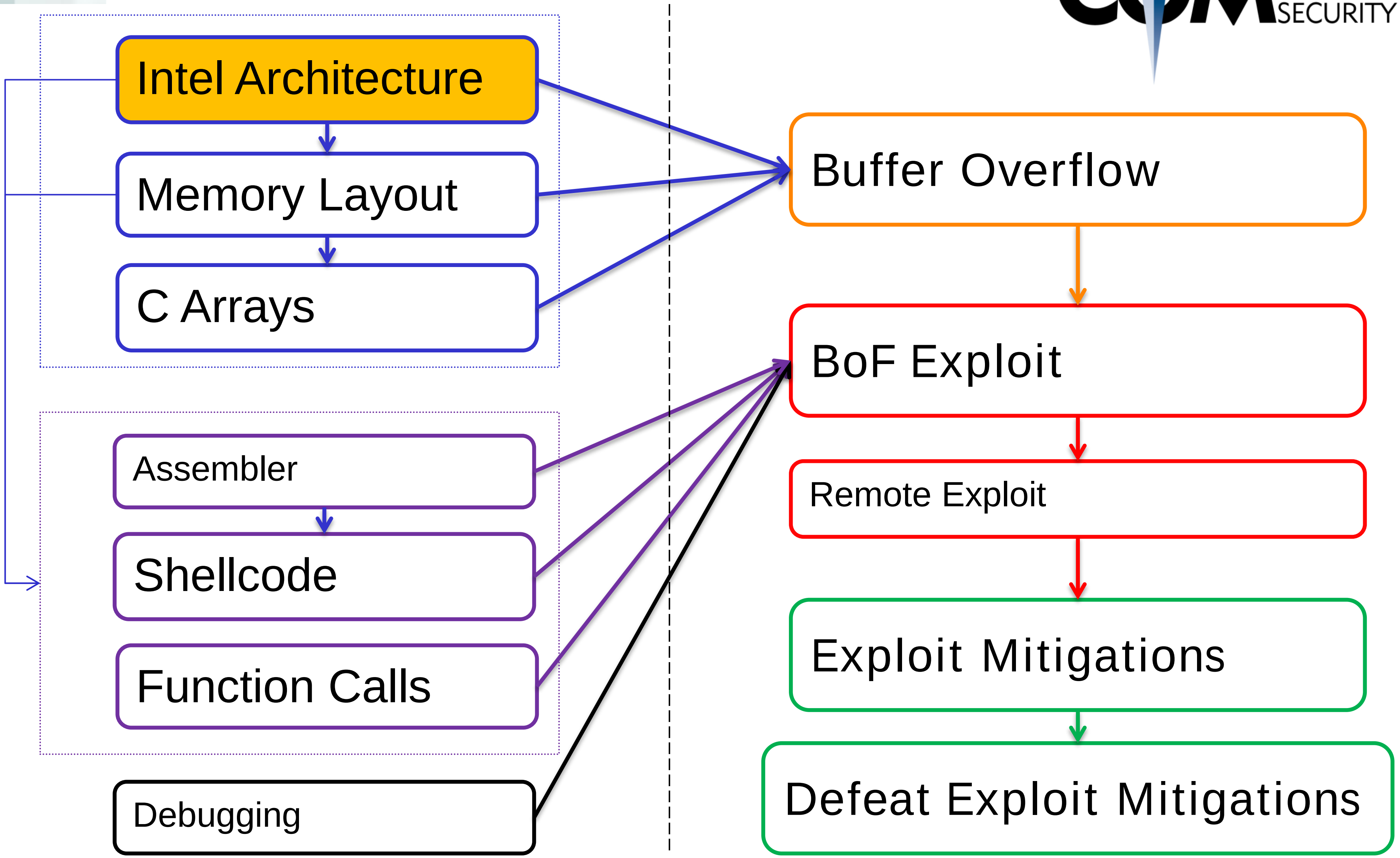
Intel Architecture

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Content


Intel Architecture
Memory Layout
C Arrays
Assembler
Shellcode
Function Calls
Debugging
Buffer Overflow
BoF Exploit
Remote Exploit
Exploit Mitigations
Defeat Exploit Mitigations

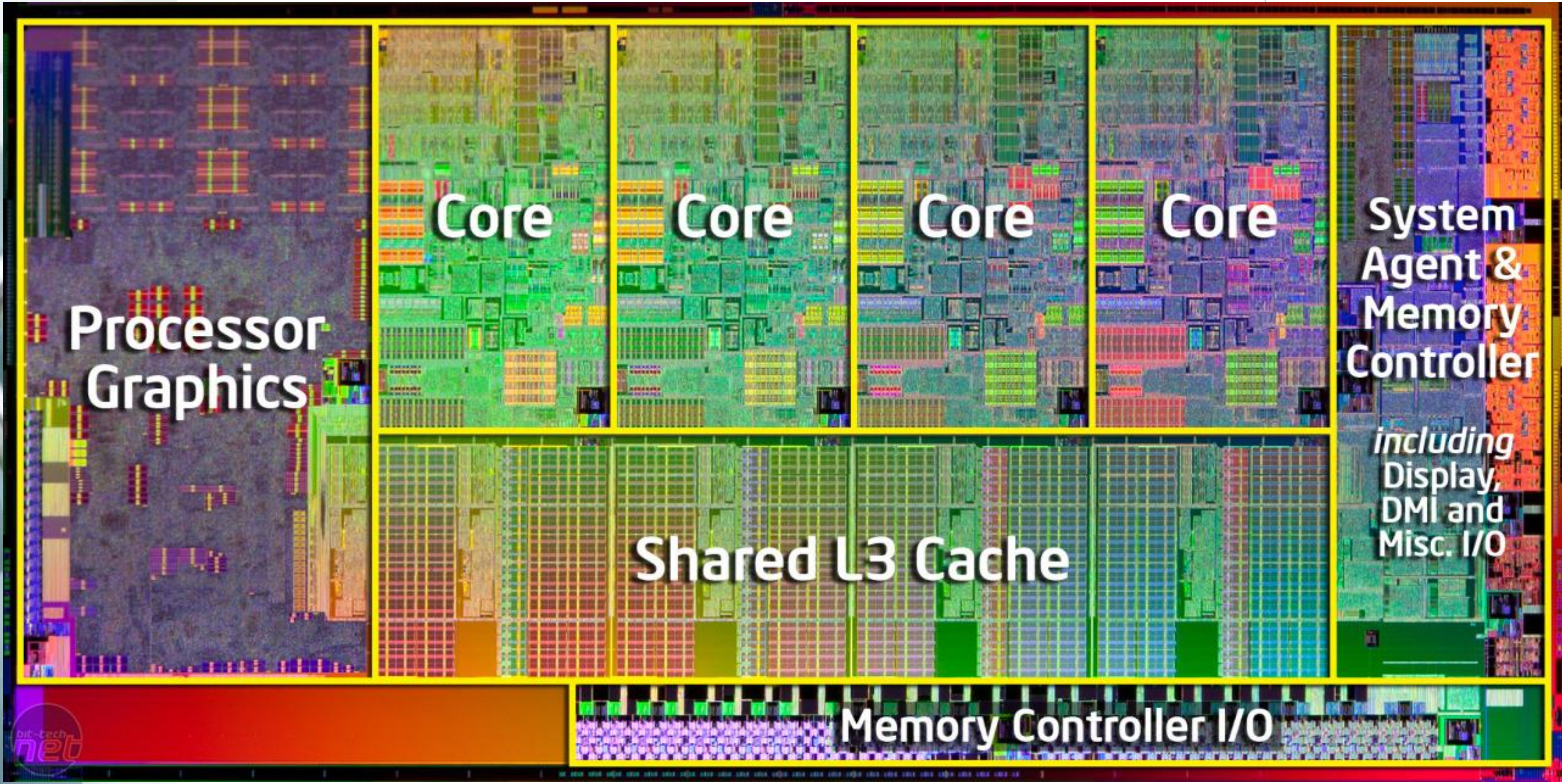
Intel Architecture
Intel CPU

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

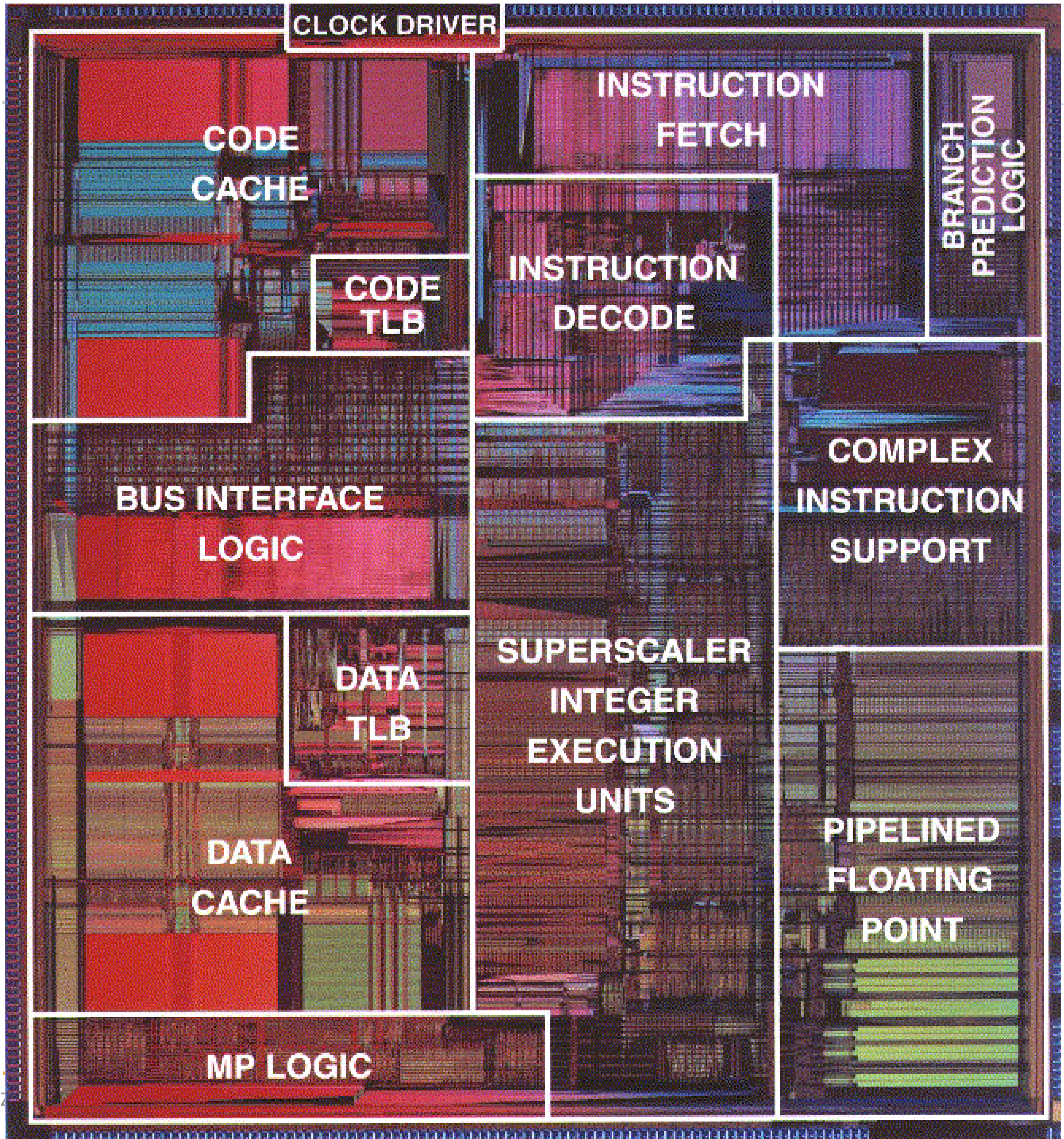
Intel CPU

Intel CPU

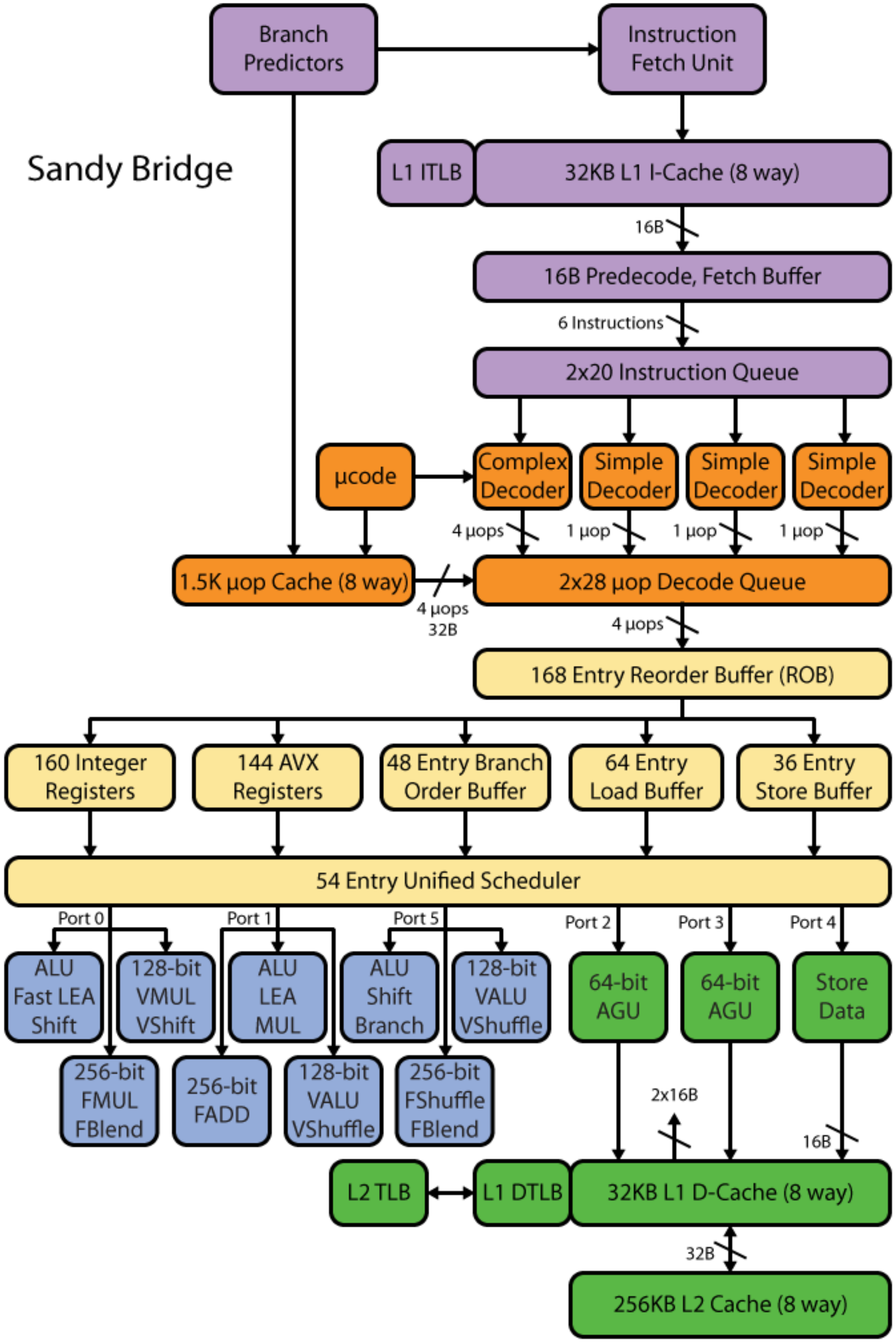

Processor Graphics
Core
Core
Core
Core
System Agent & Memory Controller
including Display, DMI and Misc. I/O
Shared L3 Cache
Memory Controller I/O
bit-tech.net

Intel CPU

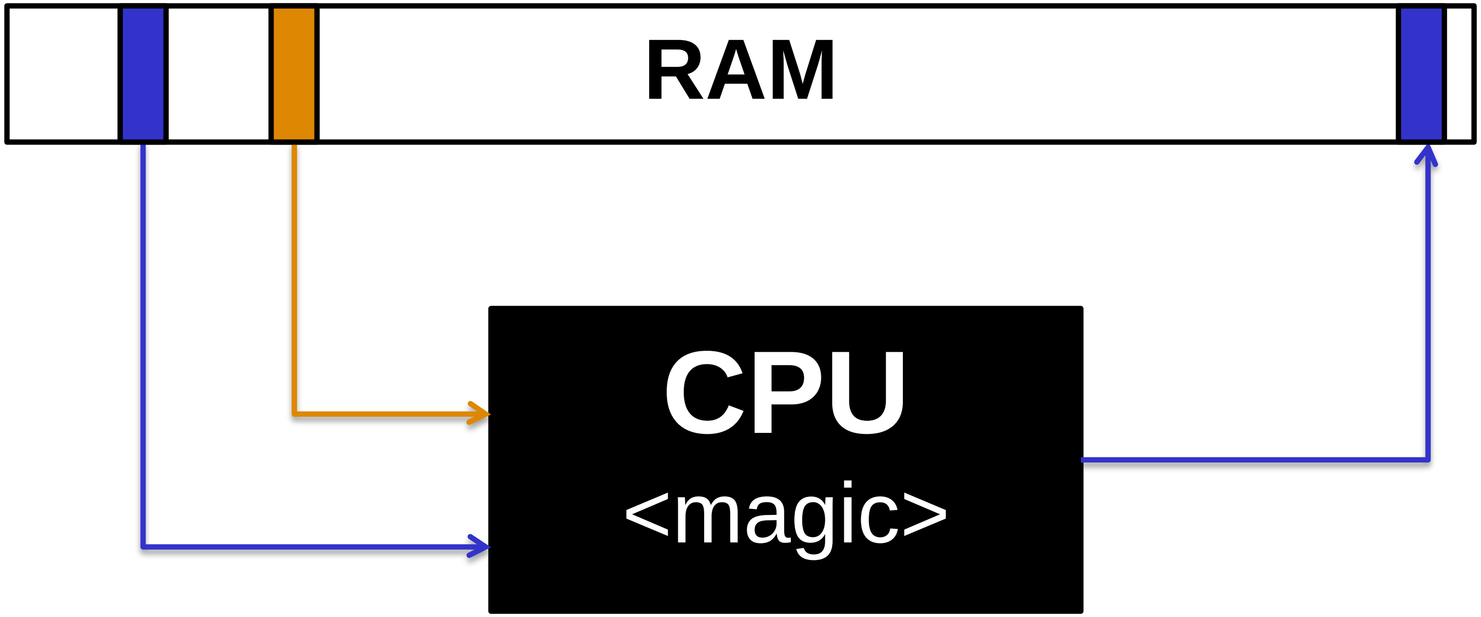
Pentium Die



Sandy Bridge



Overview: Computerz



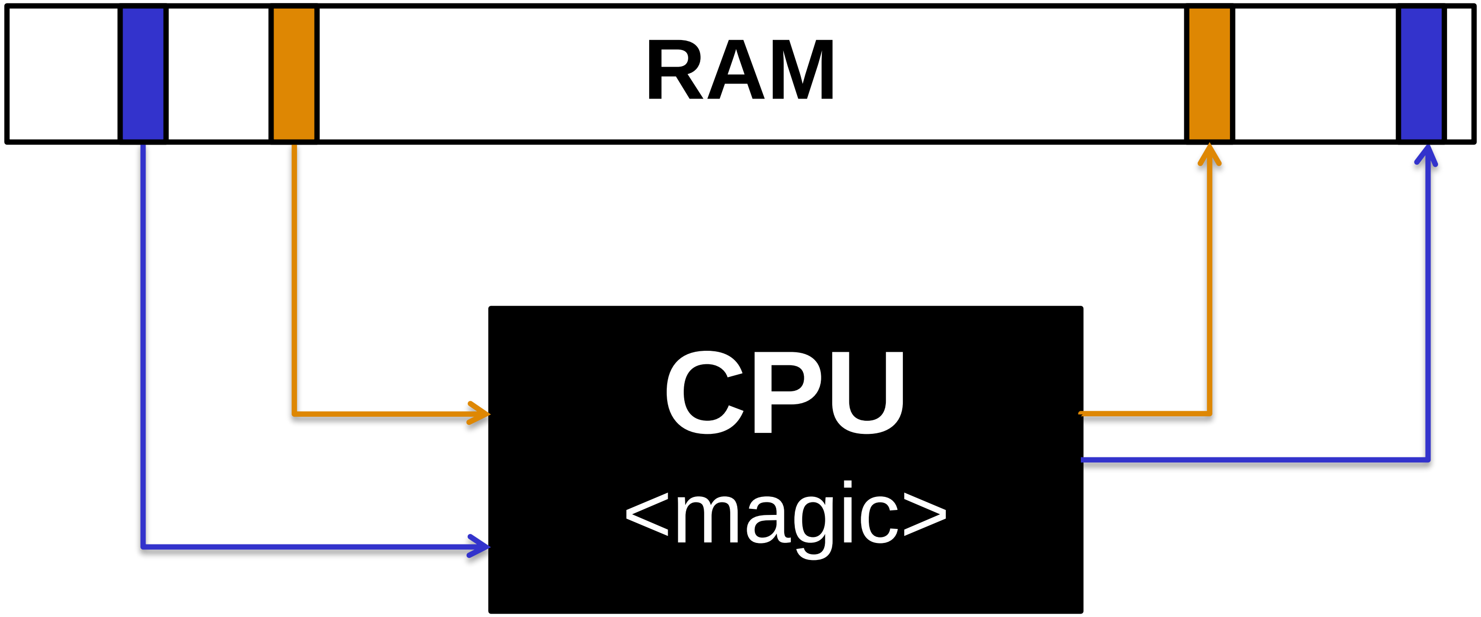
Read:

- Data
- Instructions

Write:

- Data

von Neumann Architecture



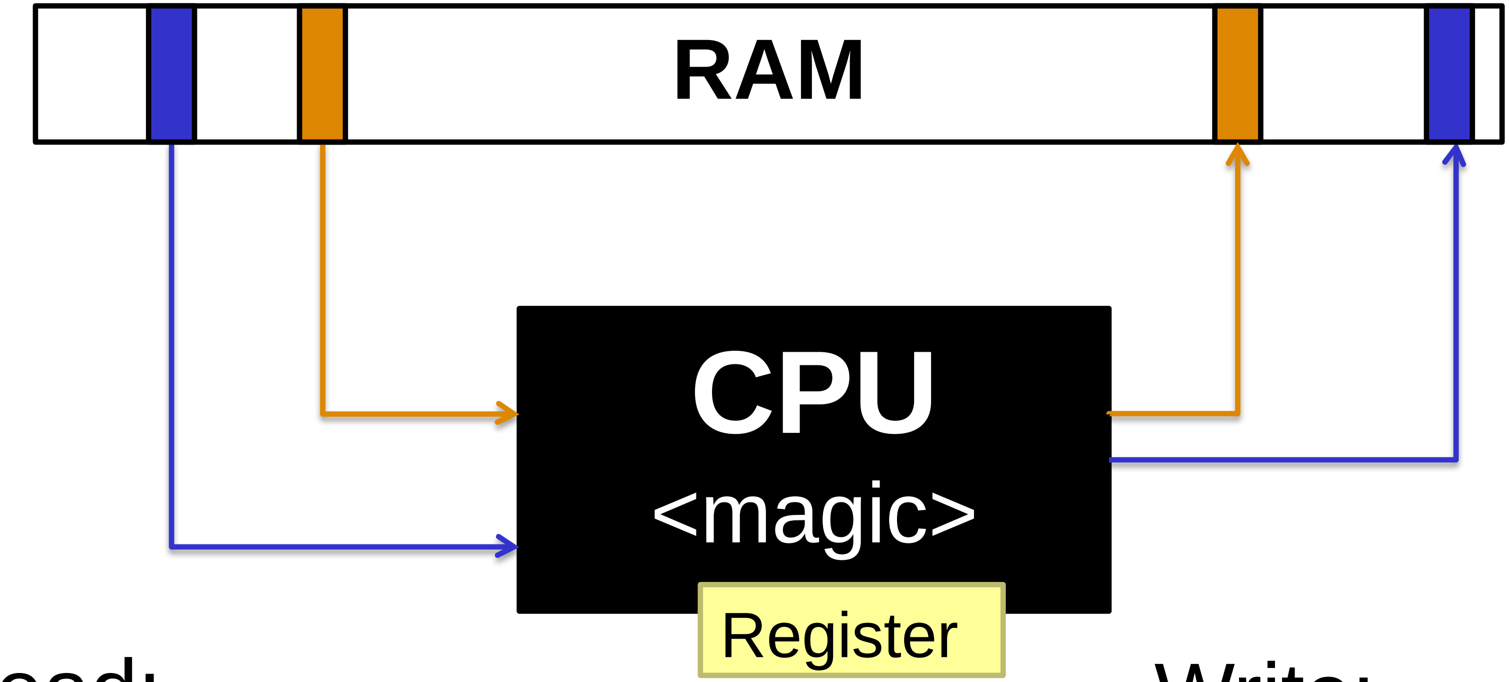
Read:

- Data
- Instructions

Write:

- Data
- Instructions

Overview: Computerz



Read:

- Data
- Instructions

Write:

- Data
- Instructions

Overview: CPU Registers

Register are the “variables” on the CPU

Immediate access for the CPU

Cannot write Memory -> Memory

- Always: Memory -> Register -> Memory

Register: <1 cycle
L1: ~3
L2: ~14
RAM: ~240

Overview: CPU Registers

Register can hold:

- Data (numbers)
- Addresses (also numbers, but with a different meaning)

Registers can do:

- Perform computations
- Read / Write memory
- Execute instructions

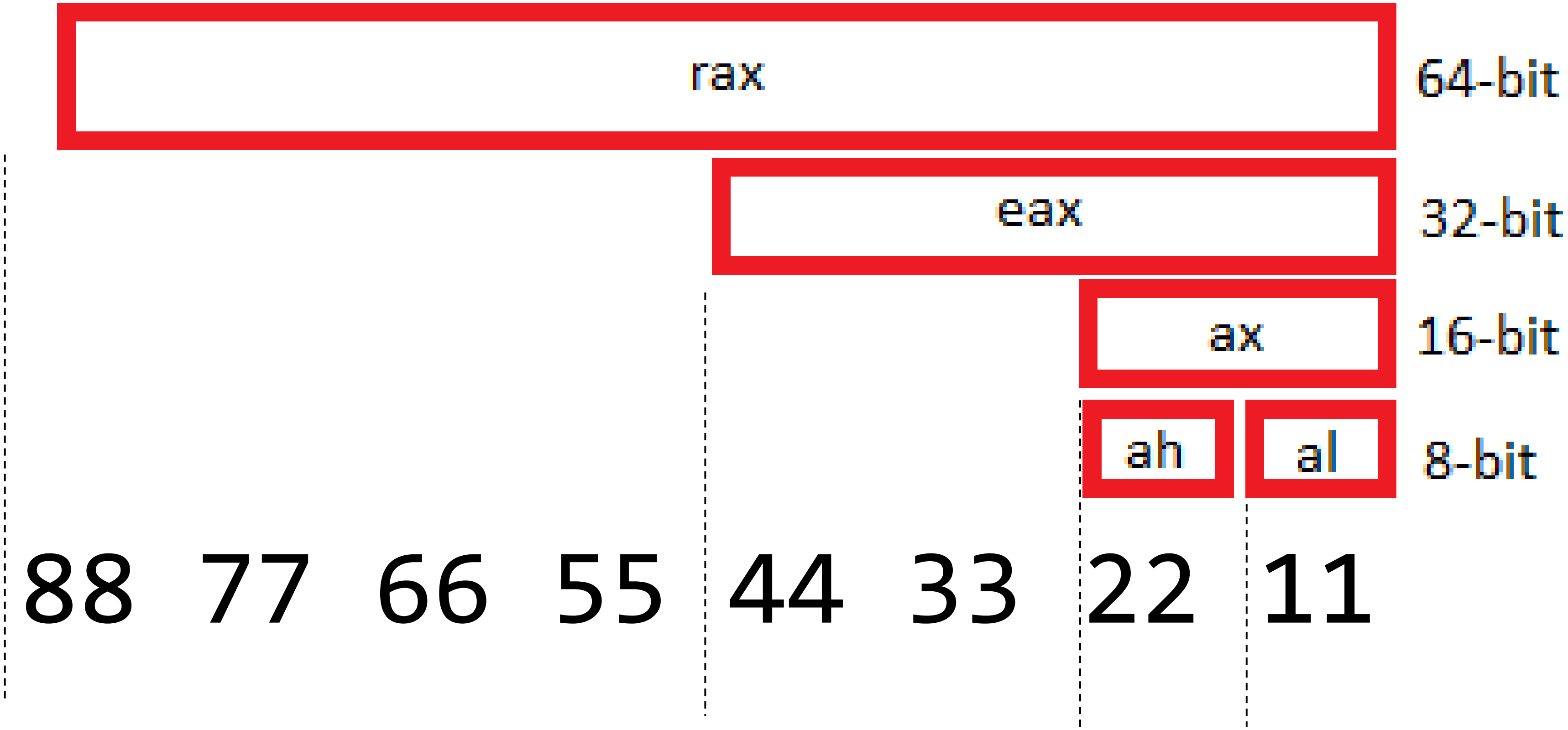
Overview: CPU Registers

32	64	Acronym	
EAX	RAX	Accumulator	Adding stuff
EBX	RBX	Base	Referencing stuff
ECX	RCX	Count	Counting stuff
EDX	RDX	Data	Stuff
ESI	RSI	Source Index	Points to a source
EDI	RDI	Destination Index	Points to a destination
	R8-R15		General Purpose

Overview: CPU Registers

32	64	Acronym	Points to?
EIP	RIP	Instruction Pointer	Next instruction to be executed
ESP	RSP	Stack Pointer	Top of Stack
EBP	RBP	Base Pointer	Current Stack Frame (Bottom)

Overview: CPU Registers



Overview: CPU Registers

Fun Fact: Current Intel CPU's are compatible to the 8086

8086:

- From 1978
- 5-10mhz

Overview: CPU Registers

Recap:

- CPU work with registers
- Registers can hold data
- Registers can also hold addresses of memory locations (to write data to)
- They can be 32 bit (**E**AX) or 64 bit (**R**AX)
- Some registers are multi-purpose
- Some registers are special (RIP, RBP, RSP)

Hex Numbers, and Little Endian

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Hex Numbers, and Little Endian

Intel CPU’s

- 1 Byte = 8 Bit
- Little endian

Hex Numbers, and Little Endian

Intel CPU's

- 1 Byte = 8 Bit
- Little endian

Others:

- CDC 6000: 18, 24 and 60 bit
- PDP1/9/15: 18 bit words

- ARM an dother RISC: Big Endian

Hex Numbers

Hex: 0 1 2 3 4 5 6 7 8 9 A B C D E F

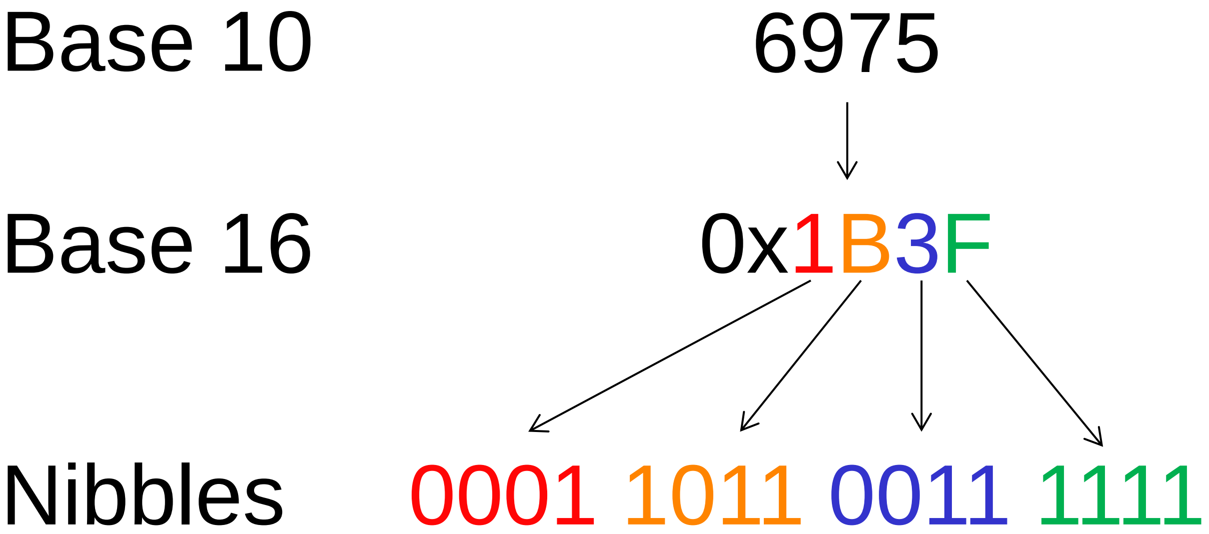
1 hex digit: 16 values (4 bit)

2 hex digits: 256 values

16 * 16 = 256

1 Byte = 8 Bit = 256 values!

Hex Numbers

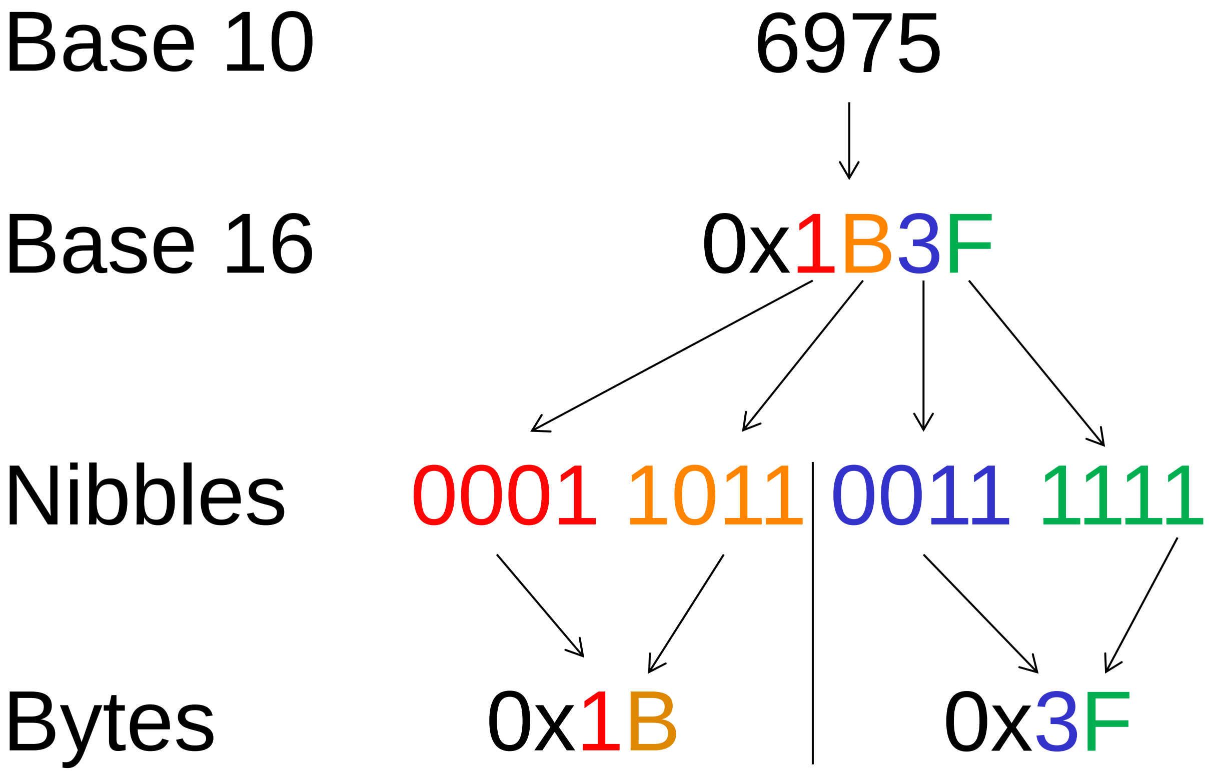


Base 10 6975

Base 16 0x1B3F

Nibbles 0001 1011 0011 1111

Hex Numbers



Base 10 6975

Base 16 0x1B3F

Nibbles 0001 1011 | 0011 1111

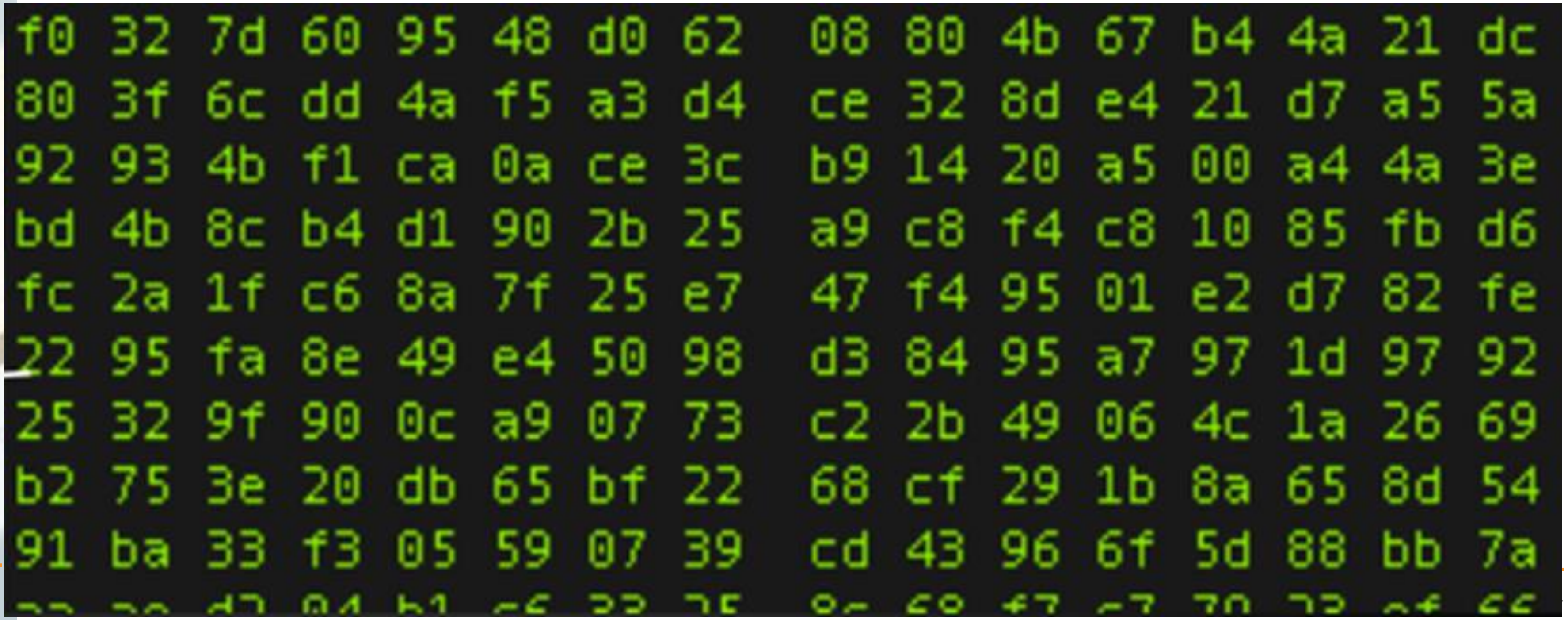
Bytes 0x1B | 0x3F

Endianness

Number: 0x1B3F

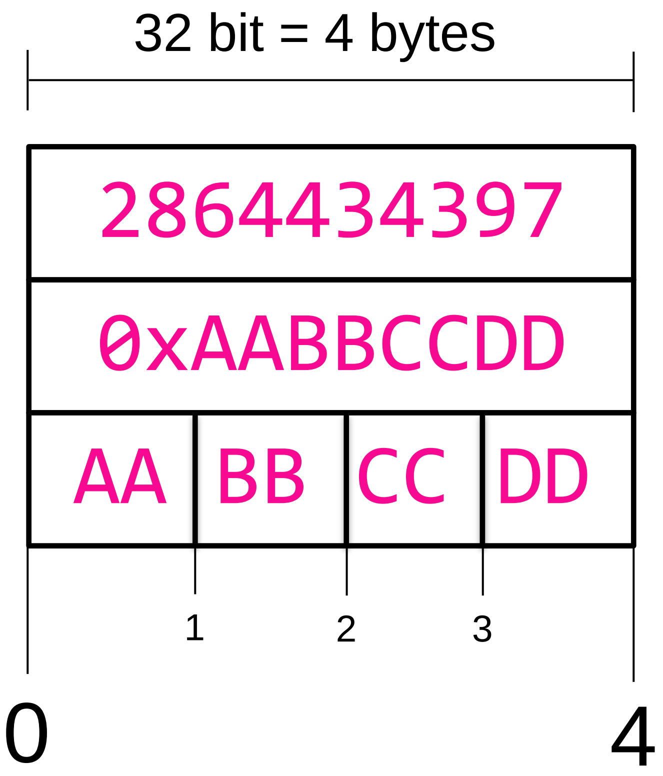
Big Endian: 0x1B 0x3F

Little Endian: 0x3F 0x1B



```
f0 32 7d 60 95 48 d0 62  08 80 4b 67 b4 4a 21 dc
80 3f 6c dd 4a f5 a3 d4  ce 32 8d e4 21 d7 a5 5a
92 93 4b f1 ca 0a ce 3c  b9 14 20 a5 00 a4 4a 3e
bd 4b 8c b4 d1 90 2b 25  a9 c8 f4 c8 10 85 fb d6
fc 2a 1f c6 8a 7f 25 e7  47 f4 95 01 e2 d7 82 fe
22 95 fa 8e 49 e4 50 98  d3 84 95 a7 97 1d 97 92
25 32 9f 90 0c a9 07 73  c2 2b 49 06 4c 1a 26 69
b2 75 3e 20 db 65 bf 22  68 cf 29 1b 8a 65 8d 54
91 ba 33 f3 05 59 07 39  cd 43 96 6f 5d 88 bb 7a
```

Endianness: Big Endian (ARM)



32 bit = 4 bytes

2864434397

0xAABBCCDD

AA	BB	CC	DD

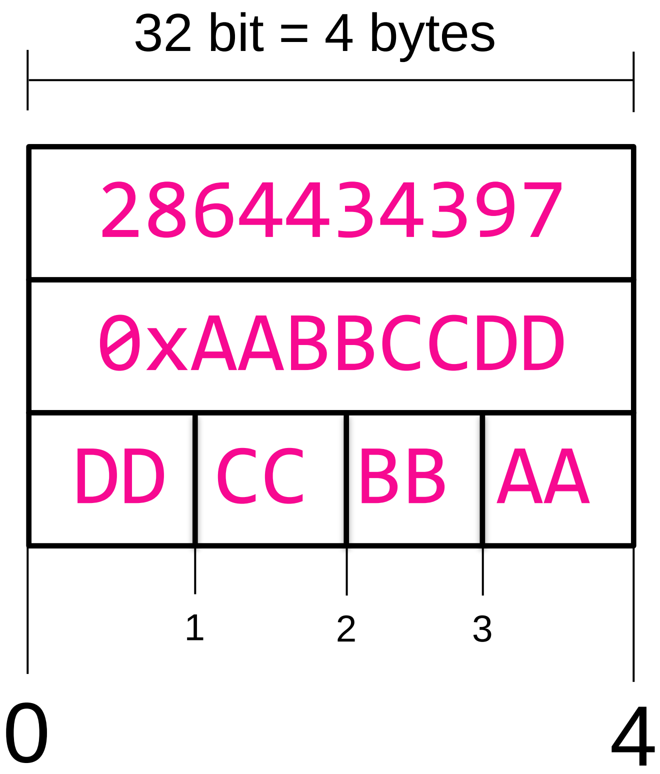
0 1 2 3 4

Number in Decimal (10)

Number in Hex (16)

Big Endian Storage

Endianness: Little Endian (Intel)



32 bit = 4 bytes

2864434397

0xAABBCCDD

DD	CC	BB	AA

Number in Decimal (10)

Number in Hex (16)

Little Endian Storage

Endianness: Little Endian (Intel)

DD	CC	BB	AA

Four 8 bit numbers:

- DD
- CC
- BB
- AA

Two 16 bit numbers:

- 0xCCDD
- 0xAABB

A 32 bit number:

- 0xAABBCCDD

??

Endianness: Little endian

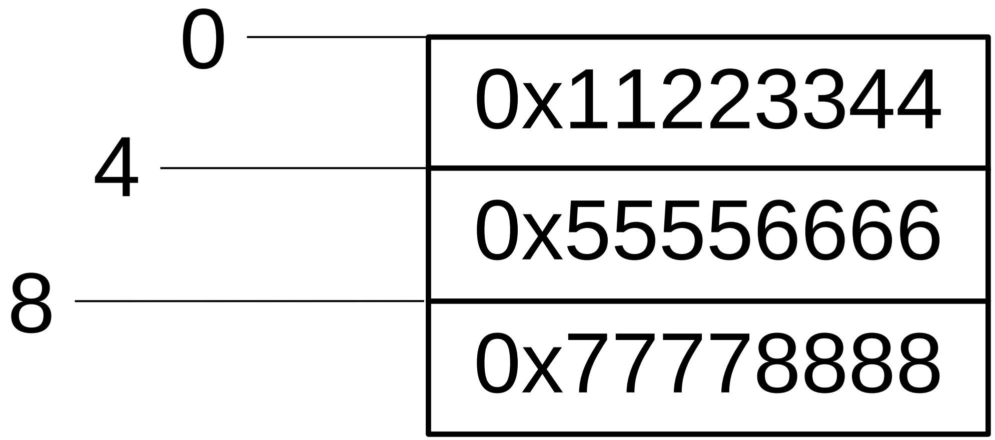
Number:

0x1122334455667788

Little Endian:

88	77	66	55	44	33	22	11
0	1	2	3	4	5	6	7

Numbers in memory



0

4

8

0x11223344

0x55556666

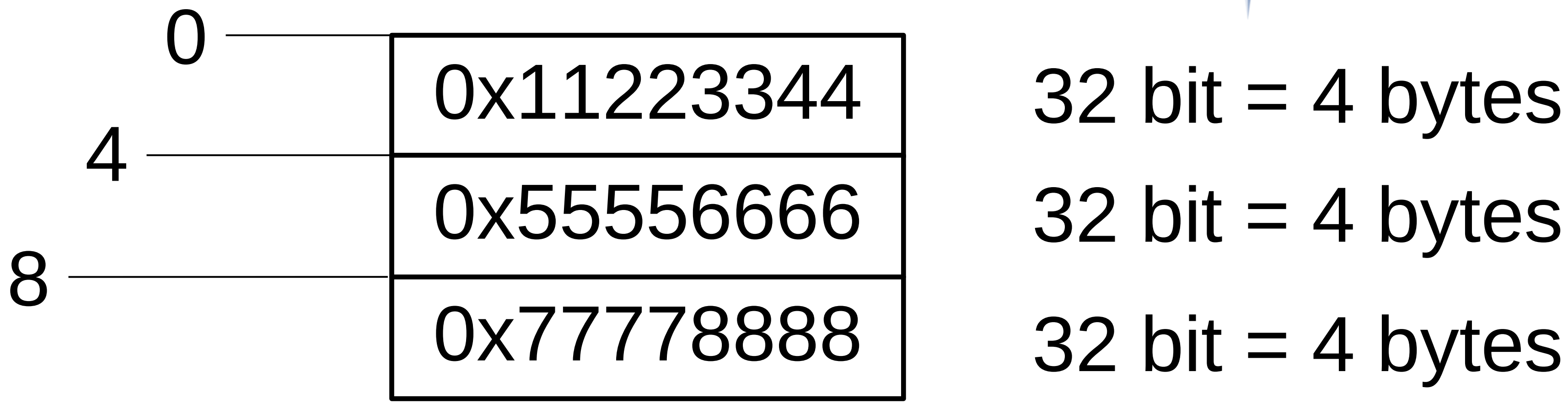
0x77778888

32 bit = 4 bytes

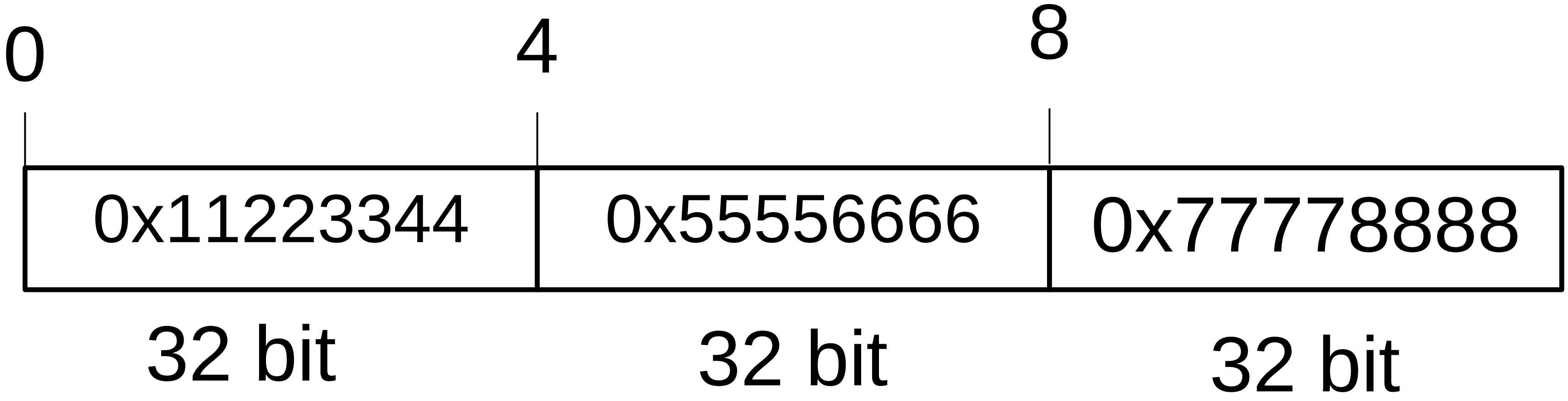
32 bit = 4 bytes

32 bit = 4 bytes

Numbers in memory

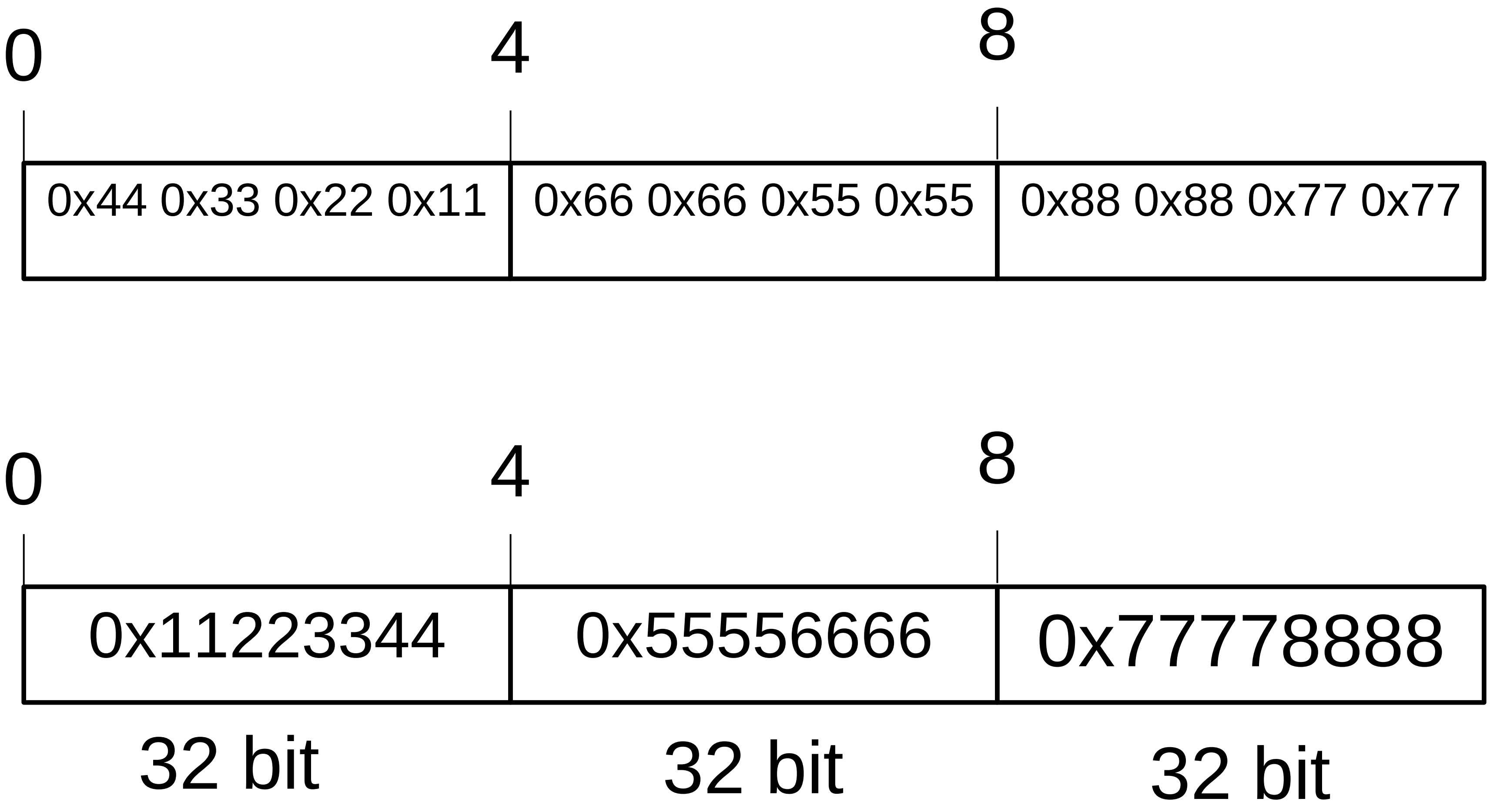


0	0x11223344	32 bit = 4 bytes
4	0x55556666	32 bit = 4 bytes
8	0x77778888	32 bit = 4 bytes



0	4	8
0x11223344	0x55556666	0x77778888
32 bit	32 bit	32 bit

Numbers in memory



0	4	8
0x44 0x33 0x22 0x11	0x66 0x66 0x55 0x55	0x88 0x88 0x77 0x77

0	4	8
0x11223344	0x55556666	0x77778888
32 bit	32 bit	32 bit

Numbers in memory

Recap:

- Numbers can be displayed in decimal, or hex (0-9, a-f)
- Numbers are stored as 16, 32 or 64 bit value as little endian
- If we look at little endian numbers as bytes, they are inverted
- If we look at numbers in memory, we can’t know if they are 8, 16, 32 or 64 bit

Operating System Basics

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

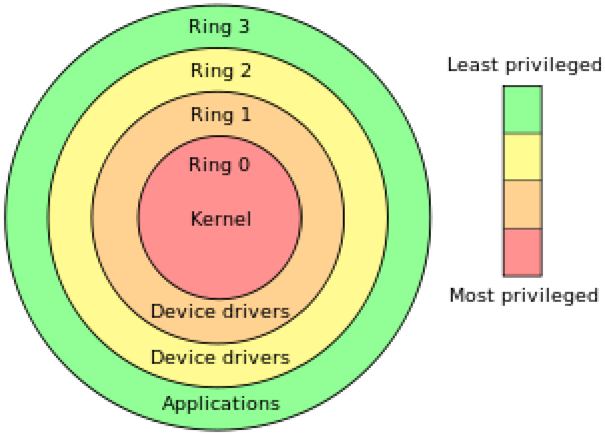
OS Basics: Rings

Ring 0: Kernel (Kernelspace)

- Not covered here
- Can be interacted with by using “syscalls”

Ring 3: Userspace

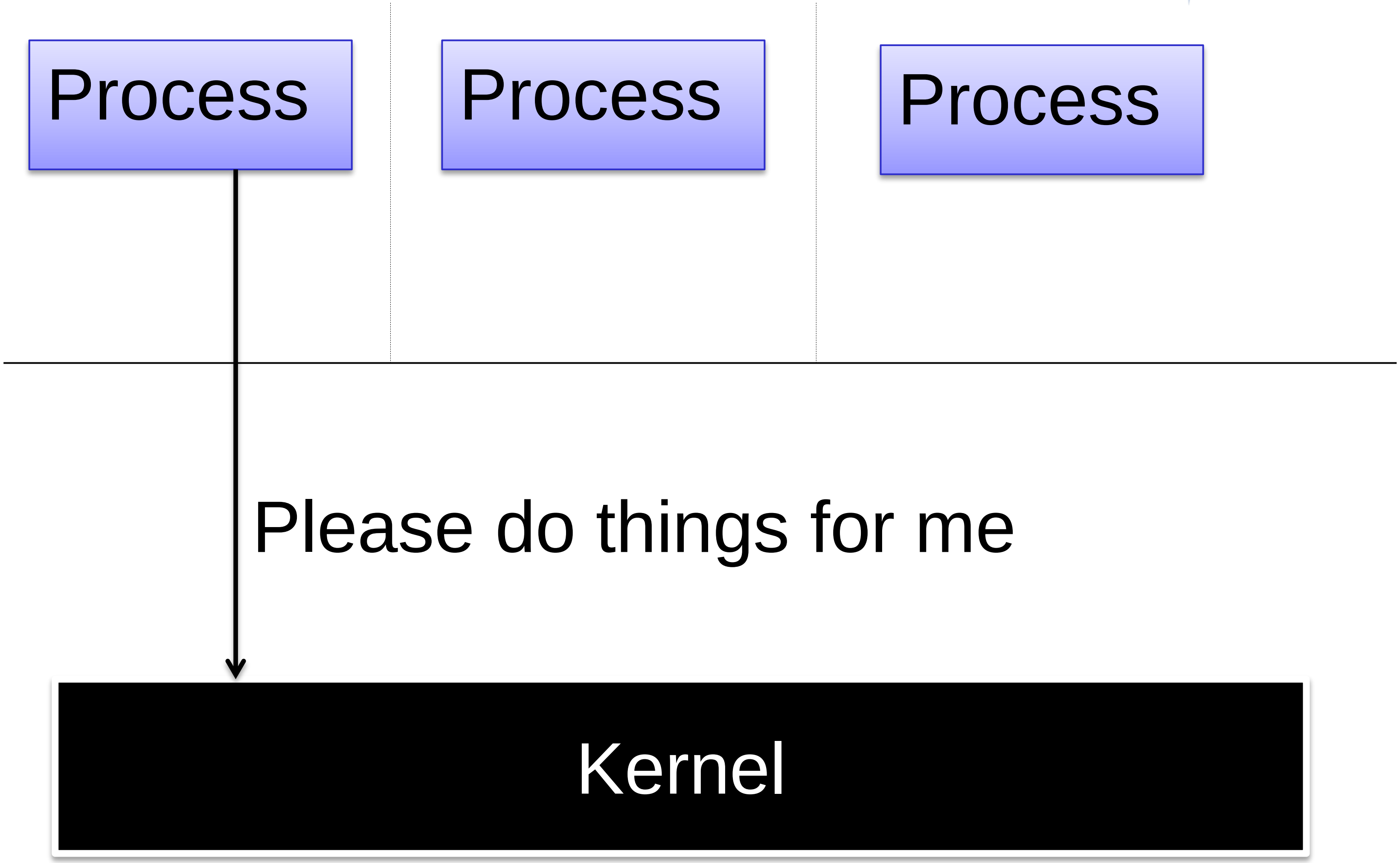
- Where all programs run
- ls, Bash, Vim, Apache, Xorg, Firefox, …



How to transit from userspace to kernelspace?

- System Calls (syscall)

OS Basics: Rings



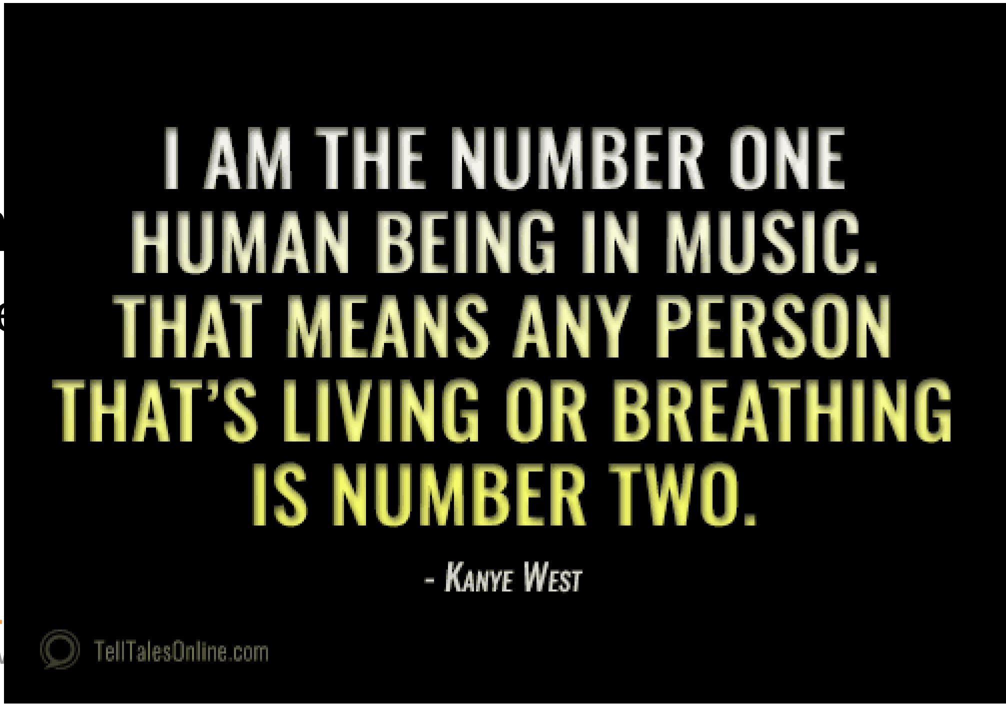
OS Basics: Processes

A Process:

- Is a running program
  - Program lives on disk (static)
  - Process lives on memory (alive)
- Process thinks he "owns" the hardware
  - RAM
  - CPU

Multiple processes can

- Everyone thinks he is the
- Like Kanye West



I AM THE NUMBER ONE HUMAN BEING IN MUSIC. THAT MEANS ANY PERSON THAT'S LIVING OR BREATHING IS NUMBER TWO.

- Kanye West

TellTalesOnline.com

OS Basics: Process and Memory

Processes can address:

- **4 GB of memory** in 32bit OS
  - (2-3 GB actually)

- Independent on how much memory there really is

What if we have:

- Only 2 GB RAM?
  - OOM (Out Of Memory) when too much memory is used
- 8 GB RAM?
  - 2 Processes can use all their 4GB!

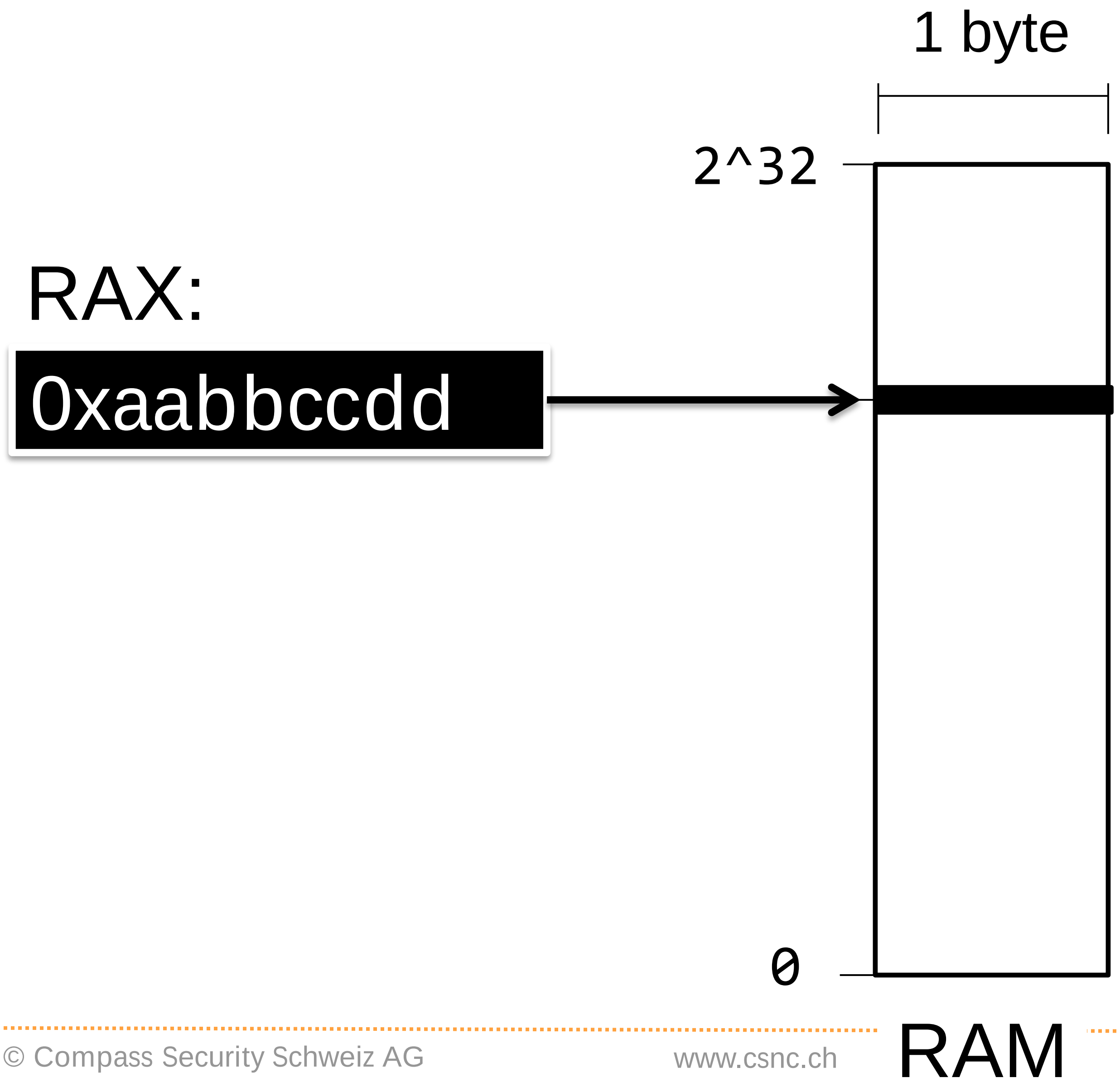
OS Basics: Process and Memory

Why 4 GB?

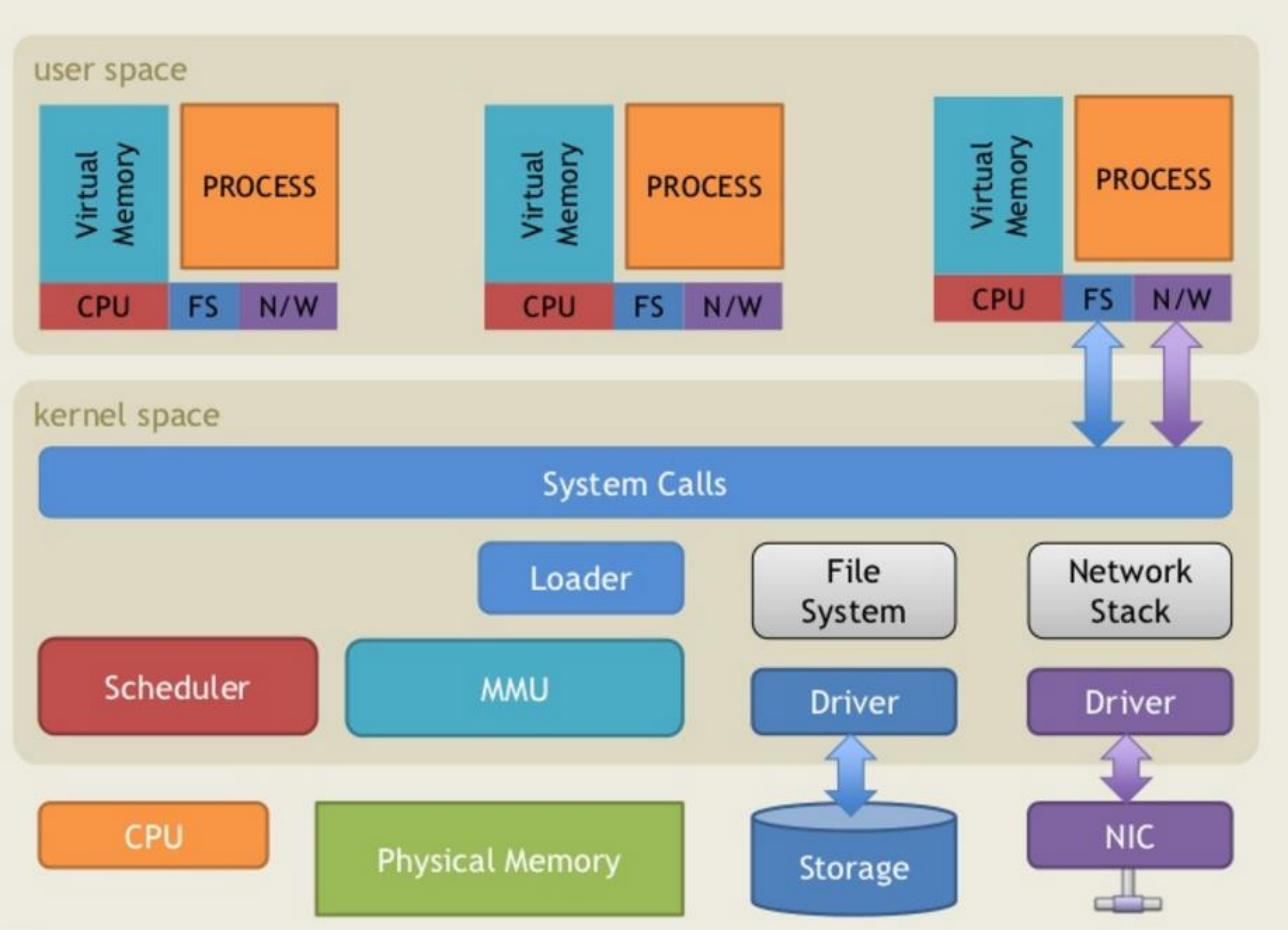
- 32 bit register
- Register are used to address memory
- 2^32 = 4 billion = 4 gigabyte

A process has therefore access to 4 billion one-byte memory locations

OS Basics: Process and Memory



OS Overview

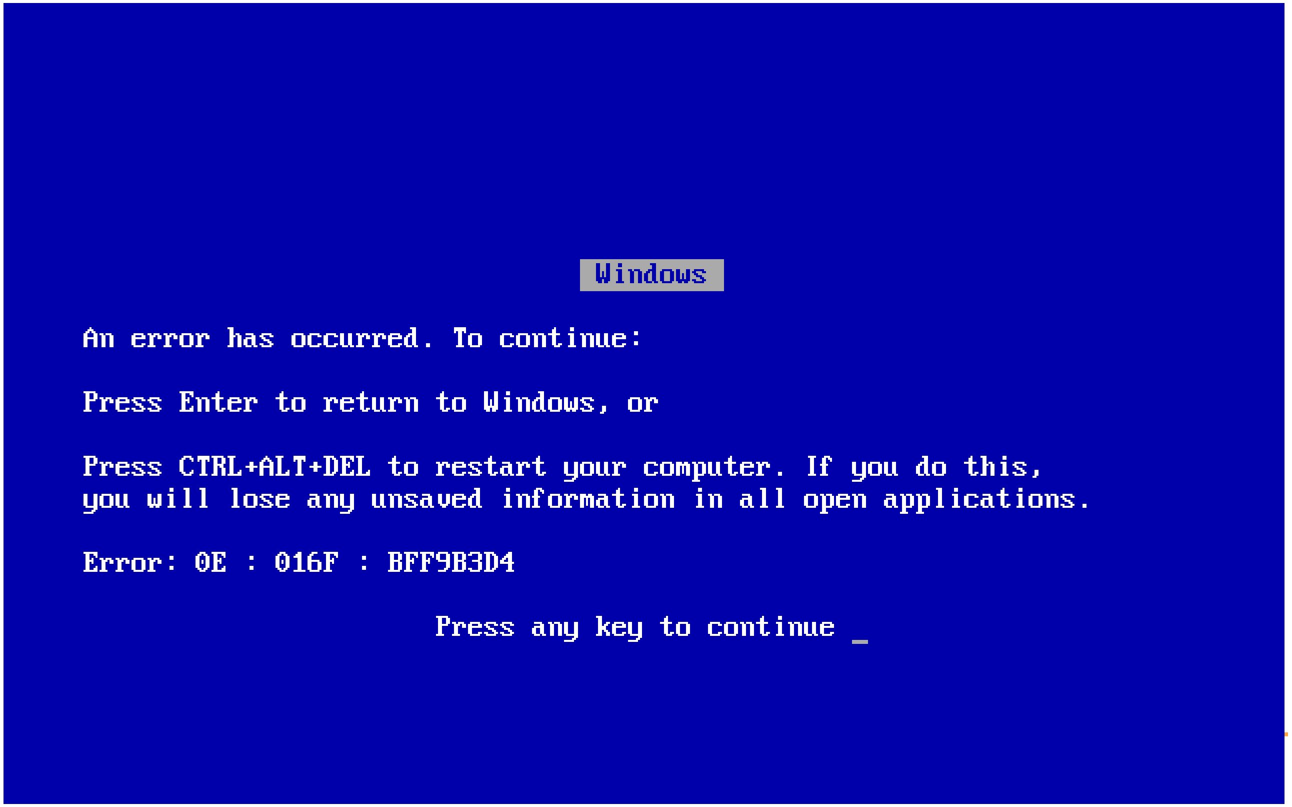


http://www.slideshare.net/saumilshah/operating-systems-a-primer

OS Overview

History lesson: “The good old times”

- Windows did not have true protected memory until windows NT/2000
  - Including all of DOS, Windows 3.1, Windows 95, 98, ME
- Every process could write into all all other processes, or even the OS
- “Blue screen of death”



```
                              Windows

  An error has occurred. To continue:

  Press Enter to return to Windows, or

  Press CTRL+ALT+DEL to restart your computer. If you do this,
  you will lose any unsaved information in all open applications.

  Error: 0E : 016F : BFF9B3D4

                        Press any key to continue _
```

OS Overview

There's only one CPU, how can:

- Multiple programs run at the same time?
- The OS and the programs run at the same time?

Solution: Interrupts

- Timer interrupts
- Interrupts are handled by the kernel
  - Time / clock
  - Network interface
  - USB devices

OS Overview

Recap:

- Processes are programs which are alive in the RAM
- Every process thinks he owns the computer (including all the RAM)

32 bit vs 64 bit

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

32bit vs 64bit

From 32 to 64 bit

- You all are probably too young for this
- But it was kinda big thing
- AMD invented the current 64 bit architecture
  - Intel wanted a new one: Itanium. Failed hard.
  - (AMD was better than Intel in most respects. Sigh).
- x86 to x64 / amd64
  - 8086, 80286, 80386, 80486, 80586 aka Pentium

- "Is windows 64 bit twice as good/fast than windows 32 bit?"
  - Width of the CPU registers define the amount of addressable memory

32bit vs 64bit

64 bit pros:

- Can address more than 4 gb of memory per computer
- 64 bit calculations are maybe a bit faster

64 bit cons:

- Programs use more space
  - Because pointers and data-types (integer) are twice as big
  - On disk, memory and cache

32bit vs 64bit

64 bit registers are prefixed with “R” (RAX, RIP, …)

New registers: R8-R15

Pointers are 64 bit

Push/Pop are 64 bit

32bit vs 64bit

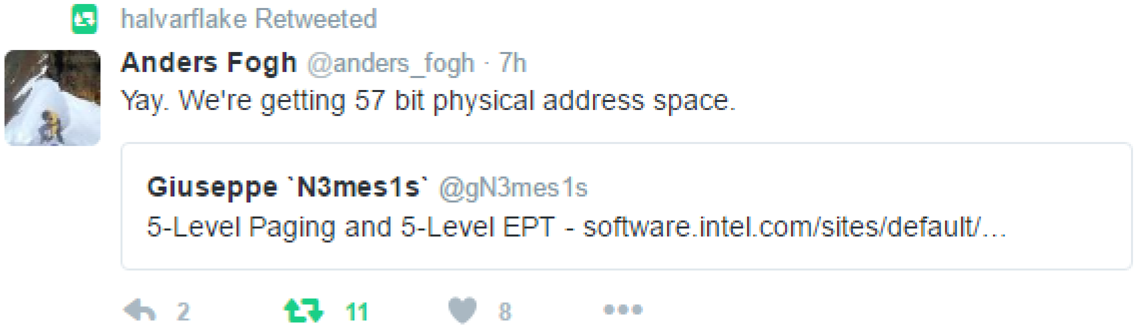
For 64 bit:

- 64 bit are 18 exabytes
- Only 47 bit are used (=140 terabytes)
- `< 0x00007fffffffffff`

32bit vs 64bit

For 64 bit:

- 64 bit are 18 exabytes
- Only 47 bit are used (=140 terabytes)
- `< 0x00007fffffffffff`



halvarflake Retweeted

Anders Fogh @anders_fogh · 7h

Yay. We're getting 57 bit physical address space.

> **Giuseppe `N3mes1s`** @gN3mes1s
> 5-Level Paging and 5-Level EPT - software.intel.com/sites/default/…

5-Level Paging and 5-Level EPT

White Paper

Revision 1.0

December 2016

32bit vs 64bit

Linux (and Windows) can execute 32 bit processes on a 64 bit OS

- C:\Program Files
- C:\Program Files (x86)

- /lib/lib
- /lib/lib64

The 32 bit process does not realize he's on a 64 bit system

- But needs a 32 bit runtime

32bit vs 64bit

Recap

- There are some differences between 32 and 64 bit
- A 32 bit process can run on a 64 bit system as 32 bit