GRATUITOUS SIB

0800:0060	31 00	xor dword ptr [eax], eax
0800:0062	31 04 20	xor dword ptr [eax], eax
0800:0065	31 04 60	xor dword ptr [eax], eax
0800:0068	31 04 a0	xor dword ptr [eax], eax
0800:006b	31 04 e0	xor dword ptr [eax], eax

In this screenshot we first see how an assembler 'should' encode XOR [EAX], EAX. The last 4 instructions are the various ways we can encode it with the pointless 'none's in the SIB byte

**XOR [ESP \* 2], EAX [0XNOPE]**

Scaled Index
[EAX] [ECX] [EDX] [EBX] none [EBP] [ESI] [EDI]
[EAX*2] [ECX*2] [EDX*2] [EBX*2] none [EBP*2] [ESI*2] [EDI*2]
[EAX*4] [ECX*4] [EDX*4] [EBX*4] none [EBP*4] [ESI*4] [EDI*4]
[EAX*8] [ECX*8] [EDX*8] [EBX*8] none [EBP*8] [ESI*8] [EDI*8]

What's the exception to use ESP as a Scaled register? as we didn't notice it as an option in the SIB byte encodings. It's because you can't. You try to write this above instruction and your assembler will give you an error and make you feel bad.



## XOR [EBP + EAX \* 2], EAX [0X31444500]

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

rB(r/r) r16(r/r) r32(r/r) mm(r/r) xmm(r/r) (In decimal) /digit (Opcode) (In binary) REG =	Value of ModR/M Byte (in Hexadecimal)											
Effective Address	Mod	R/M	AL AX EAX MM0 XMM0 0 000	CL CX ECX MM1 XMM1 1 001	DL DX EDX MM2 XMM2 2 010	BL BX EBX MM3 XMM3 3 011	AH SP ESP MM4 XMM4 4 100	CH BP EBP MM5 XMM5 5 101	DH SI ESI MM6 XMM6 6 110	BH DI EDI MM7 XMM7 7 111		
[EAX] [ECX] [EDX] [EBX] [--][--] <sup>1</sup> disp32 <sup>2</sup> [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F		
[EAX]+disp8 <sup>3</sup> [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [--][--]+disp8 [EBP]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F		
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [--][--]+disp32 [EBP]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF		
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF		

This instruction has a base register of EBP and a scaled register of EAX \* 2. Vertically aligning the 2<sup>nd</sup> operand of EAX is easy. Since we are using a scaled register, we need to find the appropriate [--][--] line horizontally.

One would think that we would pick 0x04, but that is not the case, we need to pick 0x44 due to some EBP base register complications in the SIB byte that we are about to explore on the next slide

**XOR [EBP + EAX \* 2], EAX [0X31444500]**

Table 2-3. 32-Bit Addressing Forms with the SIB Byte

r32 (In decimal) Base = (In binary) Base =			EAX 0 000	ECX 1 001	EDX 2 010	EBX 3 011	ESP 4 100	ESI 6 110	EDI 7 111
Scaled Index	SS	Index	Value of SIB Byte (in Hexadecimal)						
[EAX]	00	000	00	01	02	03	04	05	06
[ECX]		001	08	09	0A	0B	0C	0D	0E
[EDX]		010	10	11	12	13	14	15	16
[EBX]		011	18	19	1A	1B	1C	1D	1E
none		100	20	21	22	23	24	25	26
[EBP]		101	28	29	2A	2B	2C	2D	2E
[ESI]		110	30	31	32	33	34	35	36
[EDI]		111	38	39	3A	3B	3C	3D	3E
[EAX*2]	01	000	40	41	42	43	44	45	46
[ECX*2]		001	48	49	4A	4B	4C	4D	4E

**NOTES:**

- The [\*] nomenclature means a disp32 with no base if the MOD is 00B. Otherwise, [\*] means disp8 or disp32 + [EBP]. This provides the following address modes:

MOD bits   Effective Address

00   [scaled index] + disp32

01   [scaled index] + disp8 + [EBP]

10   [scaled index] + disp32 + [EBP]

[EAX*8]	11	000	C0	C1	C2	C3	C4	C5	C6	C7
[ECX*8]		001	C8	C9	CA	CB	CC	CD	CE	CF
[EDX*8]		010	D0	D1	D2	D3	D4	D5	D6	D7
[EBX*8]		011	D8	D9	DA	DB	DC	DD	DE	DF
none		100	E0	E1	E2	E3	E4	E5	E6	E7
[EBP*8]		101	E8	E9	EA	EB	EC	ED	EE	EF
[ESI*8]		110	F0	F1	F2	F3	F4	F5	F6	F7
[EDI*8]		111	F8	F9	FA	FB	FC	FD	FE	FF

Lining up the horizontal line for the scaled register of EAX \* 2 is straight forward. However, we don't find an obvious EBP base register on the vertical line. It's the [\*] line that actually gives us what we need.

The [\*] line is dependent on the displacement option we pick from the MODR/M byte. There are only 3 variations; no displacement, 8-bit displacement, and 32-bit displacement. The results are as follows:

No displacement = [ScaledReg \* n + 0x11223344]

Disp8 = [EBP + ScaledReg \* n + 0x11]

Disp32 = [EBP + ScaledReg \* n + 0x11223344]

Either of the last 2 options would technically work, but we chose the 8-bit displacement option because it would get encoded in with 3 less bytes.

So finally, we arrive at the 0x45 byte in our table. However, we aren't done until we actually put the 0x00 byte at the end, because this is our 'invisible' displacement This means that our assembly would more literally be interpreted as such: XOR [EBP + EAX \* 2 + 0x00], EAX

## IMPLIED SCALE [\* 1]

- Consider `[eax + ecx]`
  - You can't have two base registers; one has to be scaled
- Assemblers viewed a 2<sup>nd</sup> 'base' register as scaled by '1'. So:
  - `[eax + ecx * 1]`

There are things we take for granted when only writing in a high level language like assembly. If you type a pointer like `[eax + ecx]`, the thing to consider is that there can only be one base register.

An assembler (like nasm) is going to look to your 2<sup>nd</sup> register to encode as the scaled register; the assembler will treat `[eax + ecx]` more literally as `[eax + ecx * 1]`. Or it will make ecx the scaled register and scale it by 1.

## CONVERT SCALED TO BASE

- Consider `[ecx * 1]`
  - Encoding for SIB requires more bytes
- If there is no base register already:
  - Assemblers will convert a scaled by '1' register as a base. So:
    - `[ecx]`

It's one thing to have something like `[ecx * 4]`. It is unambiguous: there is no base register and we need a scaled register of `ecx * 4`.

`[ecx * 1]` on the other hand, assemblers don't do what you asked for here. If you don't pick a base register, and your scaled register is scaled by one, your assembler is just going to make it the base register.

My instinct is to get annoyed with this, as my assembly is being interpreted into machine code that I didn't intend for, as I would have and could have written `[ecx]` if that's what I wanted. The reason an assembler is going to choose this because it takes less bytes to encode (because it doesn't need the SIB byte).

## ESP \* 1

- You CAN'T scale ESP
- You write `[eax + esp * 4]`, you get an error
- You write `[eax + esp * 1]` or `[eax + esp]`
  - You Dont?
- This is because the assembler converts it for you behind your back to:
  - `[esp + eax * 1]`

So we know that we can't use ESP as the scaled register. This is why if we write something like `[eax + esp * 4]` we will get an error. But why do we not get an error if we write `[eax + esp * 1]`?

Well, if you were to assemble this and then disassemble it, you would discover that your assembler actually writes this as `[esp + eax * 1]`.

In other words, if esp is scaled by only one, and the base register itself is not also esp, it will make the base register the scaled one so esp can join back in as the base. It logically does the same thing.



## IGNORES YOU, CHOOSES LESS BYTES SOMETIMES

- This is about the commutative property, it works with 6 of the 8 general purpose registers, like this:

→ 0804:8060	80 34 0b 00	xor byte ptr [ebx+ecx], 0
0804:8064	80 34 19 00	xor byte ptr [ecx+ebx], 0

- It does work with EBP, but differently:

→ 0804:8060	80 74 05 00 00	xor byte ptr [ebp+eax], 0
0804:8065	80 34 28 00	xor byte ptr [eax+ebp], 0

- And doesn't work with ESP, because ESP doesn't scale

Speaking of swapping around the registers, this is the commutative property in mathematics (because addition). We can do this no problem with eax, ecx, edx, ebx, esi, and edi.

esp is a register that can't be swapped, because of its scaling issues as previously discussed.

We also discussed the trade-off that needs to be made when using ebp in the SIB byte, so we do this at the cost of having to add the extra disp8 null.

However, the most interesting part of this is that if you use [ebp+eax] in your assembly, it will take you literally. If it did [eax + ebp] (logically the same), it would actually take 1 less byte to encode, but it doesn't opt for less machine code in this case. Just goes to show that sometimes an assembler optimizes for this kind of stuff, but not always.



## PUT A NULL IN IT



- If a pointer doesn't have a displacement, then put in a displacement of 0x00...same difference right

0800:0060	31 04 18	xor dword ptr [eax+ebx], eax
0800:0063	31 44 18 00	xor dword ptr [eax+ebx], eax

- If there's an 8 bit displacement, make it a 32 bit displacement with 3 bytes of leading nulls

0800:0067	31 44 18 42	xor dword ptr [eax+ebx+66], eax
0800:006b	31 84 18 42 00 00 00	xor dword ptr [eax+ebx+66], eax

For instructions that don't already have displacements, there's nothing from stopping us from being a troll and adding a displacement of nothing (0x00). We can add an 8-bit or a 32-bit displacement with nothing in it and the memory pointer would be logically the same.

Additionally, if we have an 8-bit displacement, we can 'upgrade' it to 32-bit by padding 3 null bytes in front of it.

## PUT A NULL IN IT W/ THE COMMUTATIVE PROPERTY TOO

- Add a null to it and swap registers

0800:006b	31 04 18	xor dword ptr [eax+ebx], eax
0800:006e	31 04 03	xor dword ptr [ebx+eax], eax
0800:0071	31 44 03 00	xor dword ptr [ebx+eax], eax

- Add 3 nulls to it and swap registers

0800:0075	31 44 18 42	xor dword ptr [eax+ebx+66], eax
0800:0079	31 44 03 42	xor dword ptr [ebx+eax+66], eax
0800:007d	31 84 03 42 00 00 00	xor dword ptr [ebx+eax+66], eax

Of course you can get creative and mix and match these redundancies.

This slide shows us mixing the 'null upgrade' with the commutative property

BASIC MODR/M REDUNDANCY						
3B /r	CMP r32, r/m32	RM	Valid	Valid	Compare r/m32 with r32.	
39 /r	CMP r/m32, r32	MR	Valid	Valid	Compare r32 with r/m32.	
3b c0	cmp eax, eax					
39 c0	cmp eax, eax					

This redundancy works because x86 generally has no instructions that allow for both operands to be a memory location in the same instruction.

For instance, if your instruction was 'mov', you could move a value of a register into a memory location, you could also move the value in a memory location into a register, but you could never move the value of a memory location into another memory location (with only one instruction).

Because of this, you need an encoding for each scenario. However, the operand that allows for a memory pointer also allows for it to just be a register as well (allowing register to register).

This means that both encodings allow for register to register. This is where the redundancy comes into play and why we can see something like the above screenshot.

# BASIC MODR/M REDUNDANCY

Table 2-2. 32-Bit Addressing Forms with the ModR/M Byte

r8(/r) r16(/r) r32(/r) mm(/r) xmm(/r) (in decimal) /digit (Opcode) (in binary) REG =			AL AX EAX MM0 XMM0 0 000	CL CX ECX MM1 XMM1 1 001	DL DX EDX MM2 XMM2 2 010	BL BX EBX MM3 XMM3 3 011	AH SP ESP MM4 XMM4 4 100	CH BP EBP MM5 XMM5 5 101	DH SI ESI MM6 XMM6 6 110	BH DI EDI MM7 XMM7 7 111
Effective Address	Mod	R/M	Value of ModR/M Byte (in Hexadecimal)							
[EAX] [ECX] [EDX] [EBX] [ ] disp32 [ESI] [EDI]	00	000 001 010 011 100 101 110 111	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	10 11 12 13 14 15 16 17	18 19 1A 1B 1C 1D 1E 1F	20 21 22 23 24 25 26 27	28 29 2A 2B 2C 2D 2E 2F	30 31 32 33 34 35 36 37	38 39 3A 3B 3C 3D 3E 3F
[EAX]+disp8 [ECX]+disp8 [EDX]+disp8 [EBX]+disp8 [ ]+disp8 [EBP]+disp8 [ESI]+disp8 [EDI]+disp8	01	000 001 010 011 100 101 110 111	40 41 42 43 44 45 46 47	48 49 4A 4B 4C 4D 4E 4F	50 51 52 53 54 55 56 57	58 59 5A 5B 5C 5D 5E 5F	60 61 62 63 64 65 66 67	68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	78 79 7A 7B 7C 7D 7E 7F
[EAX]+disp32 [ECX]+disp32 [EDX]+disp32 [EBX]+disp32 [ ]+disp32 [EBP]+disp32 [ESI]+disp32 [EDI]+disp32	10	000 001 010 011 100 101 110 111	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	90 91 92 93 94 95 96 97	98 99 9A 9B 9C 9D 9E 9F	A0 A1 A2 A3 A4 A5 A6 A7	A8 A9 AA AB AC AD AE AF	B0 B1 B2 B3 B4 B5 B6 B7	B8 B9 BA BB BC BD BE BF
EAX/AX/AL/MM0/XMM0 ECX/CX/CL/MM1/XMM1 EDX/DX/DL/MM2/XMM2 EBX/BX/BL/MM3/XMM3 ESP/SP/AH/MM4/XMM4 EBP/BP/CH/MM5/XMM5 ESI/SI/DH/MM6/XMM6 EDI/DI/BH/MM7/XMM7	11	000 001 010 011 100 101 110 111	C0 C1 C2 C3 C4 C5 C6 C7	C8 C9 CA CB CC CD CE CF	D0 D1 D2 D3 D4 D5 D6 D7	D8 D9 DA DB DC DD DE DF	E0 E1 E2 E3 E4 E5 E6 E7	E8 E9 EA EB EC ED EE EF	F0 F1 F2 F3 F4 F5 F6 F7	F8 F9 FA FB FC FD FE FF

In the previous slide it seemed like magic that we could just swap out the machine opcode and leave the operand data (0xC0) alone. This isn't always the case. With the different encodings, the vertical and horizontal parts of the table get swapped. But in the case of using the same register with itself, it's symmetric enough to not change the value in the table.

## NASMS INTERPRETIVE DANCE IN SIB

- Or how 'eax \* 2' is the same as 'eax + eax'
- And way more unusual things

This is another byte saving optimization.  
The next slide will follow the maze of the  
MODR/M + SIB byte to find out why



## NASMS INTERPRETIVE DANCE IN SIB

```
xor eax, [eax * 2]  
xor eax, [eax + eax]
```

```
33 04 00 | xor eax, dword ptr [eax+eax]  
33 04 00 | xor eax, dword ptr [eax+eax]
```

```
33 04 45 00 00 00 00 | xor eax, dword ptr [eax*2]
```

So in the top 2 screenshots, we are comparing two different assembly instructions to the machine code nasm outputs on the right. Notably, both instructions are converted to the `[eax + eax]` form. It is logically the same as `[eax * 2]`, what does nasm have against scaling `eax`?

It is because of the side effects of not having a base register when using SIB. You can have 'none' for a scaled register, but having 'none' (or `[*]`) for the base register comes at the cost of having to use a 32-bit displacement. This was covered a few slides back (the 3 options the `[*]` uses).

If we take `[eax * 2]` literally, it doubles our machine code for the instruction. Assemblers do not see this as ideal



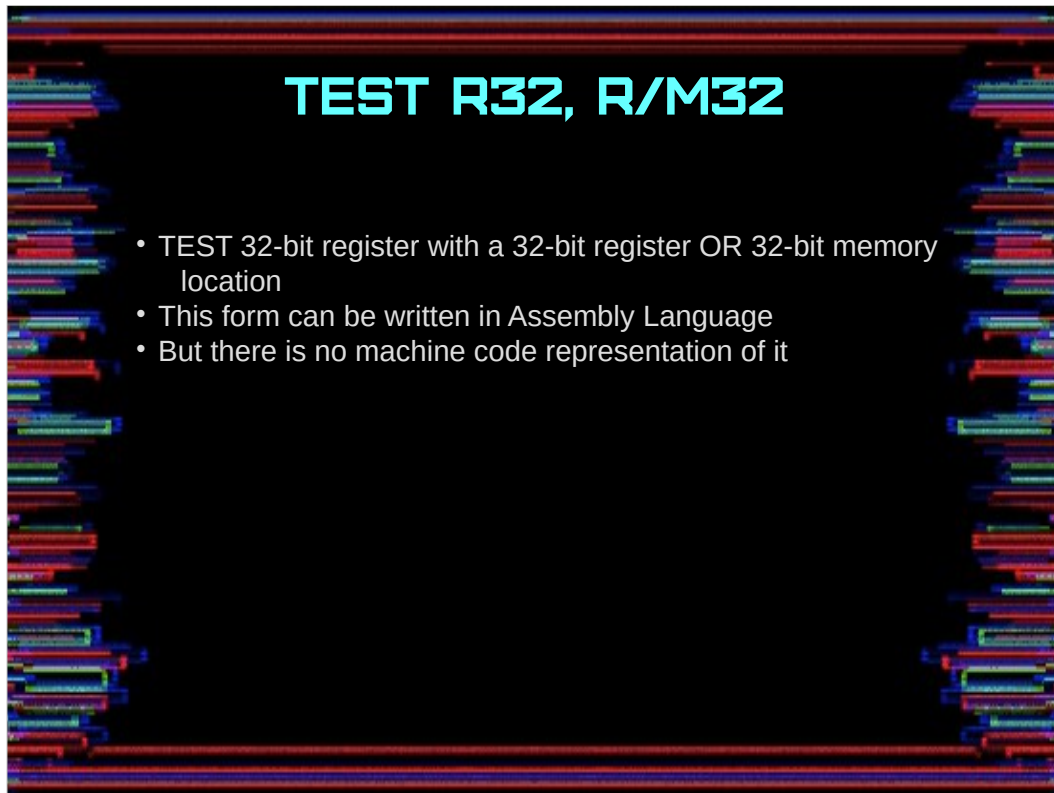


But what's really interesting is what kind of bullshit assemblers like nasm will put up with.

First of all, there is no scale of \* 5; only 1, 2, 4, and 8. But nasm is smart enough to look at this instruction and decide it is logically the same as  $eax + eax * 4$

Finally, scaling by something non-existent is one thing, but there is no such thing as subtraction in our pointer format, but it is valid assembly to nasm. Nasm is smart enough to look at  $[eax * 2 - eax]$  and know that it is pretty much the same thing as just  $[eax]$

I love nasm



I like this one. This slide is saying that you can write something in assembly like: `TEST EAX, [EAX]`

The thing is, there is no machine encoding to represent this. We previously discussed how we needed more than one encoding to mitigate being able to use a pointer for the source or destination. So what's going on here?

We will explore in the next couple slides

## CMP R32, R/M32

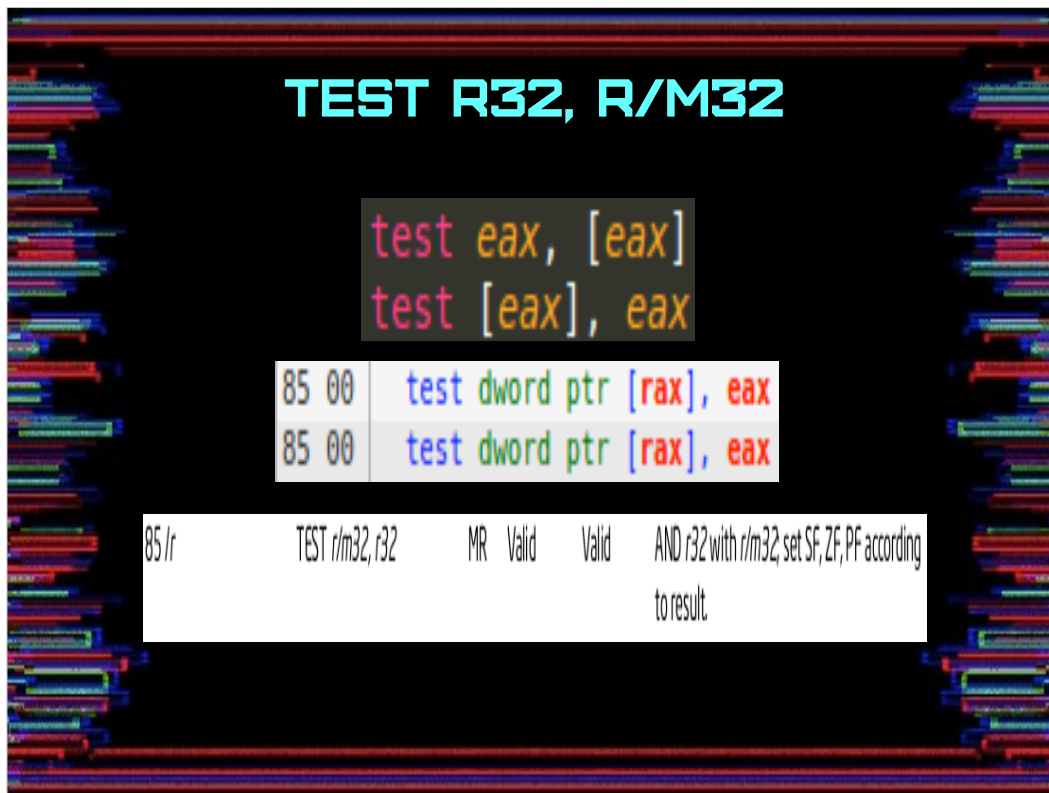
3B /r	CMP r32, r/m32	RM	Valid	Valid	Compare r/m32 with r32.
39 /r	CMP r/m32, r32	MR	Valid	Valid	Compare r32 with r/m32.

```
cmp eax, [eax]  
cmp [eax], eax
```

3b 00	cmp eax, dword ptr [rax]
39 00	cmp dword ptr [rax], eax

This slide shows the two different encodings of the cmp instruction with 32bit operands.

The last 2 screenshots compare the source assembly with the resulting machine-code in a debugger.



If we write the assembly shown on top, we get machine code comparable to the middle image.

What we see here is that the first instruction gets interpreted and converted by swapping the operands around to its only supported encoding. That is, Test r/m32, r32.

We see the encoding for this in the Intel manual (last image). Trust me, there is not corresponding encoding for the operands swapped around like other sane instructions.

So can we swap these operands and logically have the same results?

## BUT WHY?

- Review:
- $\text{CMP} = \text{SUB}$  (just for flags)
- $\text{TEST} = \text{AND}$  (just for flags)
- $5 - 3 = 8$
- $3 - 5 = -2$
- $5 \text{ AND } 3 = 1$
- $3 \text{ AND } 5 = 1$

The answer is yes. We compare CMP and TEST to see why.

Both of these instructions act like a math/logic instruction but without storing the result; it just does the instruction for the side effect.

CMP is like subtraction and TEST is like a logical AND. CMP doesn't SUB though, nor does TEST do an AND. They just set the flags so conditional jumps can have more intelligent behavior

If you try to do some commutative stuff, you see subtraction obviously isn't commutative, swapping the operands gives you different results.

TEST (and AND) on the other hand are commutative, swapping the operands gives the same result. Therefore you only really do need one encoding to represent both orders. So assemblers look at your un-encodable instruction and converts it into something that does the same thing



## REDUNDOSOURUS REX

30 c0	xor al, al
40 30 c0	xor al, al
42 30 c0	xor al, al
48 30 c0	xor al, al
4a 30 c0	xor al, al

This is just a 64-bit prefix hack. In order to access all of the extra registers that come with 64 bit processors, but also remain backwards compatible, Intel chose to prefix instructions with a byte that would change what the registers end up being.

Of course, some of the old registers are also encodable with the prefixes, and of course there are many redundancies to this; as the image of this slide demonstrates.

# REDUNDANT FENCING

## LFENCE—Load Fence

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
OF AE EB	LFENCE	NP	Valid	Valid	Serializes load operations.

## SFENCE—Store Fence

Opcode*	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
OF AE FB	SFENCE	NP	Valid	Valid	Serializes store operations.

## MFENCE—Memory Fence

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
OF AE FO	MFENCE	NP	Valid	Valid	Serializes load and store operations.

There are 3 different types of 'fence' instructions, each of them have the recommended machine code.

## REDUNDANT FENCING

```
section      .text
global      _start

_start:
    lfence
    sfence
    mfence
```

➔ 00000000:00400080	0f ae e8	lfence
00000000:00400083	0f ae f8	sfence
00000000:00400086	0f ae f0	mfence

We can see that the suggested machine code is dutifully used when comparing the assembly source and the machine code output from the disassembly

## REDUNDANT FENCING

→ 00000000:08000060	0f ae e8	lfence
00000000:08000063	0f ae e9	lfence
00000000:08000066	0f ae ea	lfence
00000000:08000069	0f ae eb	lfence
00000000:0800006c	0f ae ec	lfence
00000000:0800006f	0f ae ed	lfence
00000000:08000072	0f ae ee	lfence
00000000:08000075	0f ae ef	lfence
00000000:08000078	0f ae f8	sfence
00000000:0800007b	0f ae f9	sfence
00000000:0800007e	0f ae fa	sfence
00000000:08000081	0f ae fb	sfence
00000000:08000084	0f ae fc	sfence
00000000:08000087	0f ae fd	sfence
00000000:0800008a	0f ae fe	sfence
00000000:0800008d	0f ae ff	sfence
00000000:08000090	0f ae f0	mfence
00000000:08000093	0f ae f1	mfence
00000000:08000096	0f ae f2	mfence
00000000:08000099	0f ae f3	mfence
00000000:0800009c	0f ae f4	mfence
00000000:0800009f	0f ae f5	mfence
00000000:080000a2	0f ae f6	mfence
00000000:080000a5	0f ae f7	mfence

However, there is a lot of redundancy on this one. It so turns out that Intel suggests that this can be done with direct machine code. There's no real benefit to using any of these alternate encodings, however.

## INTEL SAYS THIS IS OKAY

Specification of the instruction's opcode above indicates a ModR/M byte of E8. For this instruction, the processor ignores the r/m field of the ModR/M byte. Thus, LFENCE is encoded by any opcode of the form 0F AE Ex, where x is in the range 8-F.

Specification of the instruction's opcode above indicates a ModR/M byte of F8. For this instruction, the processor ignores the r/m field of the ModR/M byte. Thus, SFENCE is encoded by any opcode of the form 0F AE Fx, where x is in the range 8-F.

Specification of the instruction's opcode above indicates a ModR/M byte of F0. For this instruction, the processor ignores the r/m field of the ModR/M byte. Thus, MFENCE is encoded by any opcode of the form 0F AE Fx, where x is in the range 0-7.

This is the part of the Intel manual that suggests you can use the extra 7 other end nibbles for these fence instructions.



## 'INST REG, IMM' REDUNDANCY

**CMP—Compare Two Operands**

Opcode	Instruction	Op/En	64-Bit Mode	Compat/Leg Mode	Description
<b>3C</b> <i>ib</i>	CMP <b>AL</b> , <i>imm8</i>	I	Valid	Valid	Compare <i>imm8</i> with AL.
<b>3D</b> <i>iw</i>	CMP AX, <i>imm16</i>	I	Valid	Valid	Compare <i>imm16</i> with AX.
<b>3D</b> <i>id</i>	CMP EAX, <i>imm32</i>	I	Valid	Valid	Compare <i>imm32</i> with EAX.
REX.W + <b>3D</b> <i>id</i>	CMP RAX, <i>imm32</i>	I	Valid	N.E.	Compare <i>imm32</i> sign-extended to 64-bits with RAX.
<b>80</b> <i>/7 ib</i>	CMP <b>r/m8</b> , <i>imm8</i>	MI	Valid	Valid	Compare <i>imm8</i> with r/m8.
REX + <b>80</b> <i>/7 ib</i>	CMP r/m8*, <i>imm8</i>	MI	Valid	N.E.	Compare <i>imm8</i> with r/m8.

In similar fashion to the very first redundancy explored in this presentation, there are many instructions that have an encoding for putting an immediate value into just the AL/AX/EAX register. This is because this register is so common, might as well have reduced machine code for it.

There is also the more generic encoding that allows for putting an immediate value into a MODR/M+SIB encodable operand. The redundancy comes in because AL/AX/EAX can be one of those options.

## 'INST REG, IMM' REDUNDANCY

14 55	adc al, 85	15 55 55 55 55	adc eax, 0x55555555
80 d0 55	adc al, 85	81 d0 55 55 55 55	adc eax, 0x55555555
04 55	add al, 85	05 55 55 55 55	add eax, 0x55555555
80 c0 55	add al, 85	81 c0 55 55 55 55	add eax, 0x55555555
24 55	and al, 85	25 55 55 55 55	and eax, 0x55555555
80 c0 55	add al, 85	81 e0 55 55 55 55	and eax, 0x55555555
3c 55	cmp al, 85	3d 55 55 55 55	cmp eax, 0x55555555
80 f8 55	cmp al, 85	81 f8 55 55 55 55	cmp eax, 0x55555555
0c 55	or al, 85	0d 55 55 55 55	or eax, 0x55555555
80 c8 55	or al, 85	81 c8 55 55 55 55	or eax, 0x55555555
1c 55	sbb al, 85	1d 55 55 55 55	sbb eax, 0x55555555
80 d8 55	sbb al, 85	81 d8 55 55 55 55	sbb eax, 0x55555555
2c 55	sub al, 85	2d 55 55 55 55	sub eax, 0x55555555
80 e8 55	sub al, 85	81 e8 55 55 55 55	sub eax, 0x55555555
34 55	xor al, 85	35 55 55 55 55	xor eax, 0x55555555
80 f0 55	xor al, 85	81 f0 55 55 55 55	xor eax, 0x55555555
a8 55	test al, 85	a9 55 55 55 55	test eax, 0x55555555
f6 c0 55	test al, 85	f7 c0 55 55 55 55	test eax, 0x55555555

This slide shows all of those redundancies

# REDUNDANT BIT INSTRUCTIONS

## RCL/RCR/ROL/ROR—Rotate

Opcode**	Instruction	Op/En	64-Bit Mode	Compat/Leg Mode	Description
D0 /2	RCL <i>r/m8</i> , 1	M1	Valid	Valid	Rotate 9 bits (CF, <i>r/m8</i> ) left once.
REX + D0 /2	RCL <i>r/m8*</i> , 1	M1	Valid	N.E.	Rotate 9 bits (CF, <i>r/m8</i> ) left once.
D2 /2	RCL <i>r/m8</i> , CL	MC	Valid	Valid	Rotate 9 bits (CF, <i>r/m8</i> ) left CL times.
REX + D2 /2	RCL <i>r/m8*</i> , CL	MC	Valid	N.E.	Rotate 9 bits (CF, <i>r/m8</i> ) left CL times.
C0 /2 <i>ib</i>	RCL <i>r/m8</i> , <i>imm8</i>	MI	Valid	Valid	Rotate 9 bits (CF, <i>r/m8</i> ) left <i>imm8</i> times.
REX + C0 /2 <i>ib</i>	RCL <i>r/m8*</i> , <i>imm8</i>	MI	Valid	N.E.	Rotate 9 bits (CF, <i>r/m8</i> ) left <i>imm8</i> times.
D1 /2	RCL <i>r/m16</i> , 1	M1	Valid	Valid	Rotate 17 bits (CF, <i>r/m16</i> ) left once.
D3 /2	RCL <i>r/m16</i> , CL	MC	Valid	Valid	Rotate 17 bits (CF, <i>r/m16</i> ) left CL times.
C1 /2 <i>ib</i>	RCL <i>r/m16</i> , <i>imm8</i>	MI	Valid	Valid	Rotate 17 bits (CF, <i>r/m16</i> ) left <i>imm8</i> times.
D1 /2	RCL <i>r/m32</i> , 1	M1	Valid	Valid	Rotate 33 bits (CF, <i>r/m32</i> ) left once.
REX.W + D1 /2	RCL <i>r/m64</i> , 1	M1	Valid	N.E.	Rotate 65 bits (CF, <i>r/m64</i> ) left once. Uses a 6 bit count.
D3 /2	RCL <i>r/m32</i> , CL	MC	Valid	Valid	Rotate 33 bits (CF, <i>r/m32</i> ) left CL times.
REX.W + D3 /2	RCL <i>r/m64</i> , CL	MC	Valid	N.E.	Rotate 65 bits (CF, <i>r/m64</i> ) left CL times. Uses a 6 bit count.
C1 /2 <i>ib</i>	RCL <i>r/m32</i> , <i>imm8</i>	MI	Valid	Valid	Rotate 33 bits (CF, <i>r/m32</i> ) left <i>imm8</i> times.
REX.W + C1 /2 <i>ib</i>	RCL <i>r/m64</i> , <i>imm8</i>	MI	Valid	N.E.	Rotate 65 bits (CF, <i>r/m64</i> ) left <i>imm8</i> times. Uses a 6 bit count.

Speaking of doing something so common that Intel provides a direct smaller machine code encoding for it; bitwise instructions like rotating and shifting are often done by just one bit. Because of this, there's a shortcut to have the immediate operand be just '1'.

There is also the more generic 8-bit immediate operand. But obviously '1' is a valid value in this encoding as well.

## REDUNDANT BIT INSTRUCTIONS

d0	d0		rcl	al,	1
c0	d0	01	rcl	al,	1
d1	d0		rcl	eax,	1
c1	d0	01	rcl	eax,	1
d0	d8		rcr	al,	1
c0	d8	01	rcr	al,	1
d1	d8		rcr	eax,	1
c1	d8	01	rcr	eax,	1
d0	c0		rol	al,	1
c0	c0	01	rol	al,	1
d1	c0		rol	eax,	1
c1	c0	01	rol	eax,	1
d0	c8		ror	al,	1
c0	c8	01	ror	al,	1
d1	c8		ror	eax,	1
c1	c8	01	ror	eax,	1
d0	f0		sal	al,	1
c0	f0	01	sal	al,	1
d1	f0		sal	eax,	1
c1	f0	01	sal	eax,	1
d0	f8		sar	al,	1
c0	f8	01	sar	al,	1
d1	f8		sar	eax,	1
c1	f8	01	sar	eax,	1
d0	e0		shl	al,	1
c0	e0	01	shl	al,	1
d1	e0		shl	eax,	1
c1	e0	01	shl	eax,	1
d0	e8		shr	al,	1
c0	e8	01	shr	al,	1
d1	e8		shr	eax,	1
c1	e8	01	shr	eax,	1

So this is the image of showing all of those redundancies

# BRANCH HINTS

PROGRAMMING WITH STREAMING SIMD EXTENSIONS 2 (SSE2)

## 11.4.5 Branch Hints

SSE2 extensions designate two instruction prefixes (2EH and 3EH) to provide branch hints to the processor (see "Instruction Prefixes" in Chapter 2 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*). These prefixes can only be used with the Jcc instruction and only at the machine code level (that is, there are no mnemonics for the branch hints).

74 fe	^ jz	0x0000000008048060
3e 74 fb	^ jz	0x0000000008048060

There's no real good reason to manually use a branch hint. There's also no way to do it directly with assembly.

However, you can manually machine the prefix in front of a branch instruction. It won't really affect much, but hey, you can (when you can't in assembly).



## INTEL HIDES SAL

- SAL = Shift Arithmetic Left
- Does the same thing as Shift Left (SHL)
- Therefore, everything is SHL

Similar to not having our assembly converting our TEST instruction to a equivalent form; SAL(Shift Arithmetic Left) gets converted to SHL(Shift Left). SAL and SHL are technically equivalent. The Intel manual recommends this and assemblers obey it.

The difference here is that there really is an encoding for SAL, and it is functional.

## INTEL HIDES SAL

```
1 ; Obligitory NASM stuff-----
2 section .text
3 global _start
4
5 _start:
6 ;-----
7 mov al, 55h ;init al register with 0x55
8 shl al, 1 ;logically shift bits to the left by 1
9 sal al, 1 ;'arithmetically' shift them to the left by 1
```

b0 55	mov al, 85
d0 e0	shl al, 1
d0 e0	shl al, 1

D0 /4	SHL r/m8, 1	M1	Valid	Valid	Multiply r/m8 by 2, once.
D0 /4	SAL r/m8, 1	M1	Valid	Valid	Multiply r/m8 by 2, once.

Here is our assembler converting our SAL instruction in assembly to SHL when it gets to machine code.

Note that even the machine code in the Intel manual is the same for SHL and SAL.

We will get to this next, but the /4 represents the specific instruction, where the D0 represents the group of instructions. For instance, /5 would be SHR (Shift Right).

# INTEL HIDES SAL

Opcode	Group	Mod 7,6	pfx	Encoding of Bits 5,4,3 of the ModR/M Byte (bits 2,1,0 in parenthesis)							
				000	001	010	011	100	101	110	111
80-83	1	mem, 1fB		ADD	OR	ADC	SBB	AND	SUB	XOR	CMP
8F	1A	mem, 1fB		POP							
C0,C1 reg, imm D0,D1 reg, 1 D2,D3 reg, CL	2	mem, 1fB		ROL	ROR	RCL	RCR	SHL/SAL	SHR		SAR

This table shows all of these /n numbers. We see that under '100' or /4, SHL and SAL are combined.

More interestingly, we notice that '110' or /6 is empty.


There is no way to mess around with this in assembly language, but we can do this directly in machine code to see what happens.



## USING SAL

d0 e0	shl al, 1
d0 f0	sal al, 1

b8 55 55 55 55	mov eax, 0x55555555
d0 f0	sal al, 1
d2 f0	sal al, cl
c0 f0 42	sal al, 66
66 d1 f0	sal ax, 1
66 d3 f0	sal ax, cl
66 c1 f0 42	sal ax, 66
d1 f0	sal eax, 1
d3 f0	sal eax, cl
c1 f0 42	sal eax, 66
48 d1 f0	sal rax, 1
48 d3 f0	sal rax, cl
48 c1 f0 42	sal rax, 66



ACHIEVEMENT UNLOCKED  
you can now use SAL instructions!

It is SAL. After testing it, it works. SAL unlocked!



## HIDDEN TEST

Opcode	Group	Mod 7,6	pfx	Encoding of Bits 5,4,3 of the ModR/			
				000	001	010	011
80-83	1	mem, 11B		ADD	OR	ADC	SBB
8F	1A	mem, 11B		POP			
C0, C1 reg, imm D0, D1 reg, 1 D2, D3 reg, CL	2	mem, 11B		ROL	ROR	RCL	RCR
F6, F7	3	mem, 11B		TEST Ib/Iz		NOT	NEG
FE	4	mem, 11B		INC Eb	DEC Eb		
FF	5	mem, 11B		INC Ev	DEC Ev	near CALL <sup>64</sup> Ev	far CALL Ep
0F 00	6	mem, 11B		SLDT Rv/Mw	STR Rv/Mw	LLDT Ew	LTR Ew
		mem		SGDT Ms	SIDT Ms	LGDT Ms	LIDT Ms

There's an encoding under the machine code of 0xF6 (8-bit) and 0xF7 (32-bit) for the TEST instruction, as in TEST EAX, 0x11223344.

We will use the 32-bit encoding for this example. This is a /0 encoding, to mean TEST, as in /2 would mean NOT and /3 would mean NEG and so on.

You'll notice there is a blank spot in this table that would have an instruction for /1. It so turns out that this is also a TEST instruction. If you machine encode this, the processor will run this exactly as the /0 test.

Your mileage will vary depending on the disassembler you use, for whether it tells you it is a TEST instruction or not...

## HIDDEN TEST

b8 00 00 0c d5	mov eax, 0xffffffffd50c0000
50	push rax
9d	popfd
b8 44 33 22 11	mov eax, 0x11223344
f7 c8	dw 0xc8f7
bb cc dd ee 90	mov ebx, 0xffffffff90eeddcc
90	nop
90	nop
90	nop

In the case of the EDB (Evans Debugger), the instruction is not disassembled showing the TEST it actually is. We instead see a dw (data word directive) of 0xc8f7 and then a mov instruction.

This 'mov' instruction will never run because it doesn't exist, it is actually part of the operand data of the TEST instruction. This instruction should be:

TEST EAX, 0xeedddccbb

This TEST instruction is what the processor will actually execute

## LOAD INEFFECTIVE ADDRESS

### LEA—Load Effective Address

Opcode	Instruction	Op/En	64-Bit Mode	Compat/Leg Mode	Description
8D /r	LEA r16,m	RM	Valid	Valid	Store effective address for m in register r16.
8D /r	LEA r32,m	RM	Valid	Valid	Store effective address for m in register r32.
REX.W + 8D /r	LEA r64,m	RM	Valid	N.E.	Store effective address for m in register r64.

00000000:08048060	b8 05 00 00 00	mov eax, 5
00000000:08048065	bb 1e 00 00 00	mov ebx, 30
00000000:0804806a	8d 44 d8 0a	lea eax, [rax+rbx*8+10]
00000000:0804806e	00 2e	add byte ptr [rsi], ch

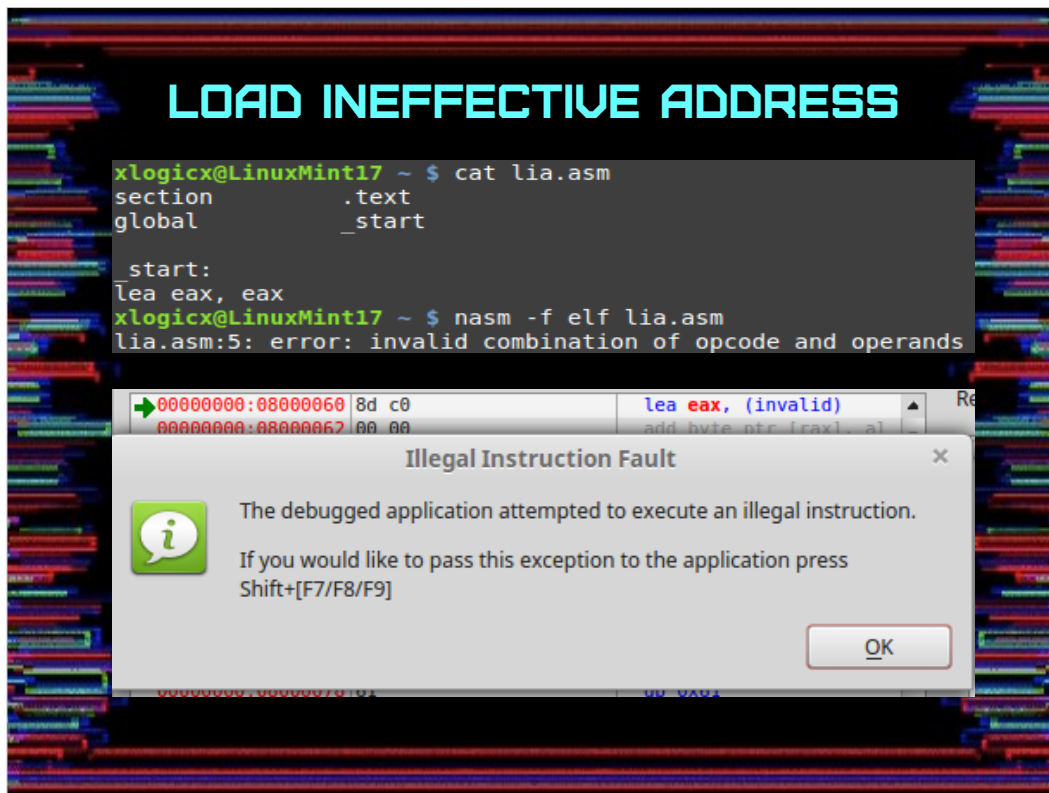
Registers  
General Purpose  
RAX: 00000000000000ff

What the Load Effective Address does is stores the pointer address into a register. So not the value of the address into the register, but the actual address that the pointer would point to.

In the above example, we are running: LEA EAX, [RAX + RBX \* 8 + 10].

Knowing EAX(RAX) is 5 and EBX(RBX) is 30 (decimal). So  $[5 + (30 * 8) + 10]$ . Simplify again to  $[5 + 240 + 10]$ . Finally, this simplifies to 255. In hex this is 0xff.

Note that RAX/EAX has 0xff as it's value after we run that LEA instruction. That's what LEA does in a nutshell. Compilers more often use this as a one instruction math hack.



Because of what this instruction does, it only makes sense to have a register as the dest operand and a pointer as the source operand.

However, the Encoding of the LEA instruction uses the MODR/M byte. This means that a register could be encoded with both operands (like and MODR/M based instruction).

If we try to do this in assembly, we get an error that we used an invalid combination of opcode and operands.

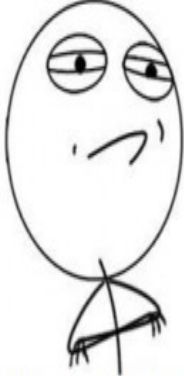
That doesn't stop us from directly encoding LEA EAX, EAX (8D C0).

However, all of this is fairly pointless as this instruction IS indeed invalid and will cause an error if it is executed. But in principle, this is a specific error that would be harder to achieve in assembly alone (without being able to machine hack)

# PREFIX ABUSE



BSWAP—Byte Swap					
Opcode	Instruction	Op/ En	64-bit Mode	Compat/ Leg Mode	Description
OF CB+rd	BSWAP r32	0	Valid*	Valid	Reverses the byte order of a 32-bit register.
REX.W + OF CB+rd	BSWAP r64	0	Valid	N.E.	Reverses the byte order of a 64-bit register.



Reverses the byte order of a 32-bit or 64-bit (destination) register. This instruction is provided for converting little-endian values to big-endian format and vice versa. To swap bytes in a word value (16-bit register), use the XCHG instruction. **When the BSWAP instruction references a 16-bit register, the result is undefined.**

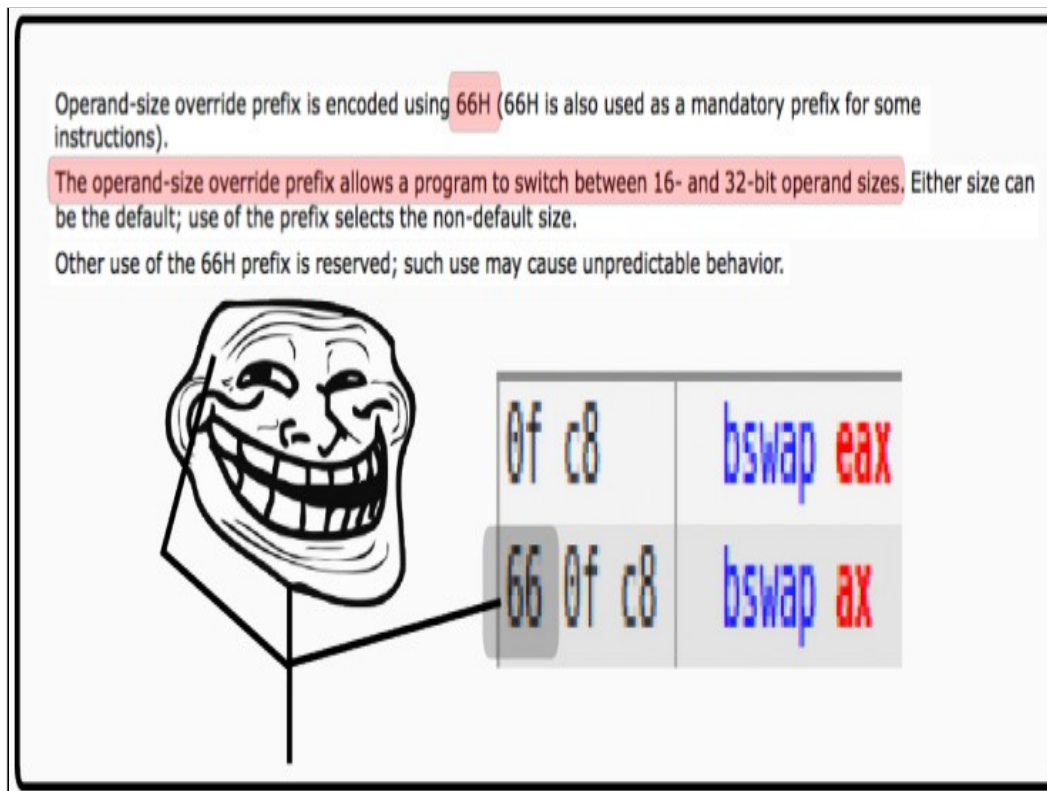
The BSWAP instruction can be used to reverse all of the bytes in a register. Notice that there is only an encoding for 64-bit and 32-bit registers, but not 16-bit registers. Even though 16-bits is enough bits to reverse 2 bytes. Why can't we do this?

Challenge accepted!



This is us in assembly attempting to write an instruction that uses bswap on a 16 bit register: BSWAP AX

Of course we get an error saying that we used an invalid combination of opcode and operands



In 32-bit x86 (64-bit is similar but not exactly the same), there are prefixes that modify the operand sizes. For many instructions there is no encoding for 16-bit instructions, just an encoding for 8-bit and 32-bit. In order to use a 16-bit encoding, you should use a 0x66 or 0x67 prefix before your instruction (depending on what part of the instruction you wanted to override)

So we put a 0x66 in front of our BSWAP EAX and achieve BSWAP AX.

It should be noted however that this instruction doesn't work as intended (in my experience, it just clears the register completely)

## REP PREFIX

For the following string instructions:

INS, MOVS, OUTS, LODS, STOS, CMPS,  
and SCAS

Ignored on all other instructions

except for repeating a NOP

```
1  section .text
2  global _start
3
4  _start:
5      rep nop
6      pause
```

0804:8060	f3 90	pause
0804:8062	f3 90	pause

The REP prefix can be used to repeat an instruction. This is really only intended to be used for instructions that operate on strings, so it doesn't do anything to any other instruction. The REP prefix byte is 0xF3

But there is one interesting exception, the screenshot shows these two different assembly instructions and how they mean the same thing to the processor.

# WHY

90	NOP	NP	Valid	Valid	One byte no-operation instruction.
F3 90	PAUSE	NP	Valid	Valid	Gives hint to processor that improves performance of spin-wait loops.

This is because for whatever reason, the pause instruction is machine encoded as 0xF390.

# CONSISTENT INSTRUCTION SIZES

The cool thing about this prefixes, is considering what would happen if you prefix a prefixed instruction with another of the same prefix. The answer is nothing. There is a limit to how many prefixes you can use; the instruction can be no larger than 15 bytes (you will get an error otherwise).

This screenshot shows some functional shellcode, and a couple of examples of the same code padded with prefixes. These examples make each instruction take the same amount of machine code bytes as every other instruction. I can't think of a reason why this would be useful, but it's still pretty cool.



## FULL OFFSETS

31 84 00 00 00 00 00 | xor dword ptr [rax+rax], eax

```
1 ; Obligatory NASM stuff-----  
2 section .text  
3 global _start  
4  
5 _start:  
6 ;-----  
7 xor [rax+rax], eax
```

31 04 00 | xor dword ptr [rax+rax], eax

Here's something interesting, looking at the top instruction, the disassembly says that the instruction is `xor [rax + rax], eax`

However, if we actually type that instruction and assemble it, we get the same disassembly, but different machine code.

What the hell is going on here?

This is just more of nasm's interpretive dance. Obviously we don't want the first instruction, this is just the 'put a null' in it trick. We obviously want the version with less bytes right?

# FULL OFFSETS

```
1 ; Obligitory NASM stuff-----  
2 section .text  
3 global _start  
4  
5 _start:  
6 ;-----  
7 xor [rax+rax*1 + 00000000h], eax
```

31 04 00	xor dword ptr [rax+rax], eax
----------	------------------------------

# MULTIBYTE NOP

0F 1F /0 NOP r/m32 M Valid Valid Multi-byte no-operation instruction.

Table 4-9. Recommended Multi-Byte Sequence of NOP Instruction

Length	Assembly	Byte Sequence
2 bytes	66 NOP	66 90H
3 bytes	NOP DWORD ptr [EAX]	0F 1F 00H
4 bytes	NOP DWORD ptr [EAX + 00H]	0F 1F 40 00H
5 bytes	NOP DWORD ptr [EAX + EAX*1 + 00H]	0F 1F 44 00 00H
6 bytes	66 NOP DWORD ptr [EAX + EAX*1 + 00H]	66 0F 1F 44 00 00H
7 bytes	NOP DWORD ptr [EAX + 00000000H]	0F 1F 80 00 00 00 00H
8 bytes	NOP DWORD ptr [EAX + EAX*1 + 00000000H]	0F 1F 84 00 00 00 00 00H
9 bytes	66 NOP DWORD ptr [EAX + EAX*1 + 00000000H]	66 0F 1F 84 00 00 00 00 00H

That is unless we don't.

The MultiByte NOP is the argument for not wanting our assembler to interpret our assembly into something optimized.

The MultiByte NOP allows for many different bytes because it takes advantage of how multibyte the MODR/M can be. The MODR/M argument doesn't actually contribute anything to the instruction in any meaningful way, it is just a dummy operand to add to the instruction size in a variable way.

So I'm going to take the suggested assembly in the intel manual and...

## MULTIBYTE NOP (SUGGESTED)

```
1  ; Obligitory NASM stuff-----
2  section      .text
3  global      _start
4
5  _start:
6  ;-----
7  db 0x66
8  nop
9  nop dword [eax]
10 nop dword [eax + 00h]
11 nop dword [eax + eax*1 + 00h]
12 nop word [eax + eax*1 + 00h]
13 nop dword [eax + 00000000h]
14 nop dword [eax + eax*1 + 00000000h]
15 nop word [eax + eax*1 + 00000000h]
```

...and I'm gonna put it in an assembly source file and assemble it with nasm...

## MULTIBYTE NOP [SUGGESTED]: TEH UNDERWHELM

66 90	nop
67 0f 1f 00	nop dword ptr [eax]
67 0f 1f 00	nop dword ptr [eax]
67 0f 1f 04 00	nop dword ptr [eax+eax]
66 67 0f 1f 04 00	nop dword ptr [eax+eax]
67 0f 1f 00	nop dword ptr [eax]
67 0f 1f 04 00	nop dword ptr [eax+eax]
66 67 0f 1f 04 00	nop dword ptr [eax+eax]

This is our result...

This for sure got an interpretive dance performed on it.

## MULTIBYTE NOP (SUGGESTED): W/O NULLS

```
1 ; Obligitory NASM stuff-----
2 section .text
3 global _start
4
5 _start:
6 ;-----
7 db 0x66
8 nop
9 nop dword [eax]
10 nop dword [eax + 00h]
11 nop dword [eax + eax*2 + 11h]
12 nop word [eax + eax*2 + 11h]
13 nop dword [eax + 11111111h]
14 nop dword [eax + eax*2 + 11111111h]
15 nop word [eax + eax*2 + 11111111h]
```

I next try to mitigate this by putting some non null offsets into the pointers, this prevents the assembler from optimizing them out.

Of course we are misadventuring from what Intel suggests...



## BETTER, BUT STILL SUCKS

66 90	nop
67 0f 1f 00	nop dword ptr [eax]
67 0f 1f 00	nop dword ptr [eax]
67 0f 1f 44 40 11	nop dword ptr [eax+eax*2+17]
66 67 0f 1f 44 40 11	nop dword ptr [eax+eax*2+17]
67 0f 1f 80 11 11 11 11	nop dword ptr [eax+0x11111111]
67 0f 1f 84 40 11 11 11 11	nop dword ptr [eax+eax*2+0x11111111]
66 67 0f 1f 84 40 11 11 11 11	nop dword ptr [eax+eax*2+0x11111111]

...but as you can see, it works a little bit better. But only a little bit.

## WHAT IT SHOULD LOOK LIKE, BUT HAD TO USE DIRECT MACHINE CODE

66 90	nop
0f 1f 00	nop dword ptr [rax]
0f 1f 40 00	nop dword ptr [rax]
0f 1f 44 00 00	nop dword ptr [rax+rax]
66 0f 1f 44 00 00	nop word ptr [rax+rax]
0f 1f 80 00 00 00 00	nop dword ptr [rax]
0f 1f 84 00 00 00 00 00	nop dword ptr [rax+rax]
66 0f 1f 84 00 00 00 00 00	nop word ptr [rax+rax]

To get the (exact) machine code advertized in the Intel manual, I could find no other way but to manually program this in machine code



But why go through any of that trouble!

I'd rather just be ignorant and prefix up a normal NOP

## SELF MODIFYING CODE

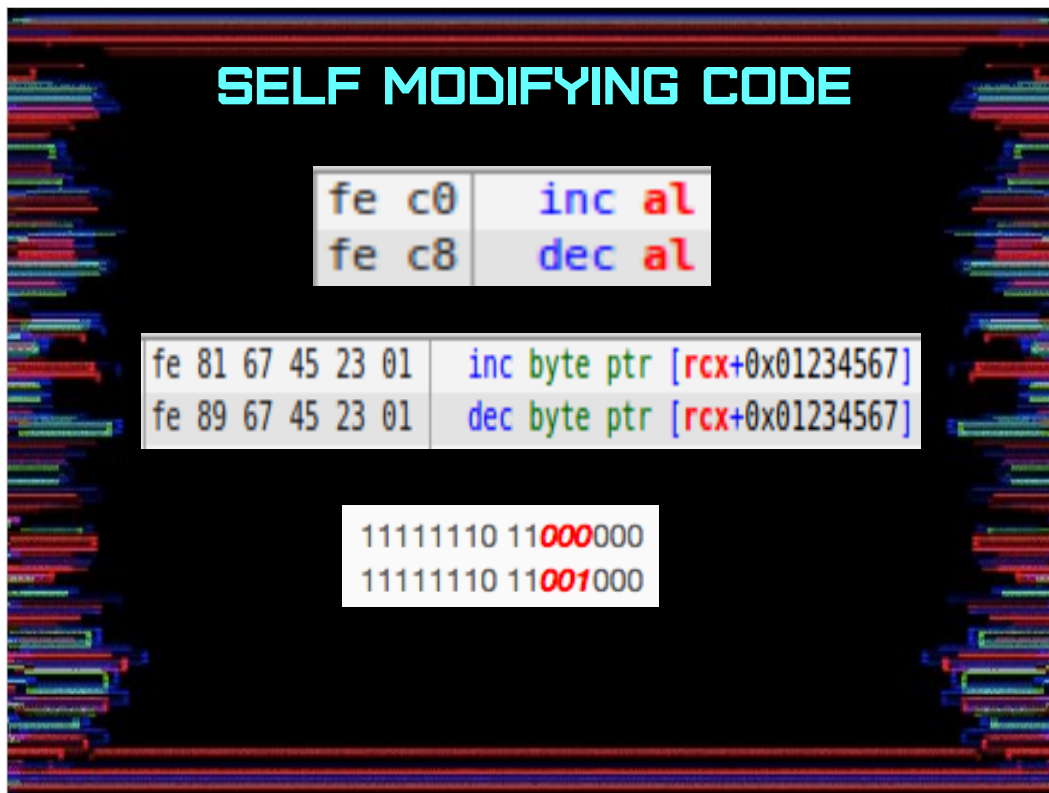
with basic arithmetic

Because similar machine code formats

FE /0	INC r/m8	M	Valid	Valid	Increment r/m byte by 1.
FE /1	DEC r/m8	M	Valid	Valid	Decrement r/m8 by 1.

Ignoring stuff like exploit development, an understanding of machine code can also be extremely useful for self modifying code. There are MANY different strategies/techniques a programmer could take to achieve cool self modifying code. We will only really explore one PoC example here.

For this example, we can ADD a value to a [pointer] that happens to be the memory location of another instruction. Instructions with the /n format have the instruction itself encoded in the number of /n. For example, INC is 0xFE /0 and DEC is 0xFE /1. If we just added the right number to the right location of the INC instruction, it would be convertible to a DEC instruction.

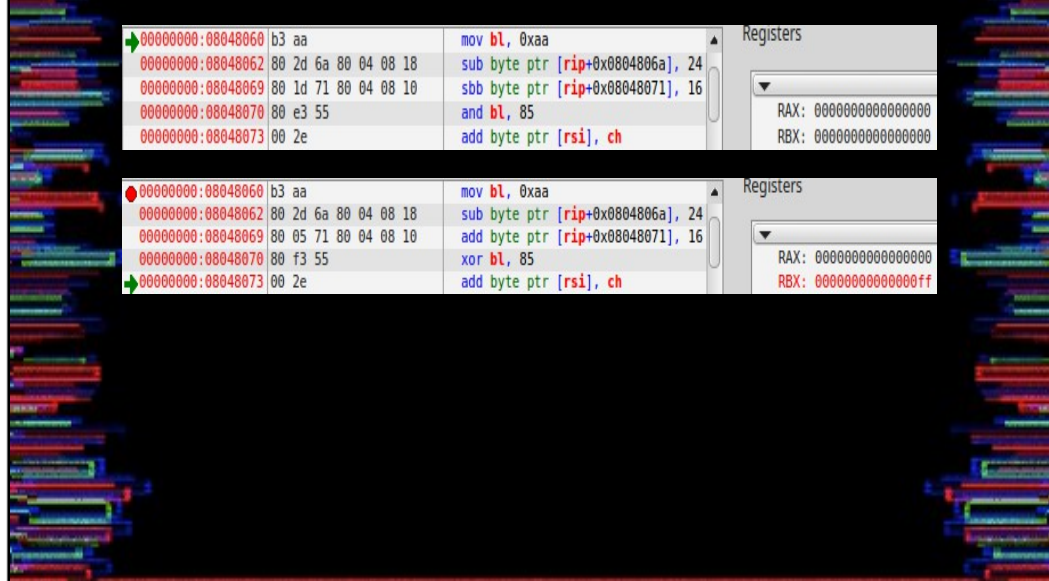


This slide shows the machine code and assembly to show the very small differences.

The last image shows the machine code of the first image in binary isolating out the 3 bits that control which instruction it is.

In red, the 000 means INC and the 001 means DEC. The difference to the 2 instruction is just one bit.


## SELF MODIFYING CODE DEMO



This demo will show a series of 3 instructions that are using this trick. When you get to the 3<sup>rd</sup> instruction, it isn't the same instruction it looked like before the program ran.

These 2 screenshots are more for the benefit of the PDF version of these slides. Time permitting, a live demo of this will be done during the presentation.

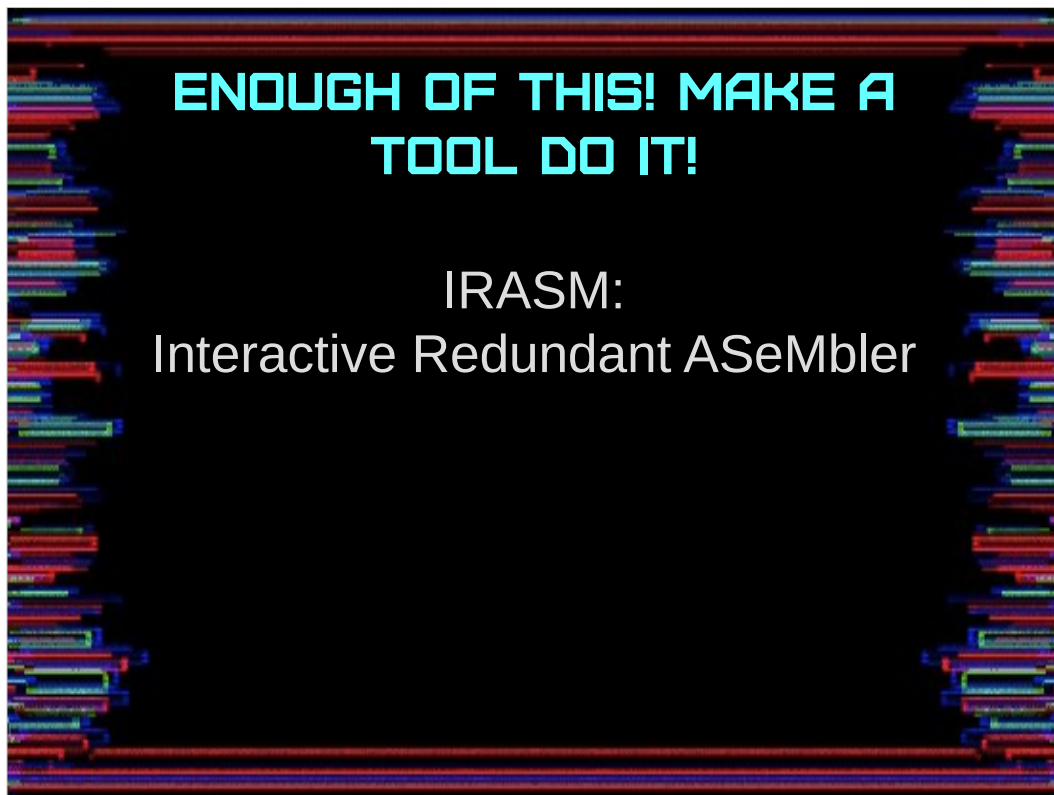




CACTUSCON 2017 - BOOT AND PLAY

I will be giving a talk at CactusCon 2017 in September called Boot and Play. It is about 512 byte boot sector programs that are games and puzzles.

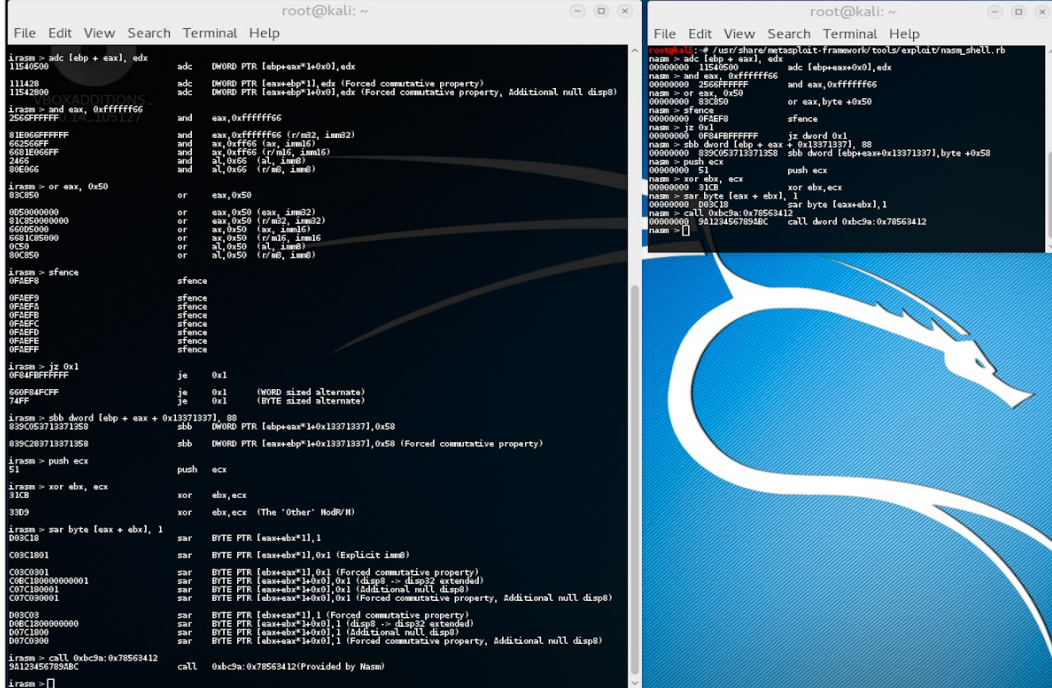
Self modifying code is a nice trick to have in the bag because it helps get the byte count down. The above trick that I mentioned is a trick that I use in TronSolitaire (<https://github.com/XlogicX/tronsolitaire>)



This is another 'demo' slide. This is where I demonstrate what the demo can do.

Hint: it pretty much does everything with the concepts described in this whole talk. It's like `nasm_shell`, but it outputs many other valid variations of machine code that represents the same assembly input.

# PDF VERSION ONLY

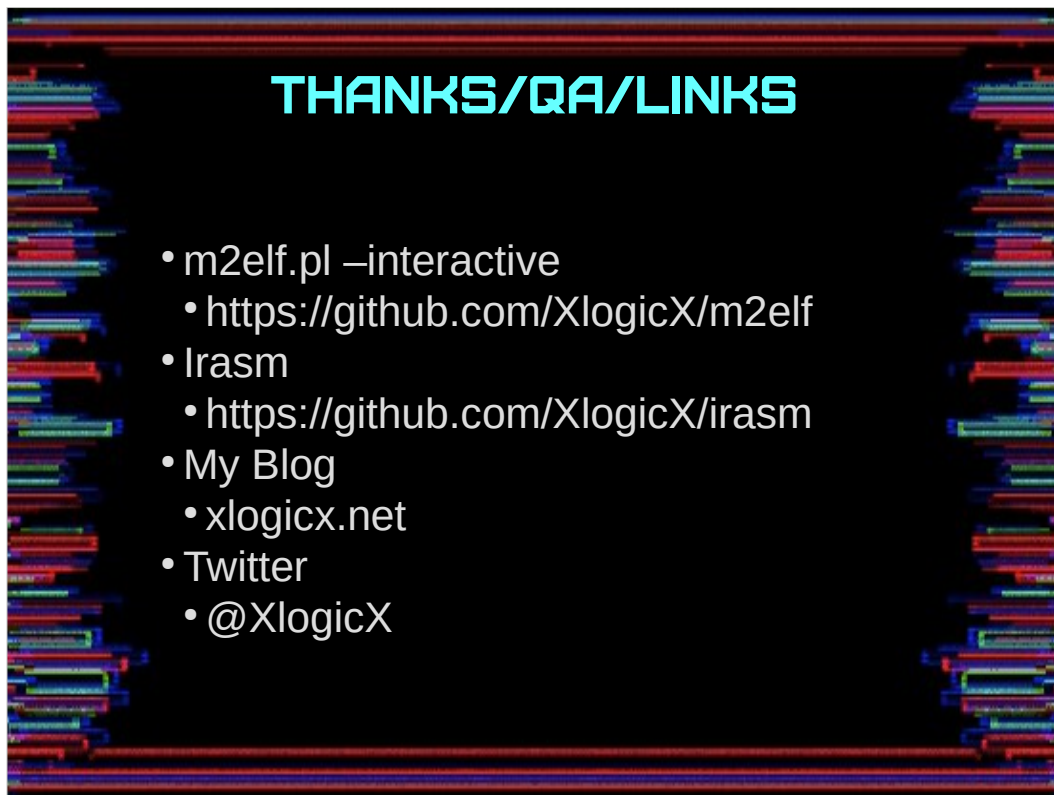


```
root@kali: ~  
File Edit View Search Terminal Help  
irasm -> adc [ebp + eax], edx  
11E40500      adc      DWORD PTR [ebp+eax*1+0x0],edx  
11E42800      adc      DWORD PTR [eax+ebp*1],edx (Forced commutative property)  
11E42800      adc      DWORD PTR [eax+ebp*1+0x0],edx (Forced commutative property, Additional null disp8)  
25000000      and      eax, 0xffffffff  
81E00000      and      eax, 0xffffffff (r/m2, imm32)  
6C250000      and      eax, 0xffff (ax, imm16)  
6C250000      and      eax, 0xffff (r/m16, imm16)  
24000000      and      al, 0x65 (al, imm8)  
90C050      and      al, 0x65 (r/m8, imm8)  
irasm -> or eax, 0x50  
8ACB50      or      eax, 0x50  
00C00000      or      eax, 0x50 (eax, imm32)  
81C0500000      or      eax, 0x50 (r/m32, imm32)  
6600C050      or      ax, 0x50 (ax, imm16)  
6681C05000      or      ax, 0x50 (r/m16, imm16)  
0C50      or      al, 0x50 (al, imm8)  
80C050      or      al, 0x50 (r/m8, imm8)  
irasm -> sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
0FA0F0      sfdene  
irasm -> jz 0x1  
0FA0F0      jz      0x1  
660FA0F0      jz      0x1 (WORD sized alternate)  
74FF      jz      0x1 (BYTE sized alternate)  
irasm -> sub dword [ebp + eax + 0x13371337], 88  
83C053713371358      sub      DWORD PTR [ebp+eax*1+0x13371337],0x58  
83C053713371358      sub      DWORD PTR [eax+ebp*1+0x13371337],0x58 (Forced commutative property)  
irasm -> push ecx  
51      push    ecx  
irasm -> xor ebx, ecx  
31CB      xor      ebx, ecx  
3109      xor      ebx, ecx (The 'Other' ModRM)  
irasm -> sar byte [eax + ebx], 1  
00C110      sar      BYTE PTR [eax+ebx*1],1  
00C11001      sar      BYTE PTR [eax+ebx*1],0x1 (Explicit imm8)  
00C11001      sar      BYTE PTR [eax+ebx*1],0x1 (Forced commutative property)  
00C11000000001      sar      BYTE PTR [eax+ebx*1+0x0],0x1 (disp8 -> disp32 extended)  
00C1100001      sar      BYTE PTR [eax+ebx*1+0x0],0x1 (Additional null disp8)  
00C1100001      sar      BYTE PTR [eax+ebx*1+0x0],0x1 (Forced commutative property, Additional null disp8)  
00C11003      sar      BYTE PTR [eax+ebx*1],1 (Forced commutative property)  
00C11000000000      sar      BYTE PTR [eax+ebx*1+0x0],1 (disp8 -> disp32 extended)  
00C11000      sar      BYTE PTR [eax+ebx*1+0x0],1 (Additional null disp8)  
00C11000      sar      BYTE PTR [eax+ebx*1+0x0],1 (Forced commutative property, Additional null disp8)  
irasm -> call 0x78563412  
341234567856C      call     0x78563412(Provided by Name)  
irasm ->
```

```
root@kali: ~  
File Edit View Search Terminal Help  
nasmshell: # /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb  
nasm -> adc [ebp + eax], edx  
00000000 11E40500      adc      [ebp+eax*0x0],edx  
nasm -> and eax, 0xffffffff  
00000000 25000000      and      eax, 0xffffffff  
nasm -> or eax, 0x50  
00000000 8ACB50      or      eax, byte +0x50  
nasm -> sfdene  
00000000 0FA0F0      sfdene  
nasm -> jz 0x1  
00000000 0FA0F0      jz      dword 0x1  
nasm -> sub dword [ebp + eax + 0x13371337], 88  
00000000 83C053713371358      sub      dword [ebp+eax+0x13371337],byte +0x58  
nasm -> push ecx  
00000000 51      push    ecx  
nasm -> xor ebx, ecx  
00000000 31CB      xor      ebx, ecx  
nasm -> sar byte [eax + ebx], 1  
00000000 00C110      sar      byte [eax+ebx],1  
nasm -> call 0x78563412  
00000000 341234567856C      call     dword 0x78563412  
nasm ->
```

This slide wont be displayed in the main presentation, instead I will demo the tool live, but since the PDF version can't do that, this is a screenshot showing irasm side by side with nasmshell. The same assembly instructions are entered into both, you see the left hand side is more verbose.





I tend to speak fairly quick and am good at time management, so I may have time for questions. It really depends on this years DEF CON policy on Q/A. Regardless, I will make myself available for more in depth Q/A in the hangout room after I deliver the talk.

This slide is more just to leave up the links to the tools and my contact info / blog