Lecture-1 (Kickstart: Logistics & Intro.)
CS665-Fall 2019
Secure Memory Systems

Biswa@CSE-IITK

Instructor

Biswa ~~(Biswabandan, Sir, Prof., Dr., Er., *-Biswa~~)

Sir/Prof./…… outlawed with CS665 and Biswa

Website: http://www.cse.iitk.ac.in/biswap

Contact: KD 203, biswap@cse.iitk.ac.in
email: [CS665-yourname]

Teaching and Research Interests:
Computer Architecture, Arch-OS interface for performance and Security

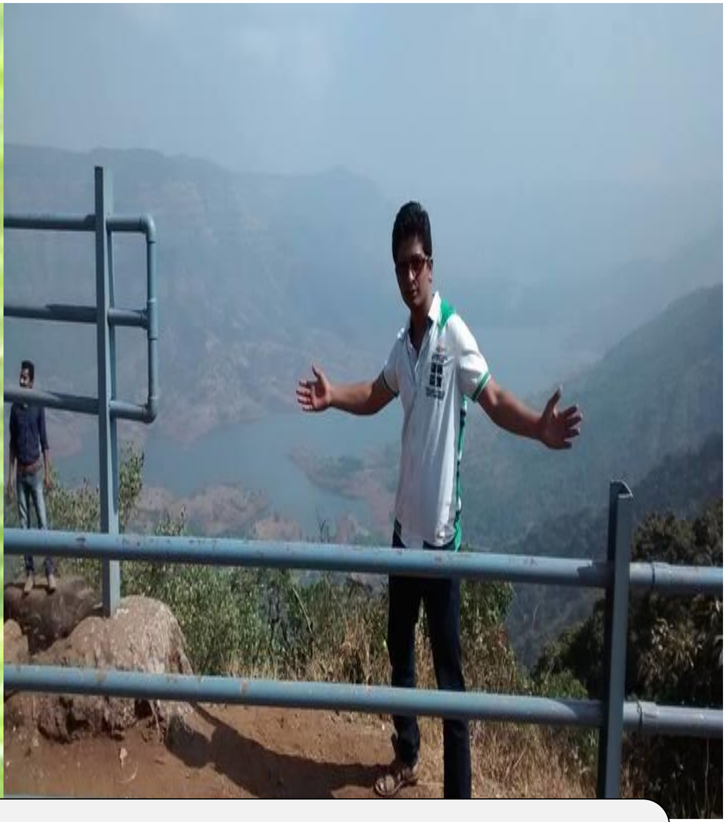
Course Staff: Crazy4Sys@CARS

Biswa

Saurabh

Upasana (the only woman from Masters in pure systems)

Sujeet



Sleeps 24/7 and asks why?

Android Security

Architecture-OS security

&Biswa = KD-203

&Crazy4 = KD-222

Office Hours

Mon: 12 noon

Tues & Thurs:
12 to 1 PM

Wed & Satur: 4 to 5 PM
Will be busy post Sept. 20

Mon: 5 to 6 PM
Fri: 12 to 1 PM

Sundays: we do not work. Expect the same from you all ☺

Before CS665: Non-technical things that affect technical things

Then kick-start CS665

Logistics

When: Mon/Tues. 03.30 PM:5 PM/2PM:3.30PM (*flexible*)
Where: KD 101, What: You know it, Exam dates: Next slide ☺

Course website: www.cse.iitk.ac.in/~biswap/CS665-F19.html

Piazza: For online discussions (Refer course website)

Submission of assignments: Canvas

https://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html

Register/Drop ASAP (if interested/not interested)

End-term: ∞ points (marks), November

Start preparing

Tell me the text-book then !!

Follow the following Books

No book, no exam for CS665

10+2+JEE : 100 books for $n years

Then: No comments

B.Tech.: 10 books per every 4 months

Mostly mugging up, then ....

So,

Don’t

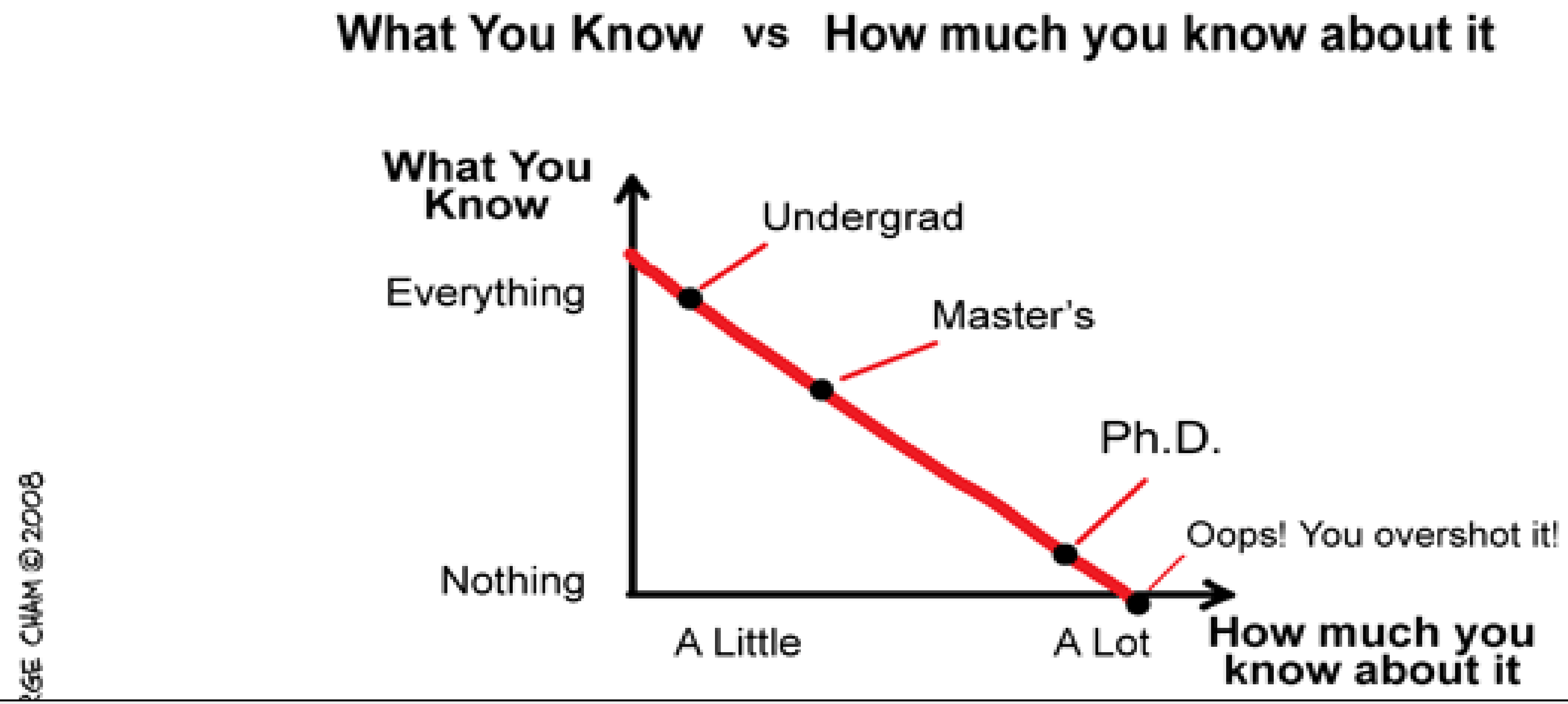
Please, do not credit this course if you are good at

1. *Mugging up*
2. *Writing exams*
3. *Taking notes: Day in Day out*
4. *Sitting silently in the class*

Why So?

Graduate level course

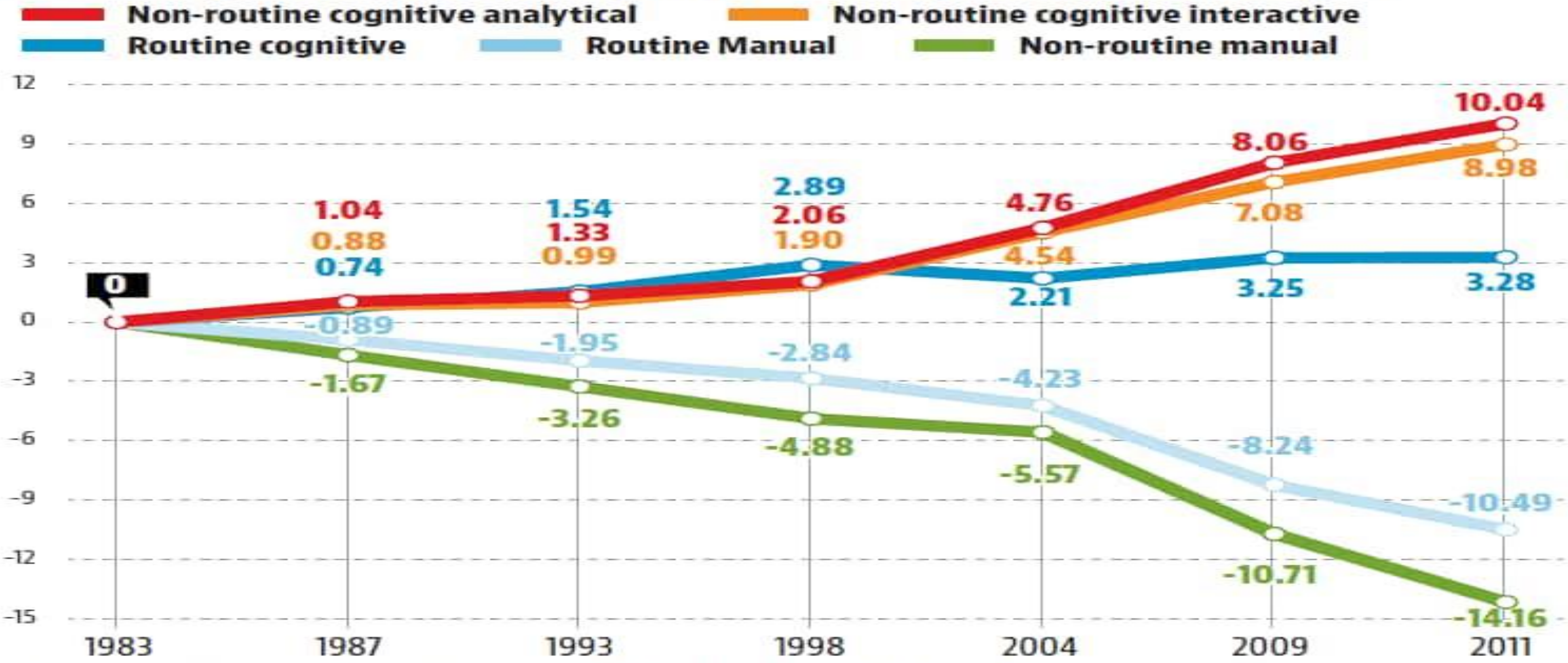
Mastery: Knowing More and More about less and less



Just the beginning of a new journey. So do not put a full stop.

Changing nature of jobs

The share of cognitive-skill based jobs has been increasing while less and less manual jobs are being created in the Indian economy



Lines show percentage point change in task intensity of different kind of jobs

SOURCE: EPW, CHANGING TASK CONTENT OF JOBS IN INDIA: IMPLICATION AND WAY FORWARD, PANKAJ VASHISHT, JAYDEV DUBEY, 19 JAN, 2019

Cognition

Process of acquiring knowledge and understanding through

thought,

experience,

and the senses.

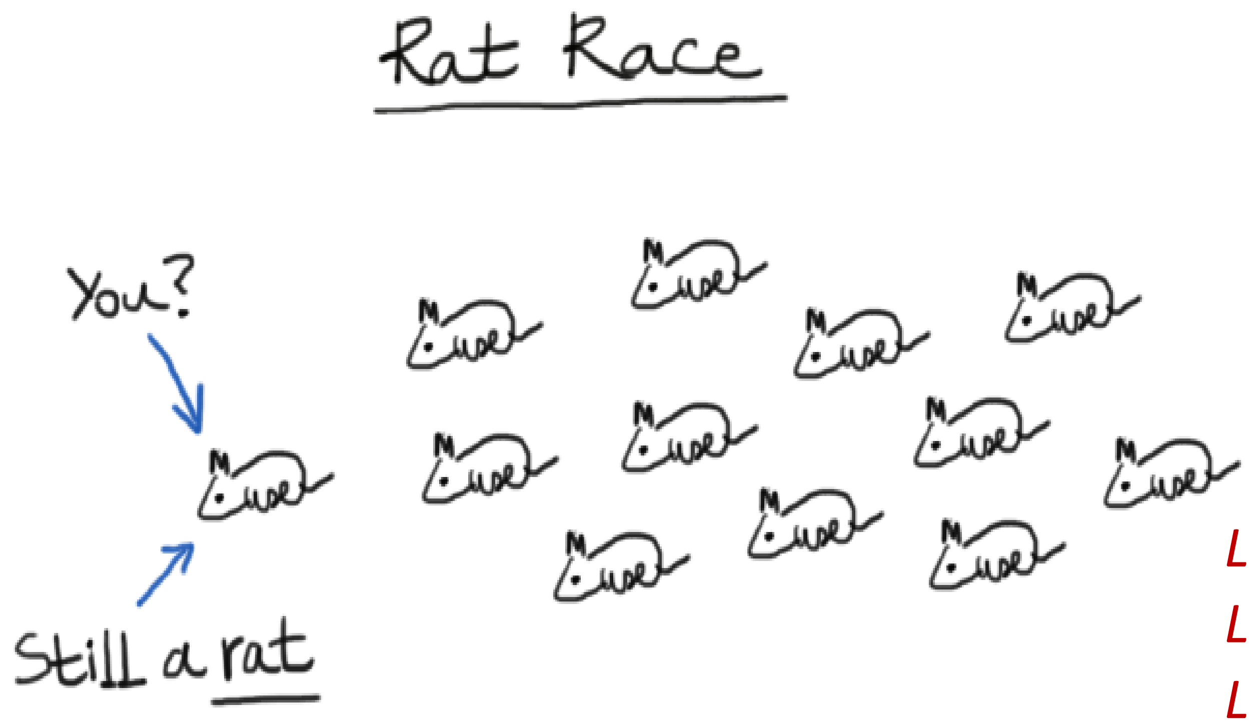
Please: Be Aware of It (Herd ….)

I DON'T KNOW WHERE WE'RE GOING, BUT FROM THE LOOK OF THIS CROWD, IT'S GOTTA BE GOOD!

***The first principle** is that you must not **fool** yourself –
and you are the easiest person to **fool***

If all then why not me, Ask, if all then why me too ?

CS665: Will not be a



Learn at your own speed,

Learn as a group, not as an individual

Learn how to deal with failure and then bounce back

Walk, no need to run ☺

"When your only competition/race is becoming a better you, you will always win the game."

Learn What?

Tenacity

Learning to learn (lifelong learner), passion, curiosity

How to fail and bounce?
without burning out

Perseverance for excellence

Thick Skin (comments/feedbacks will be about your work and not YOU)

What about talent?

Talent ☺ [Most Over-hyped word on/in the planet]

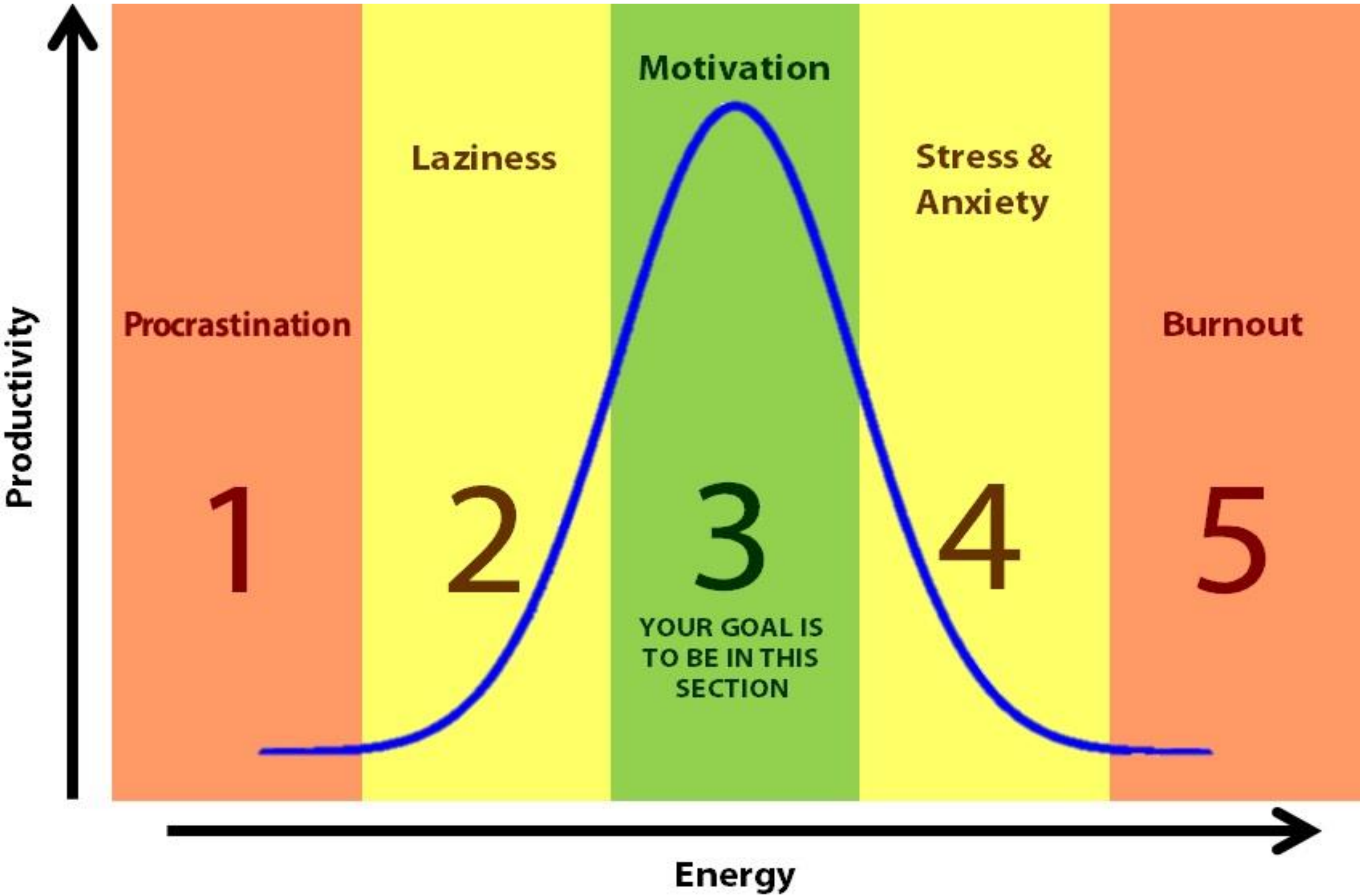
I am the one with the lowest IQ in this room ☹ and I am fine with it ☺

Talent opens the 1st door
Not the nth door. Hardwork opens even the (n+1) st

You all are talented right?
JEE/GATE top rankers
Learn how to deal with failure
Do not run away ☺

Hard work and Burnout

Take a break (hard break) once in a week.



Skills not to have: Intellectual Corruption(theft)

Reason: Comparison with others, desperation

Trying to achieve more with less effort ☹

When you can’t make it then fake/steal it

Learn from who knows, ask, how ? Do not cheat/complain

CS665: The Difference

Consumer

Mugging up, Writing answers!! Grades ☺

Punished if you fail (F grades)

Heard about DeepBlockSecurity for QClouds?

Producer

Group-learning and thinking. Asking Qs. Why and why? Whynot?

What if? What may? How? Why not?

Not believing in textbooks. Learning by doing.

Multiple answers/ideas/insights ☺

You will get full points if you fail *successfully*

Pride in saying "I DO NOT KNOW"

CS665: Why Group?

Why group? I LLNESS -> WE LLNESS (helps minimizing the race, ego??)

Systems is all about a cohesive group. Imagine a break-up between gcc and x86, or Linux kernel and x86. Damn!!

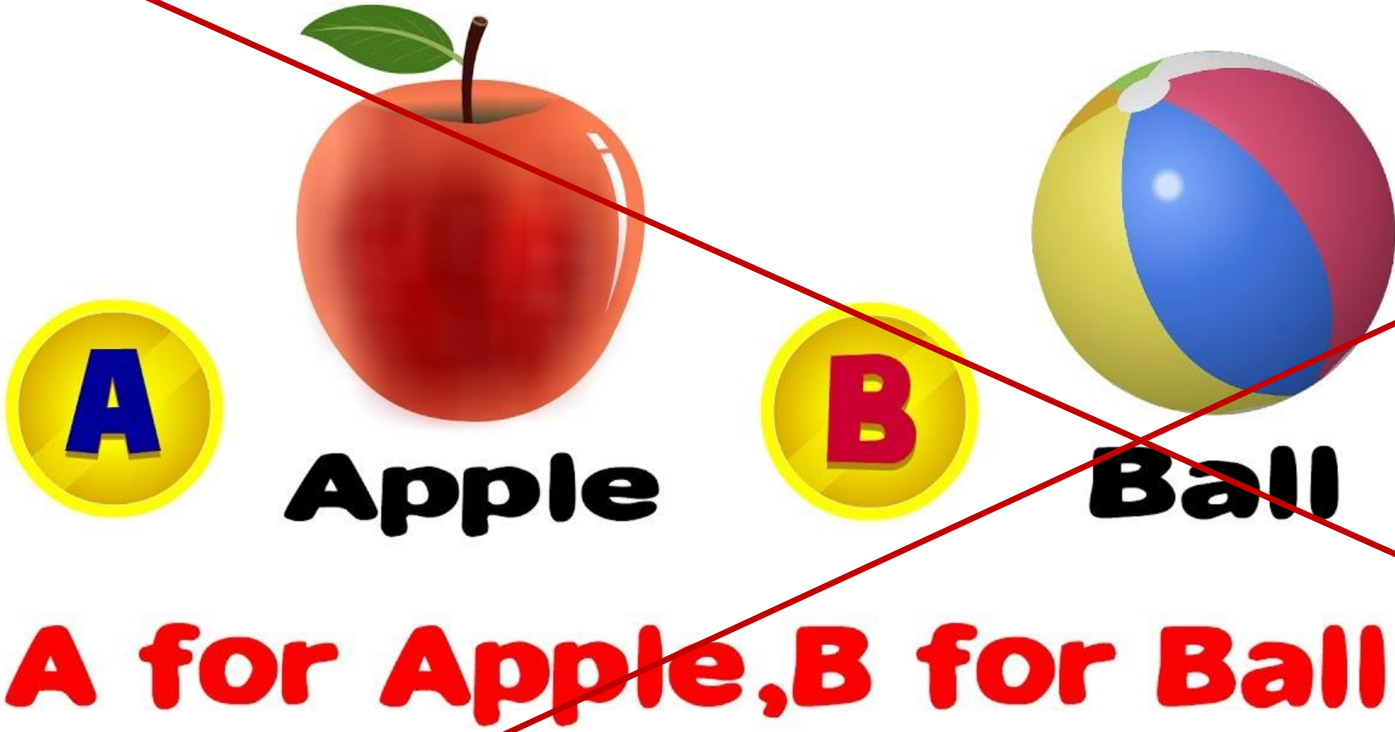
Each group must meet Biswa once in a week over a cup of coffee/tea/water/air ☺

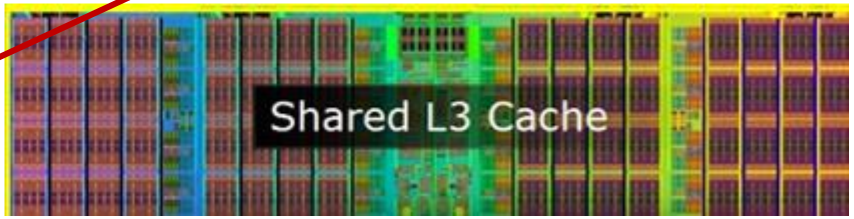
Two options for grading:

(i) All groups start from 100 points on July 29th ☺

(ii) All groups start from zero point

Lectures format





C for Cache, D for DRAM

Who Said This?

"You can know the name of a bird in all the languages of the world, but when you're finished, you'll know absolutely nothing whatever about the bird… So let's look at the bird and see what it's doing—that's what counts. I learned very early the difference between knowing the name of something and knowing something."

So let's learn:

How to learn, how to ask questions, how to code, how to think critically, how to build/analyze systems, Crazy4 will be there.

Lectures = Discussions

Why and How of many things

Lecture Hours: We will discuss/debate on the intricacies

I am excited but I don’t know: ……… so many things

Make sure you are ready to learn: rest we will take care.

We will learn soon

What I expect from you?

No open-screens (no nomophobics): No open smart-phones (phones) & laptops/tablets. Keep your phones in silent mode

Ask questions & participate in in-class discussions (worth bonus points)

Understand, implement, and analyze ideas (Hard work and honesty)

I will be honest, give my 100% to facilitate learning, help you almost 24/7

One of the feedbacks:
Biswa, your average response time for all of my responses is: 369.25 seconds

In a nutshell

Commitment: To learn, to make things happen

Excuse: Ditch this word

Honesty and Trustworthiness

What Can you Expect from Me/Crazy-4?

We/I will be with you every step along the way helping you hone your skills

We/I will be there to listen you (whenever something bothers you).

New to IIT:
Feel free to drop by even for non-technicalities. We will address it.

"Everything is difficult before it becomes easy. You have to just LOVE it".

Let’s check assessment policies

Cheating

In any form will lead to zero point in that assignment. Grade will be capped down (one level).

Dates of assignments: You will decide. YES YOU ☺
(*check your schedule and let us know by August 6th*)

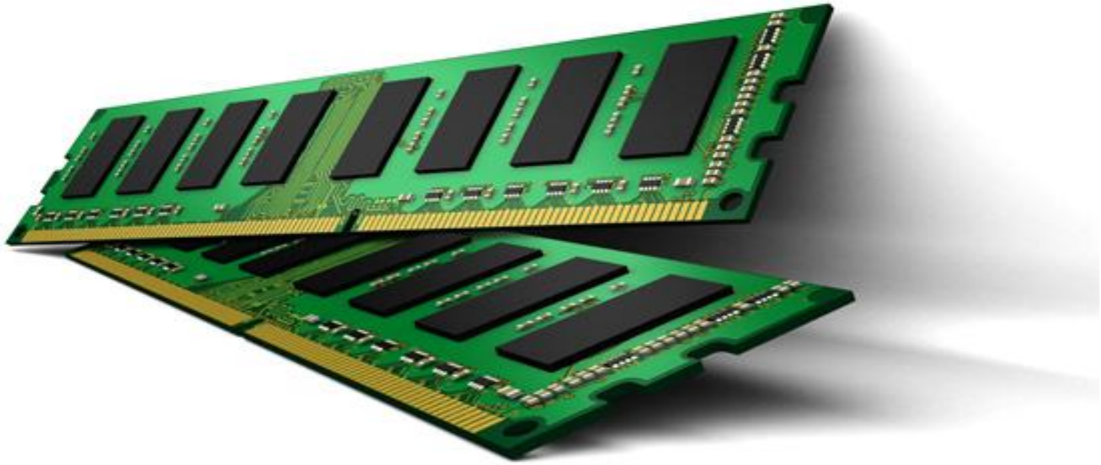
Dropping CS665

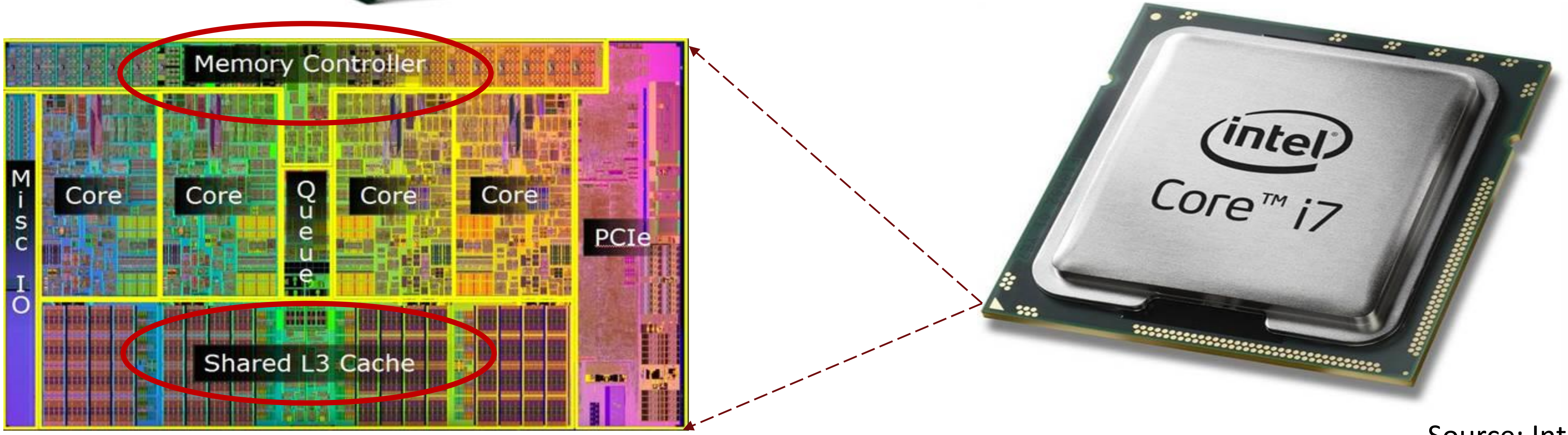
Not allowed after August 13th 2019. Drop the course before that. Why? It will affect your group. Yes (all the assignments are group based)

CS665 in a Nutshell

Then kick-start CS665. Questions before we move on??

Welcome: Secure Memory Systems: SMS (F19)





Source: Intel

Flashback: SMS (F18, best so far for me)

- Let’s start from the feedback. It was offered first time in 2018. So initial glitches were there.
- We have taken care of all the suggestions from F18.
- TAs are the students who took the course. Consult them if still in doubt. My office door is as always open ☺

Poems@CS-665-F18

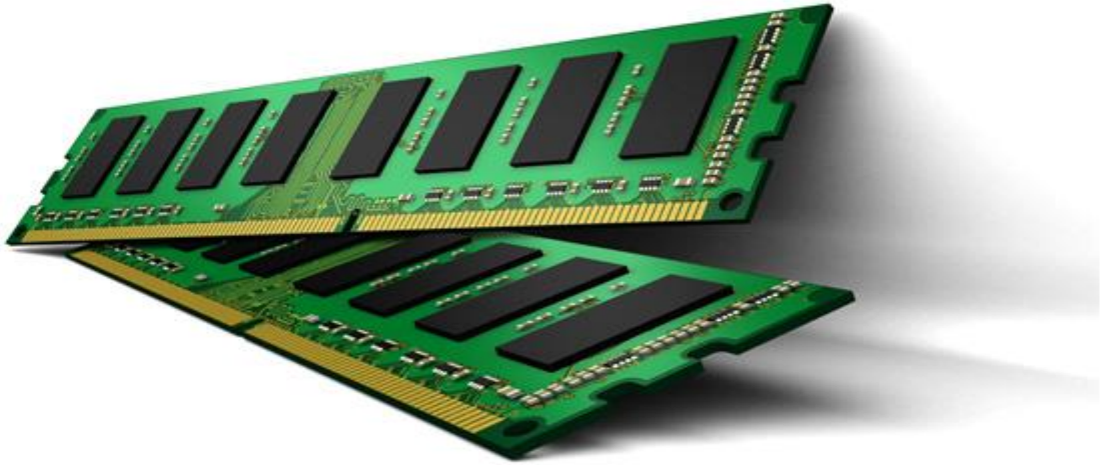
Siva: Where the memory systems are Without fear of attacks
God take my world into those systems
Where no one else need information of others

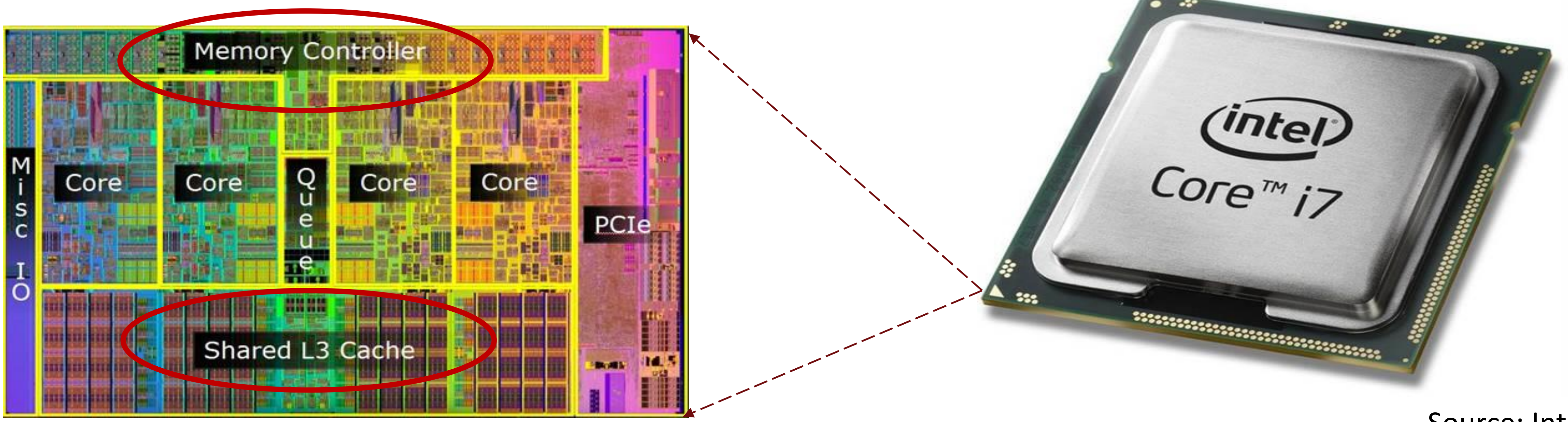
Upasana (**Lana Del Rey ☺**): CS 665 CS 665 CS665 !!
CS 665 is secure memory systems
Learn, learn, learn, Otherwise you are done !!

Jatin: Oh little CS665 You taught us well
I will remember you Whether I go to Heaven or hell !!

Supriya: To new students of CS665 2019
Roses are red Violets are blue
I loved CS665 So will you

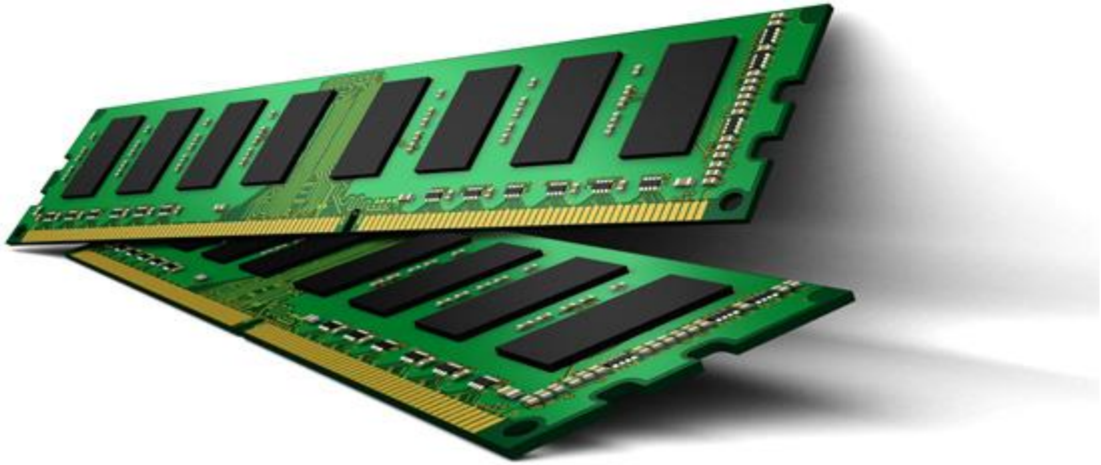
Memory Systems?

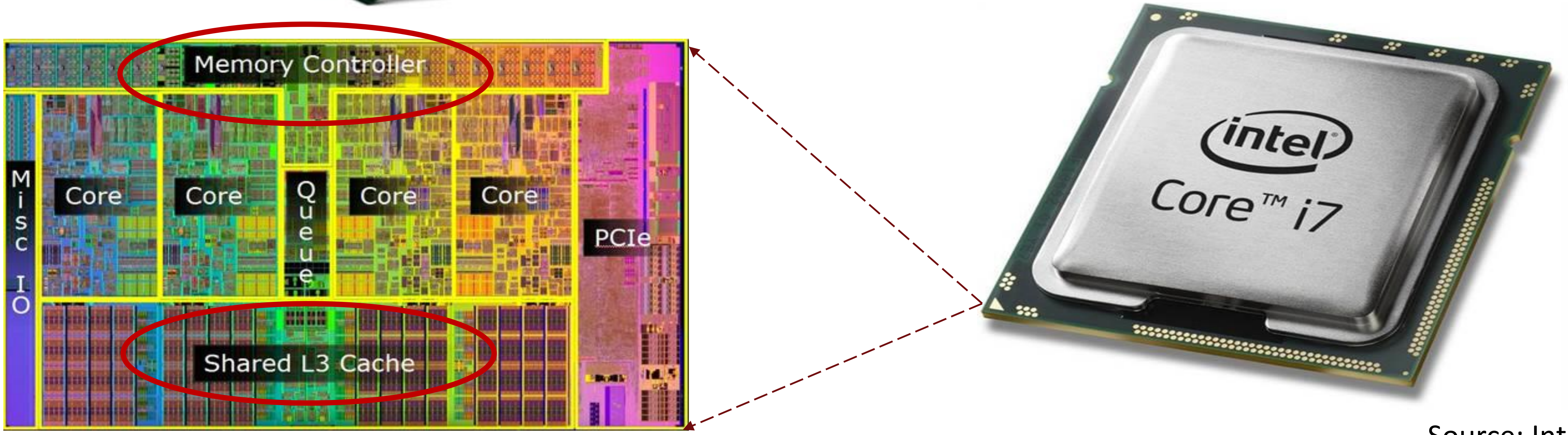




Source: Intel

Systems?





Source: Intel

Code/Experiments/non-theory (in India)

Let’s watch it: Feynman on Scientific method

Indian context (my example): what is the value of g ?

9.8 m/s^2, what else? No wonder we are bad at building systems☹

When I did some experiments ☹

Similarly: Think about this statement “Sun rises in the east”. Correct/incorrect?

Frame of inertia/frame of human centeredness

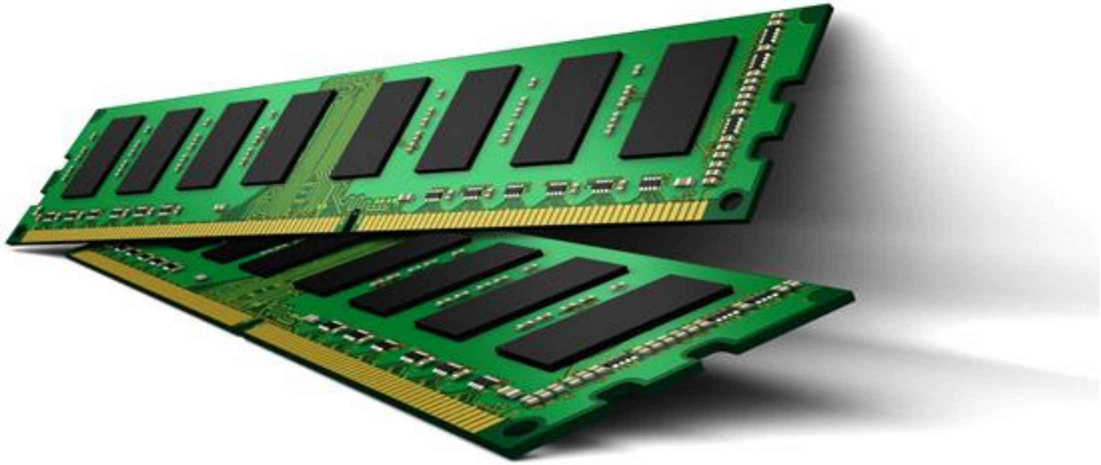
Learning by doing it/seeing it (remember cognition) [not 9.8:why?] [precisely]

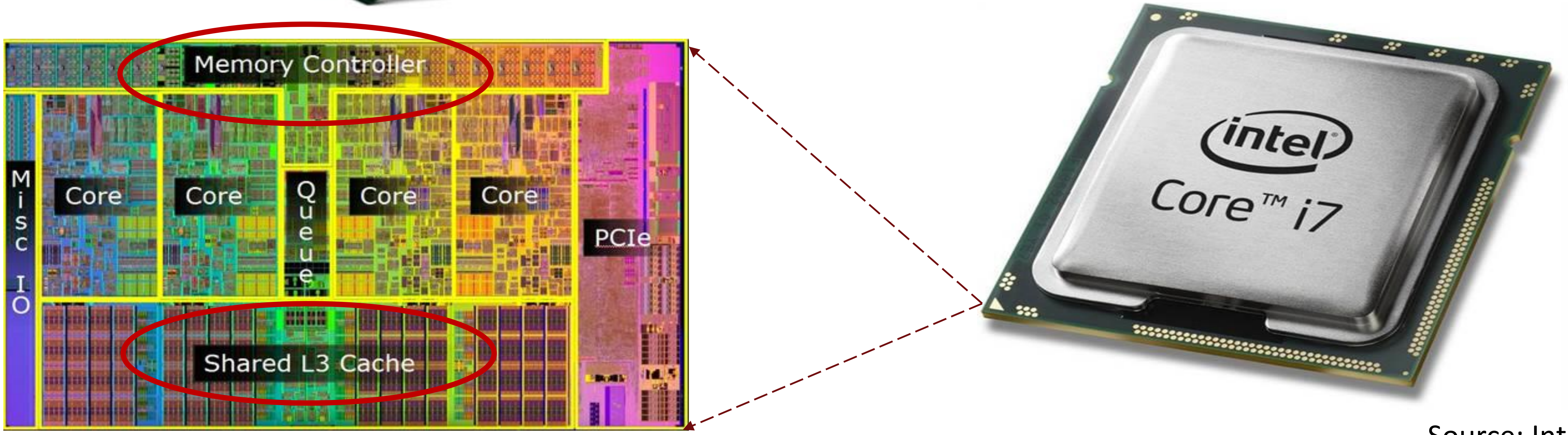
Something to Proud of too (Talking -> Doing ☺)

Image tweeted by @isro

OK!! Can you Move On to the Course Please? Sure ☺

Why Secure?





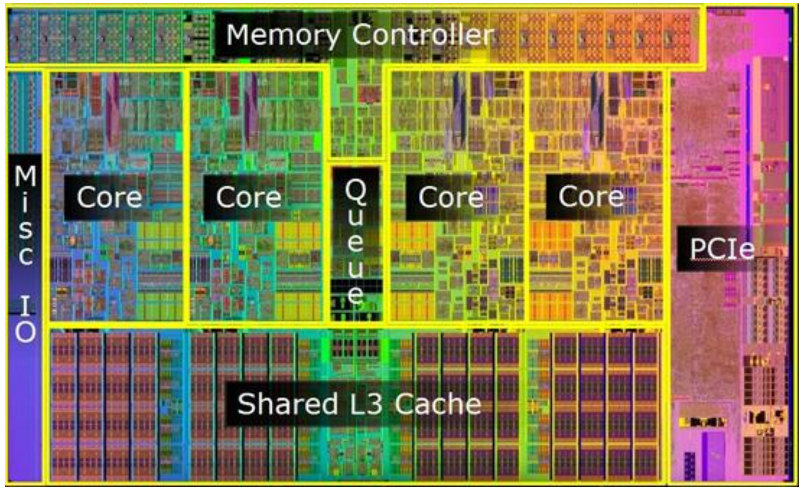
Source: Intel

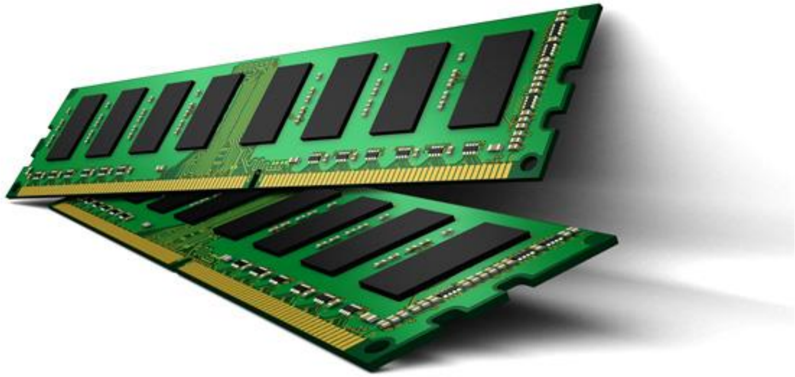
What is Secure? Security?

Security
in India:

OK!! Security!! What does text-book say?

- Confidentiality: Examples please !!
- Integrity
- Availability





Pre-req

- Instruction pipelining
- LOAD/STORE, PC
- Cache, L1/L2, TLBs, page tables
- Tag/Index/Offset
- Direct/Associative mapping
- SRAM/DRAM
- Latency/Throughput
- Virtual/Physical address
- Process/Thread
- Programming in C/C++

Score yourself

10 – Good
5 – Knowledgeable
0 – No Knowledge

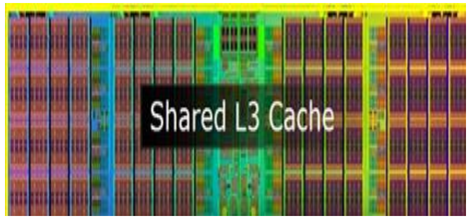
Your score

> 40	– *Welcome*
> 20 & ≤ 40	– Let’s Talk
< 20	– Next Time

However, if you are motivated to learn:
I will be there to help you

Let’s See: But who is Spy/Victim?

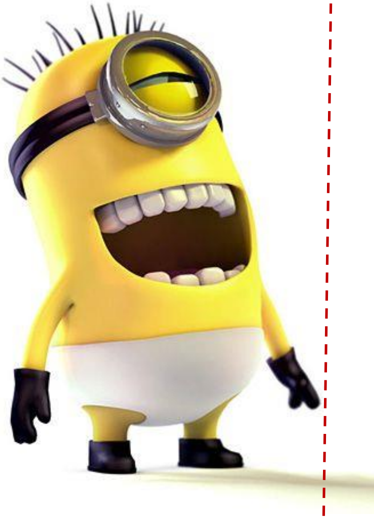
Spy

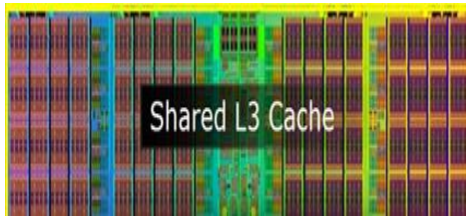


Victim

Side-channel attacks

Let’s play

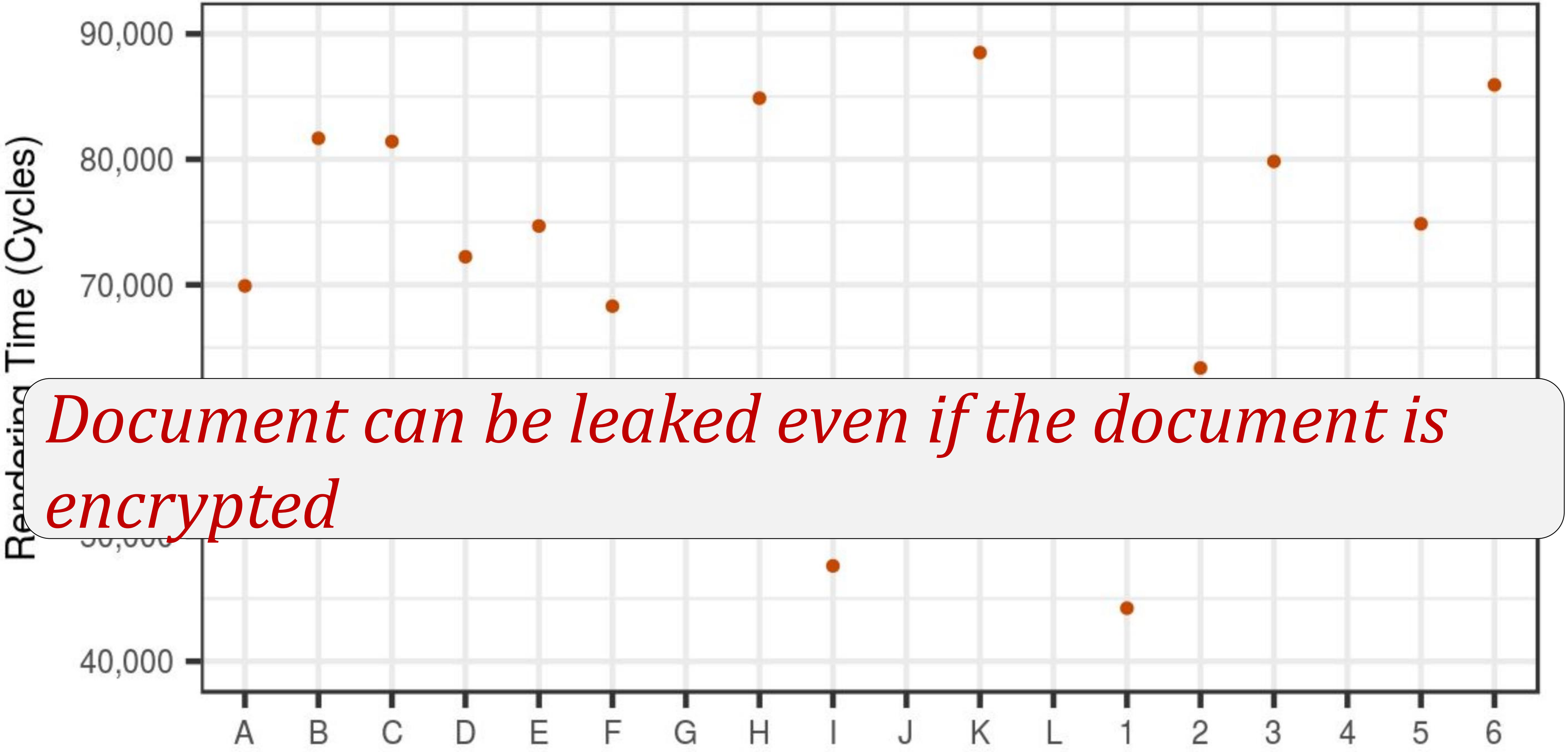




Oh Yes!!

Covert-channel attacks

10K Feet View: Timing Channel



Document can be leaked even if the document is encrypted

Story Begins: Rest of the Course .... Two Teams

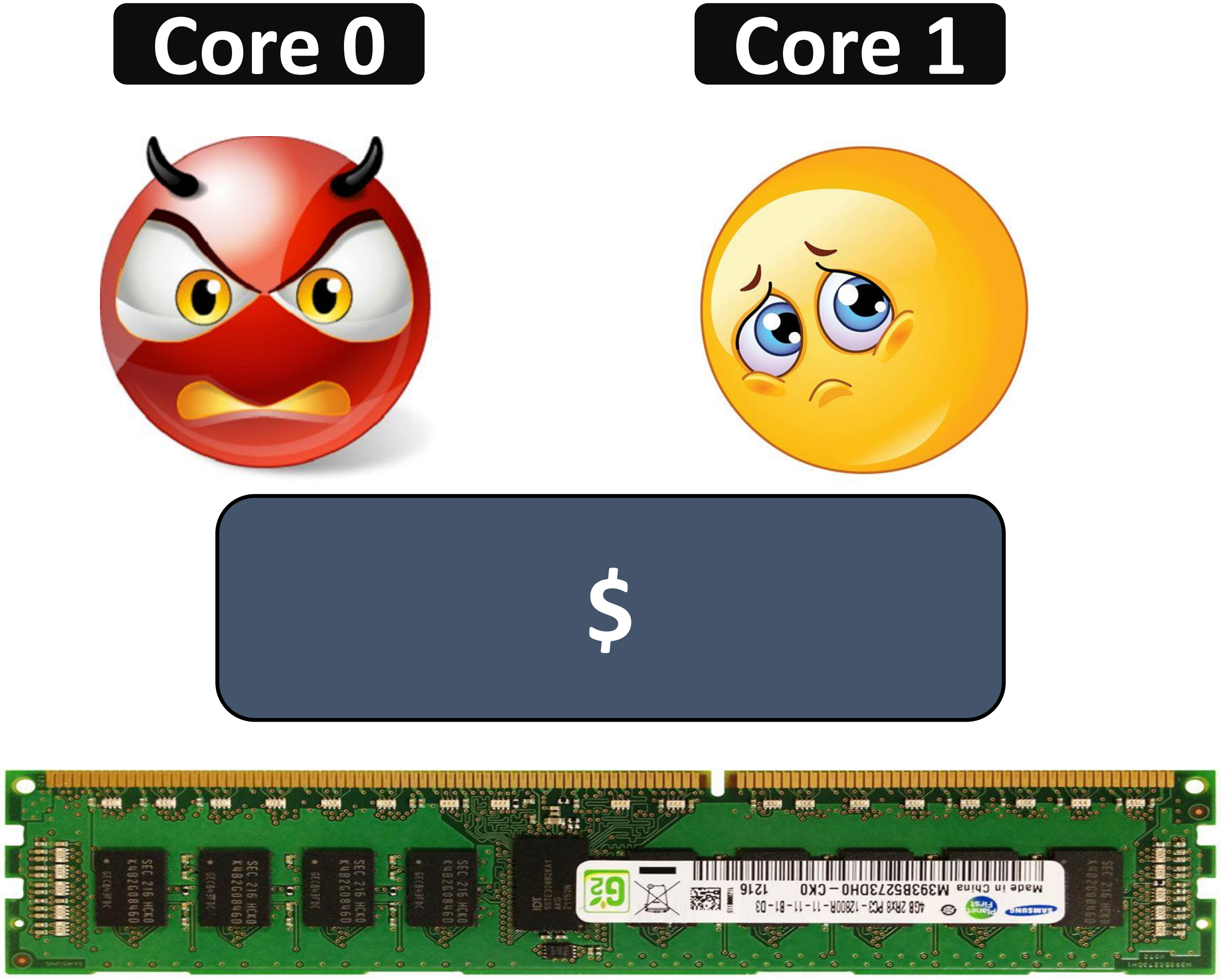
Gogo

Gollu

CIA properties:

Mommmmmy !!!!!

Who is The Spy?

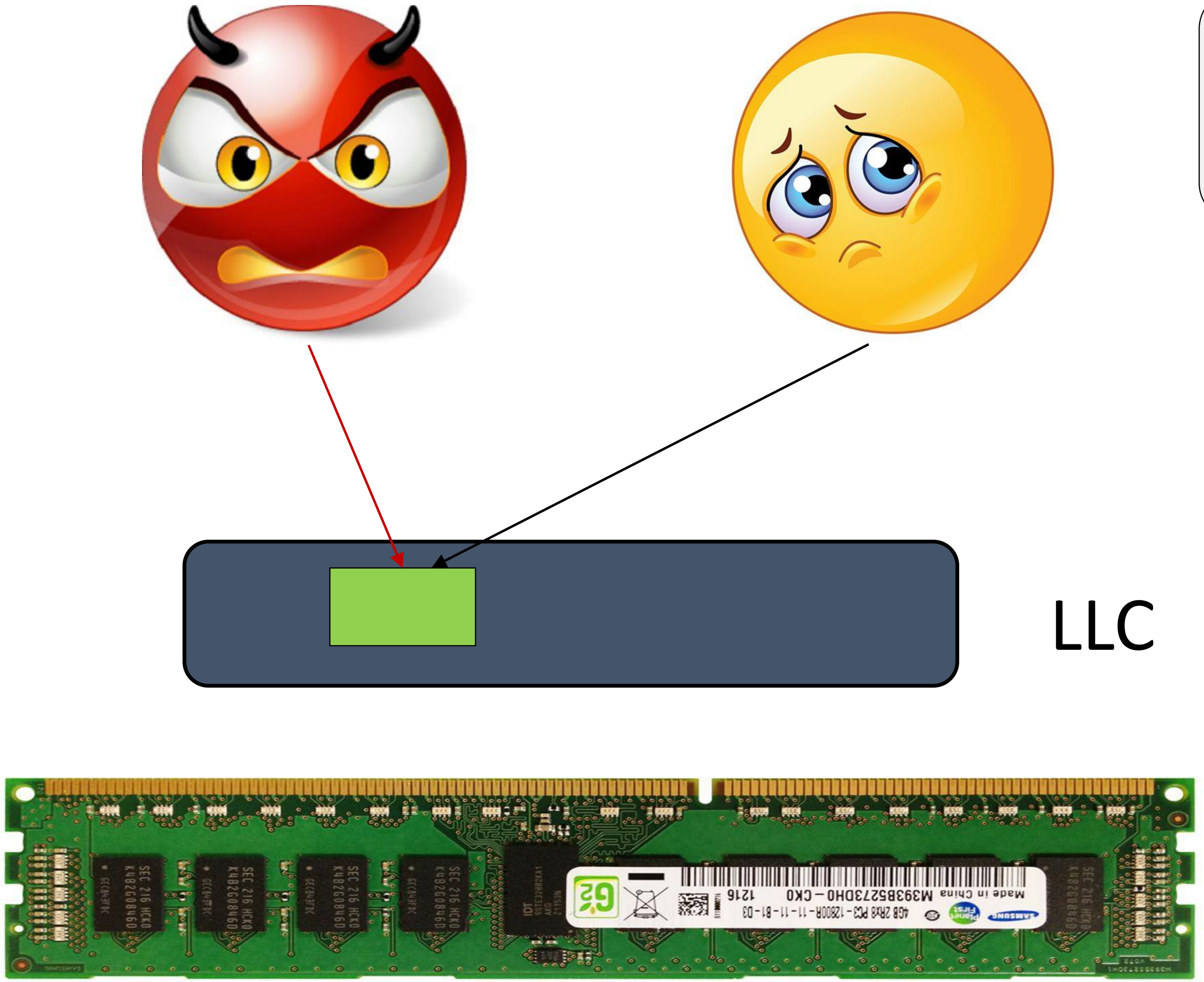


Core 0

Core 1

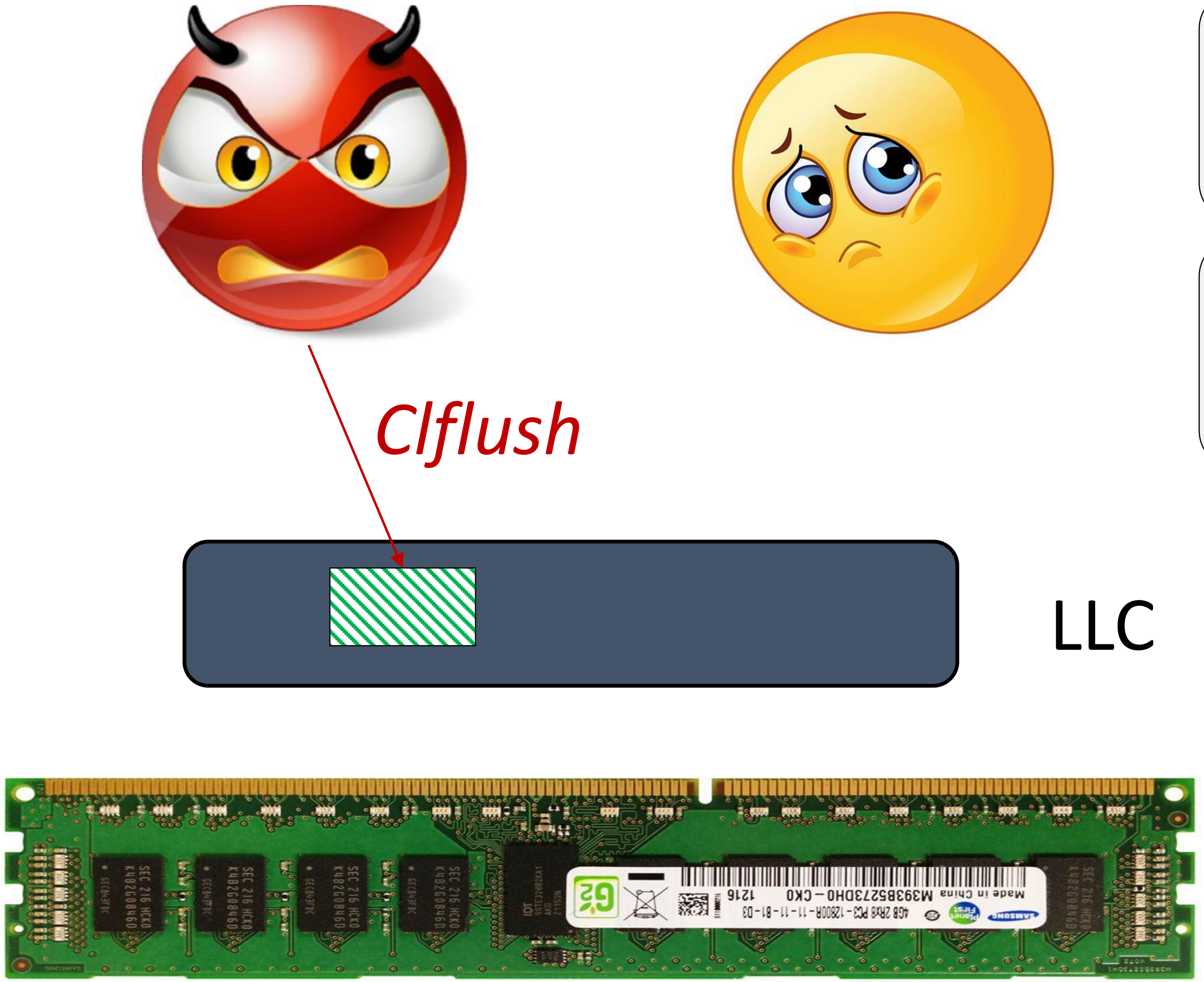
$

Simple Example: Flush + Reload



Step 0:Gogo *maps* the shared library, shared in the cache

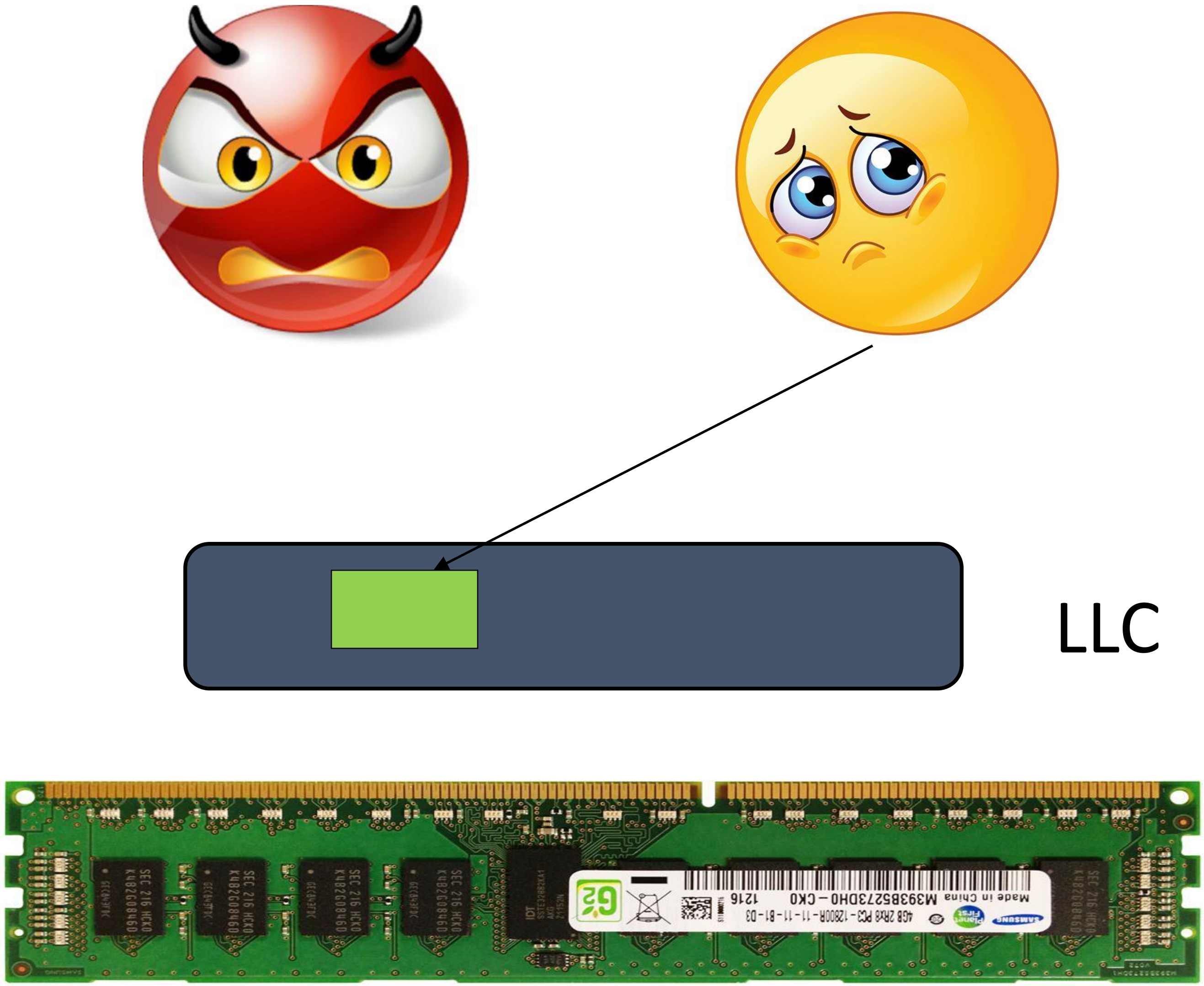
Flush + Reload



Step 0:Gogo *maps* the shared library, shared in the cache

Step 1:Gogo *flushes* the cache block

Flush + Reload

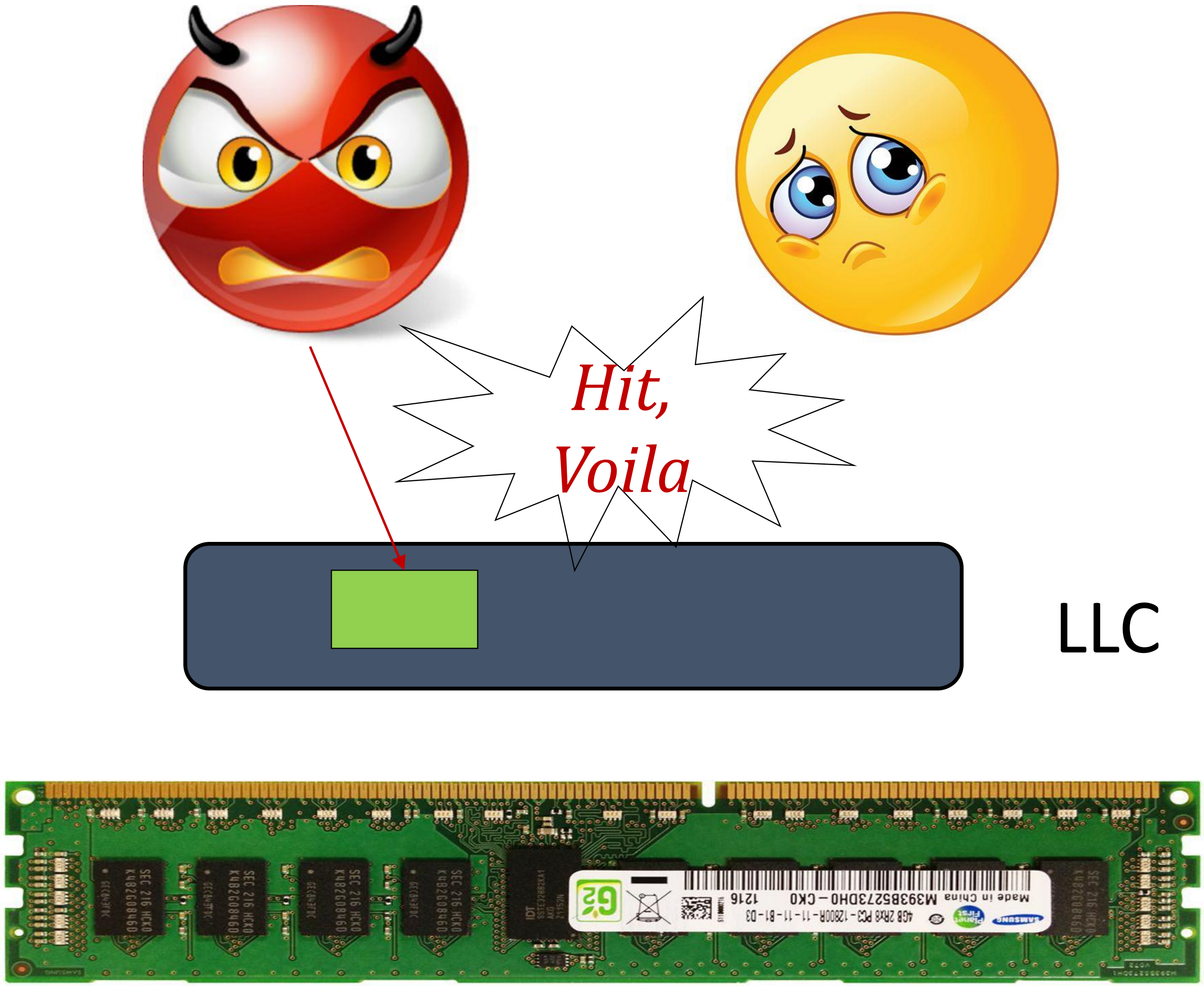


Step 0:Gogo *maps* the shared library, shared in the cache

Step 1:Gogo *flushes* the cache block

Step 2: Gollu *reloads* the cache block

Flush + Reload



Step 0:Gogo *maps* the shared library, shared in the cache

Step 1:Gogo *flushes* the cache block

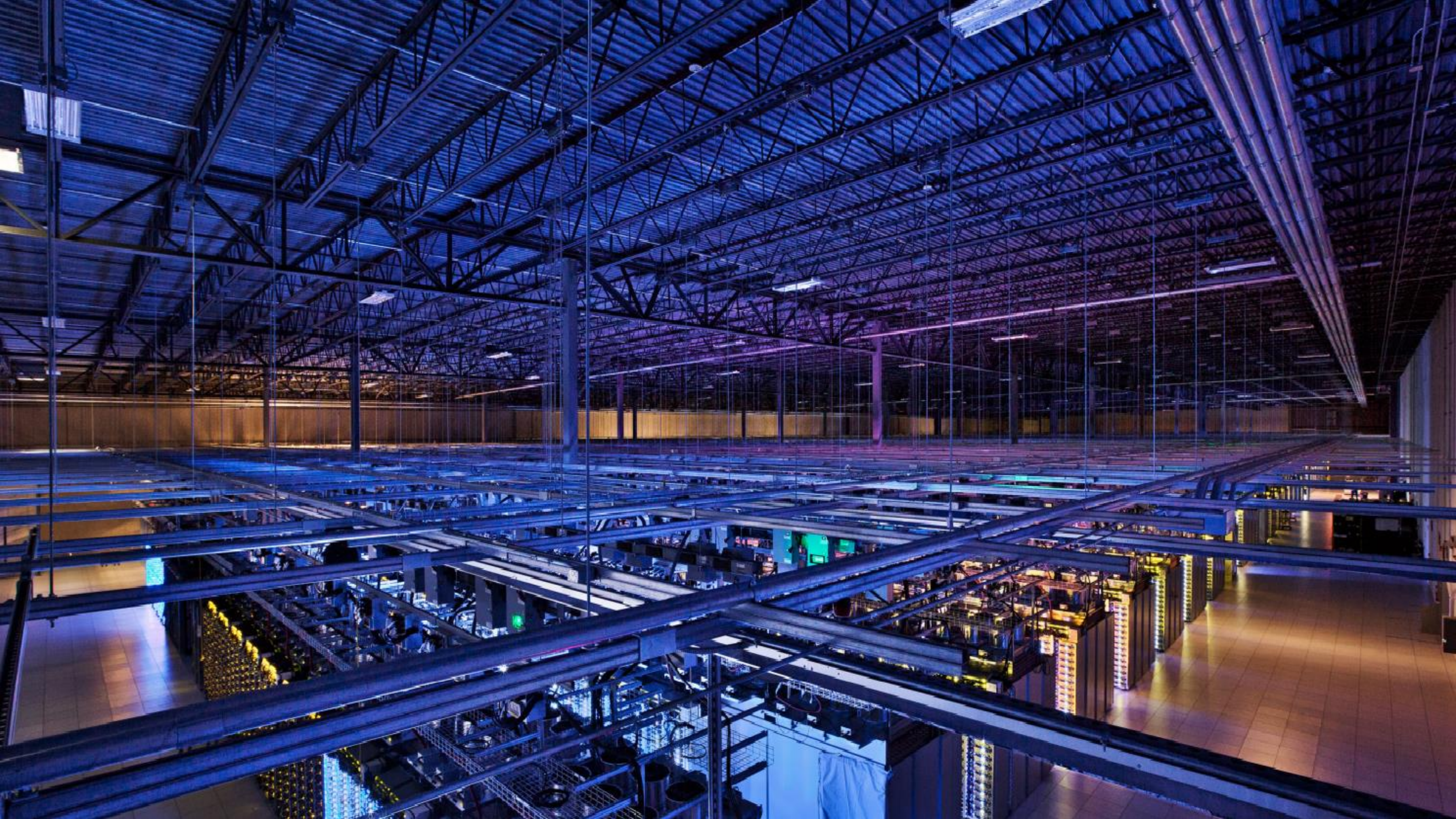
Step 2: Gollu *reloads* the cache block

Step 3: Gogo *reloads* the cache block (hit/miss)

I Use Cloud: He he he ……

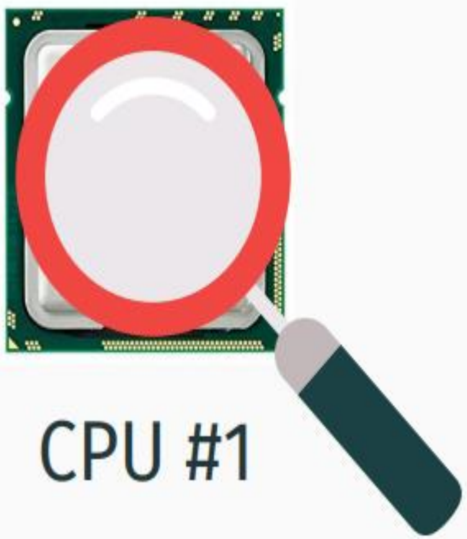
I use cloud

No fear of information leakage ??



Hmmm

Dissect It

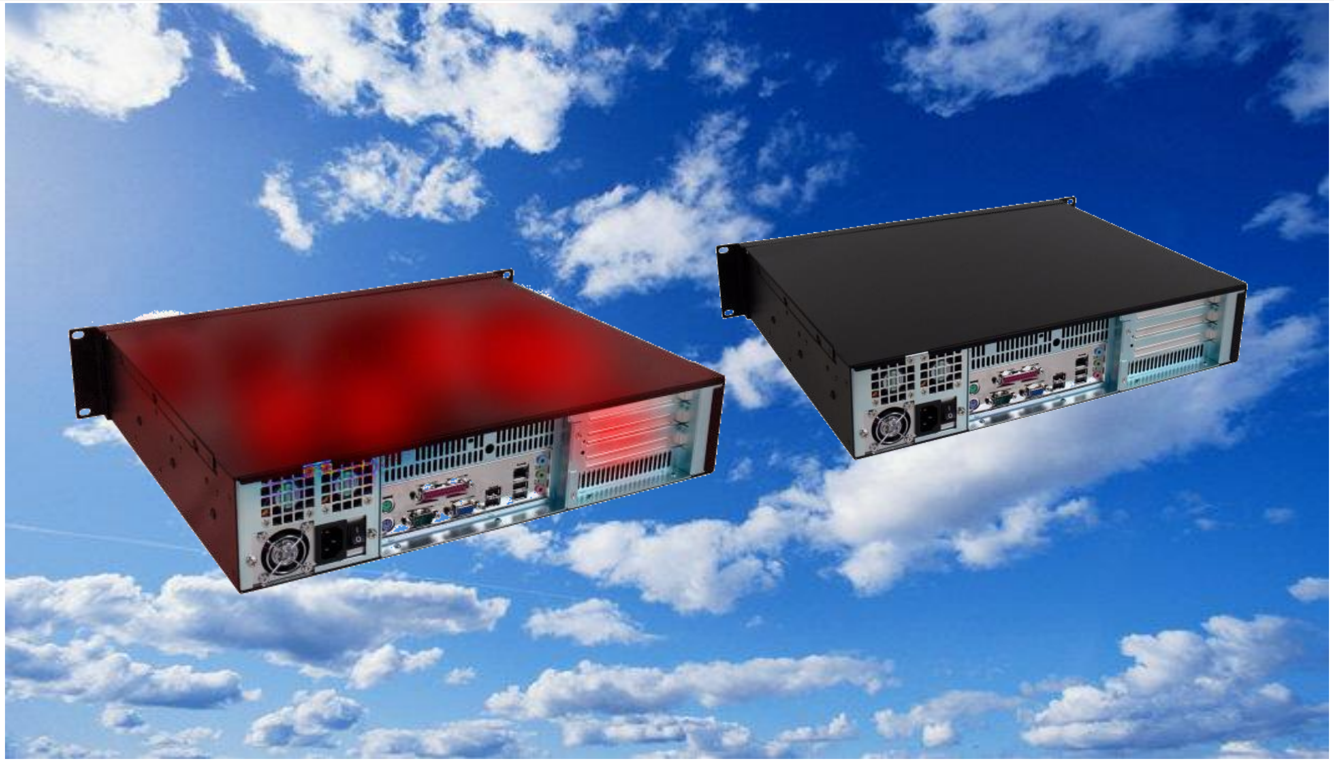


CPU #1

CPU #2

DRAM

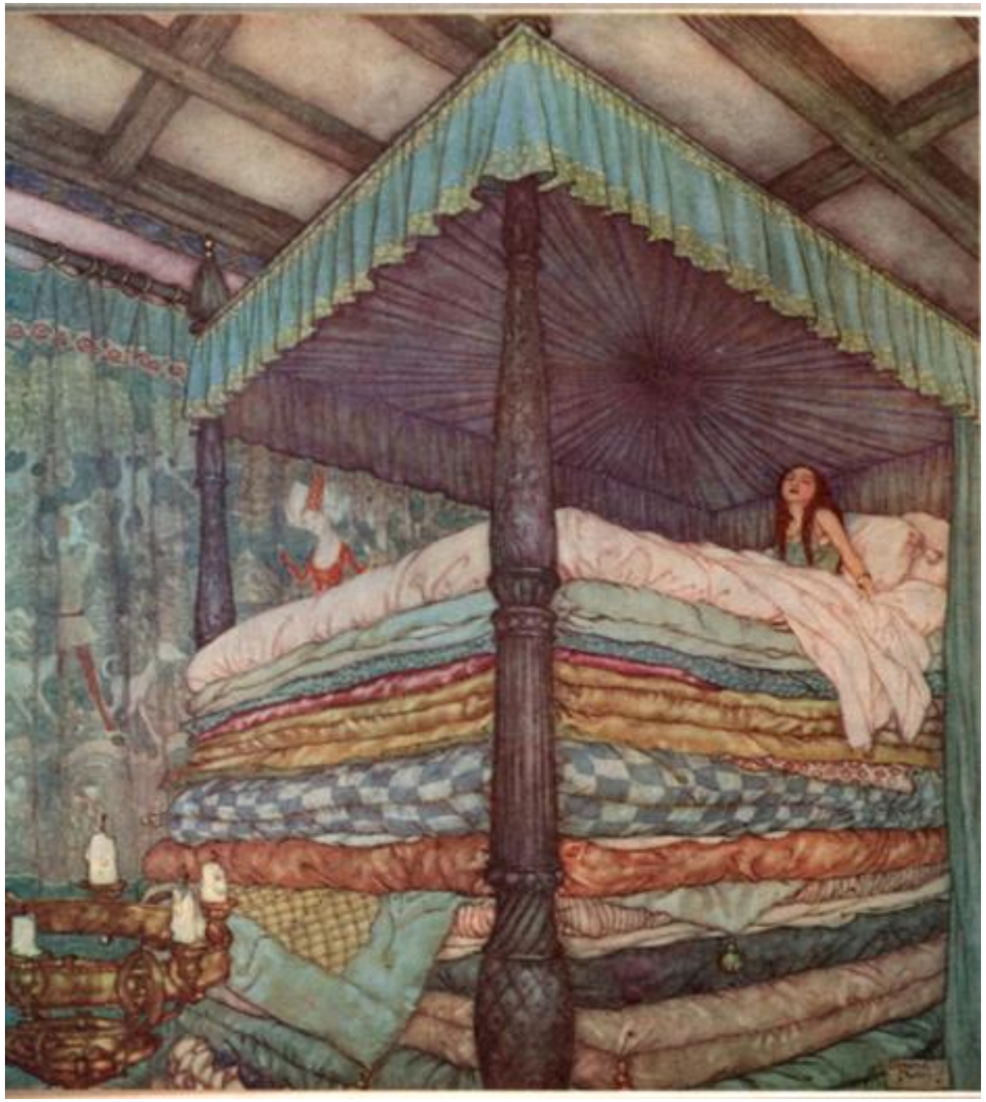
Same Problem Again!

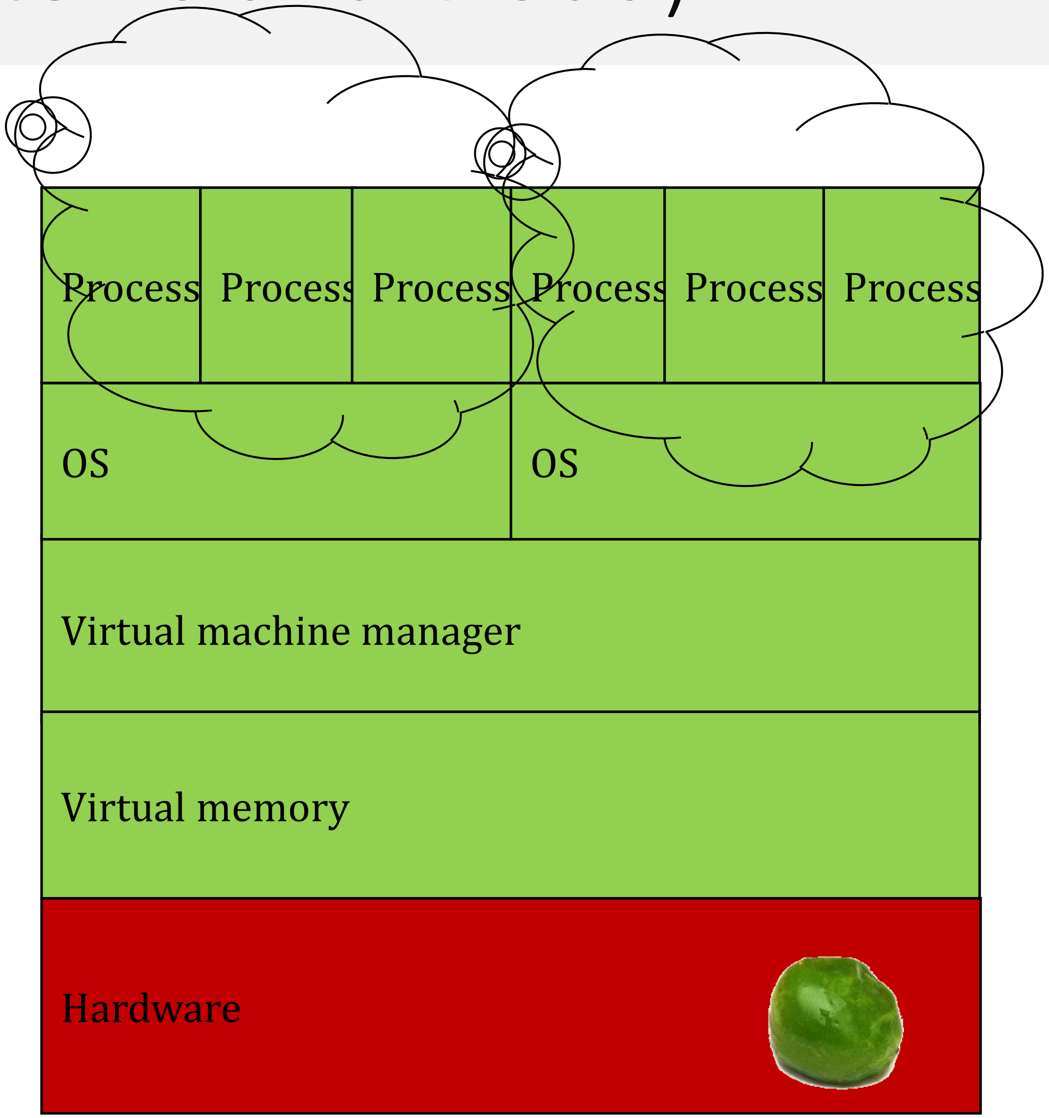


Gotcha!!

[Courtesy: Eran Tromer]

Peas and Princess (Memory Systems and Cloud)





Process | Process | Process | Process | Process | Process

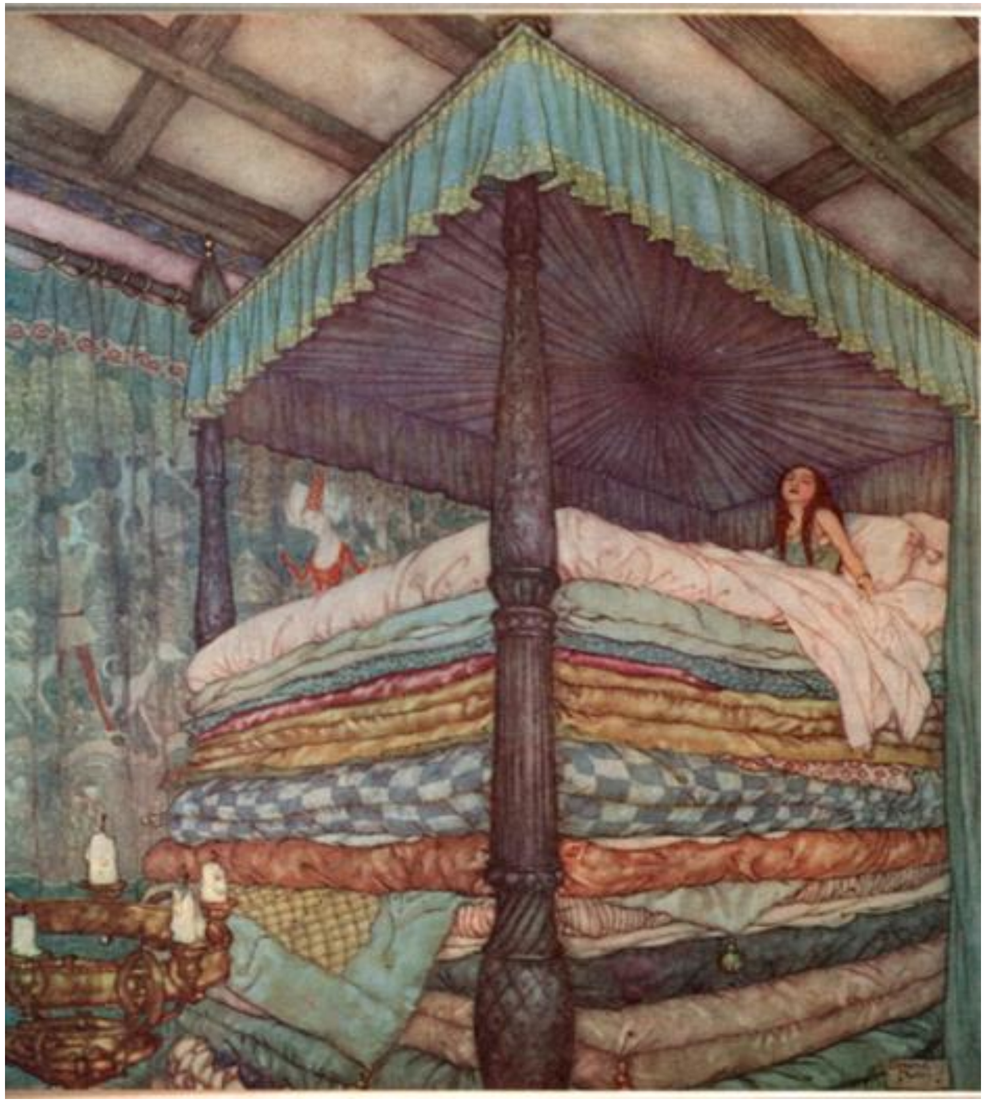
OS | OS

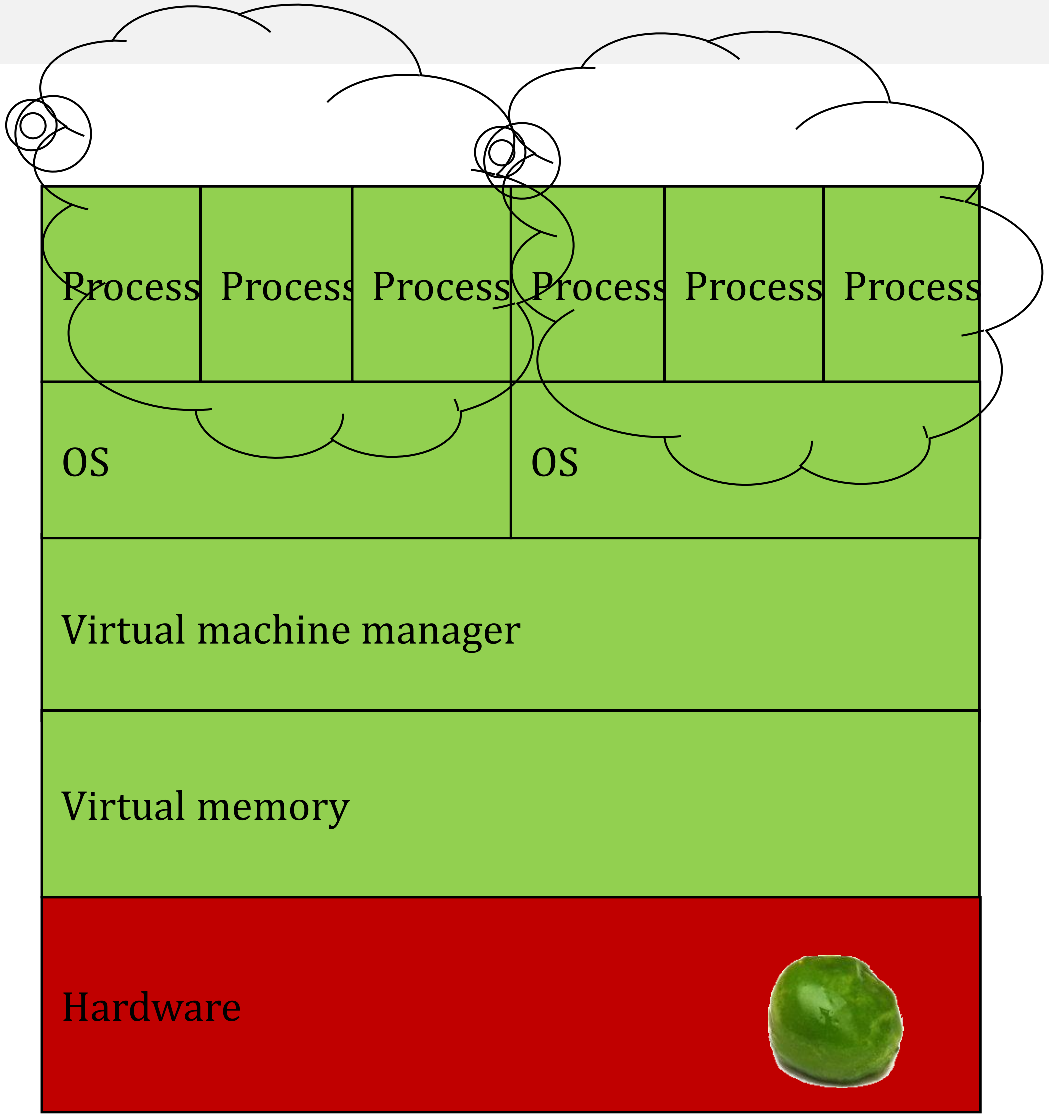
Virtual machine manager

Virtual memory

Hardware

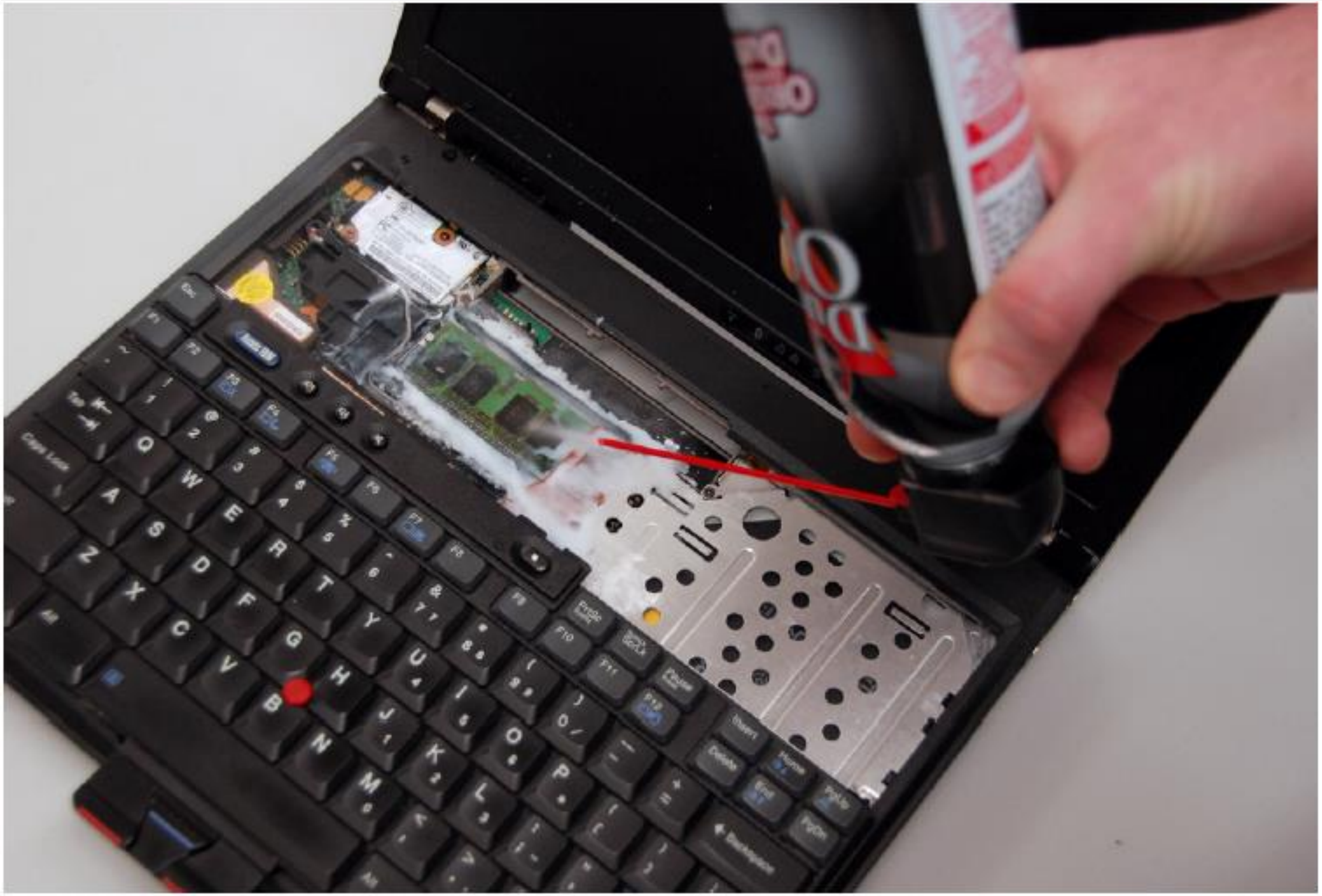
Same Story Again! Oh NO !





Process	Process	Process	Process	Process	Process
OS			OS		
Virtual machine manager					
Virtual memory					
Hardware					

Some Other Forms: Cold Boot Attacks



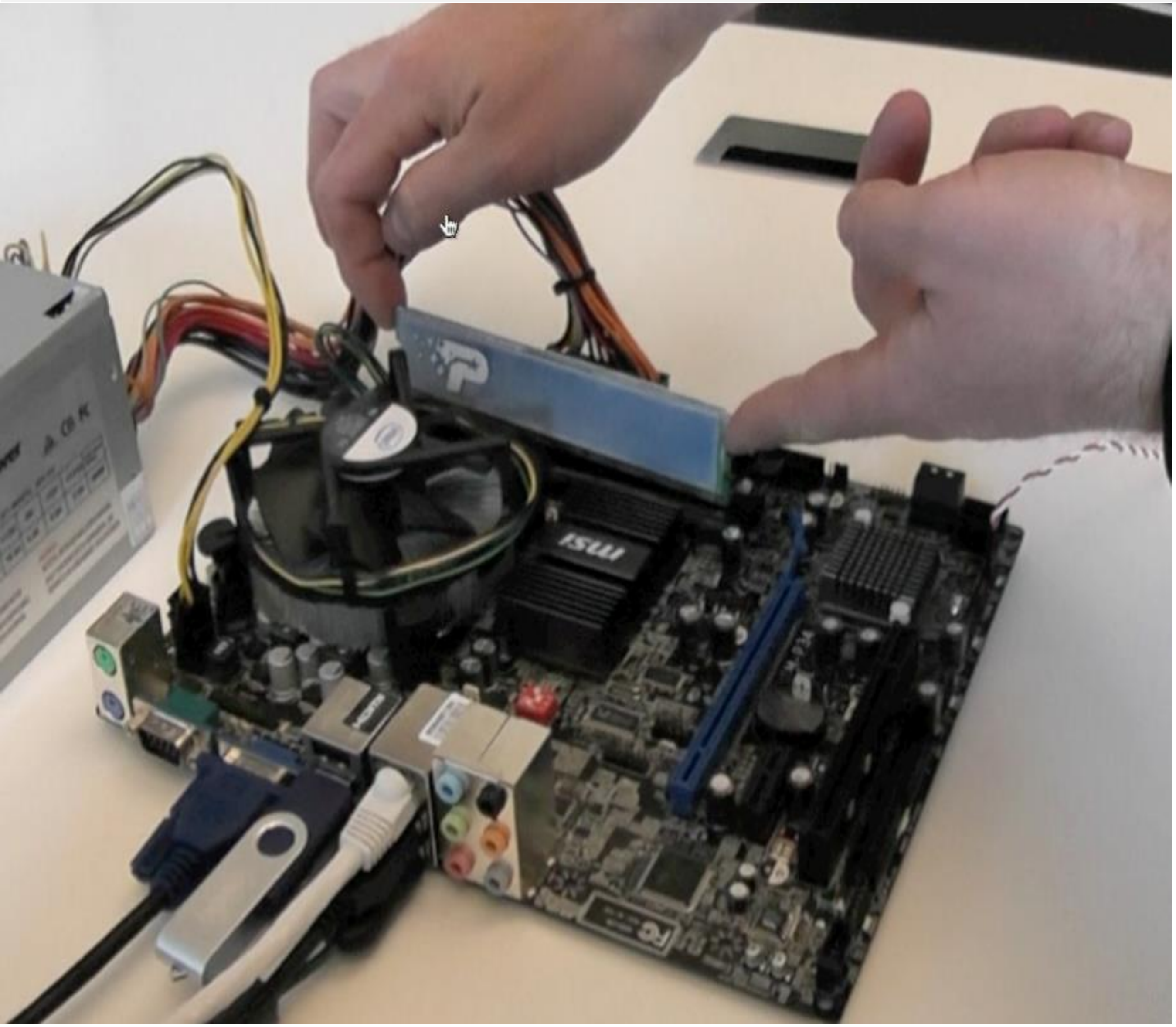
Before powering off

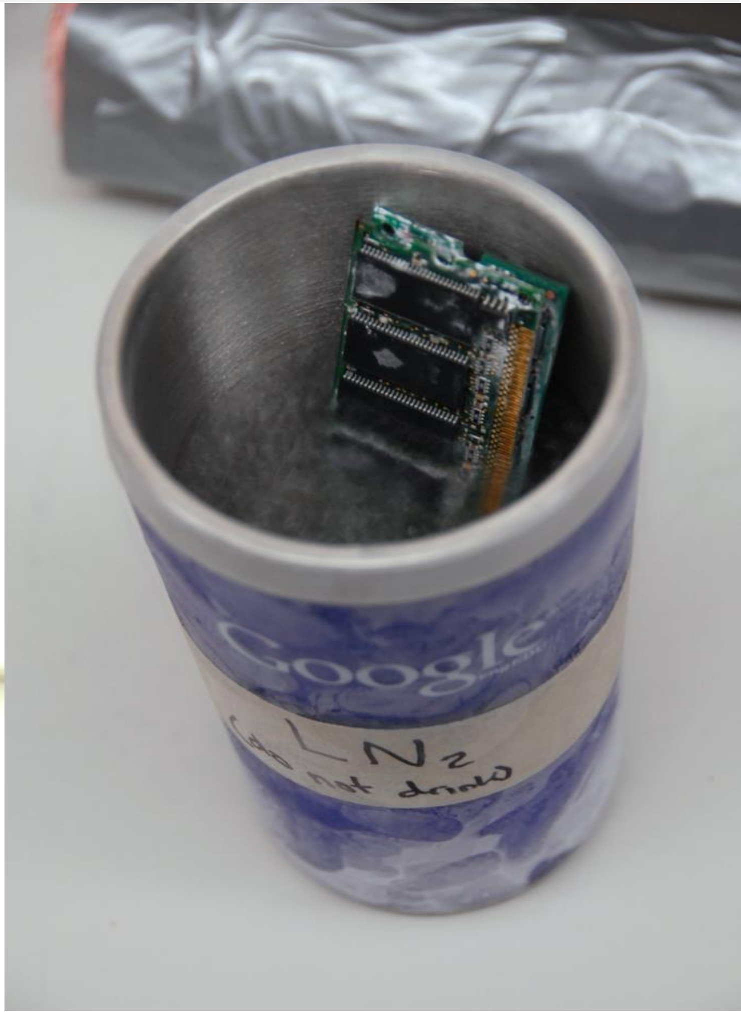
Freeze it to -50 ° C

Cool It

Esc
F1
F2
F3
Tab
Caps
START/STOP SET
MODE
SPLIT/RESET SELECT
6:48 29
GO Walkin

Put It Back



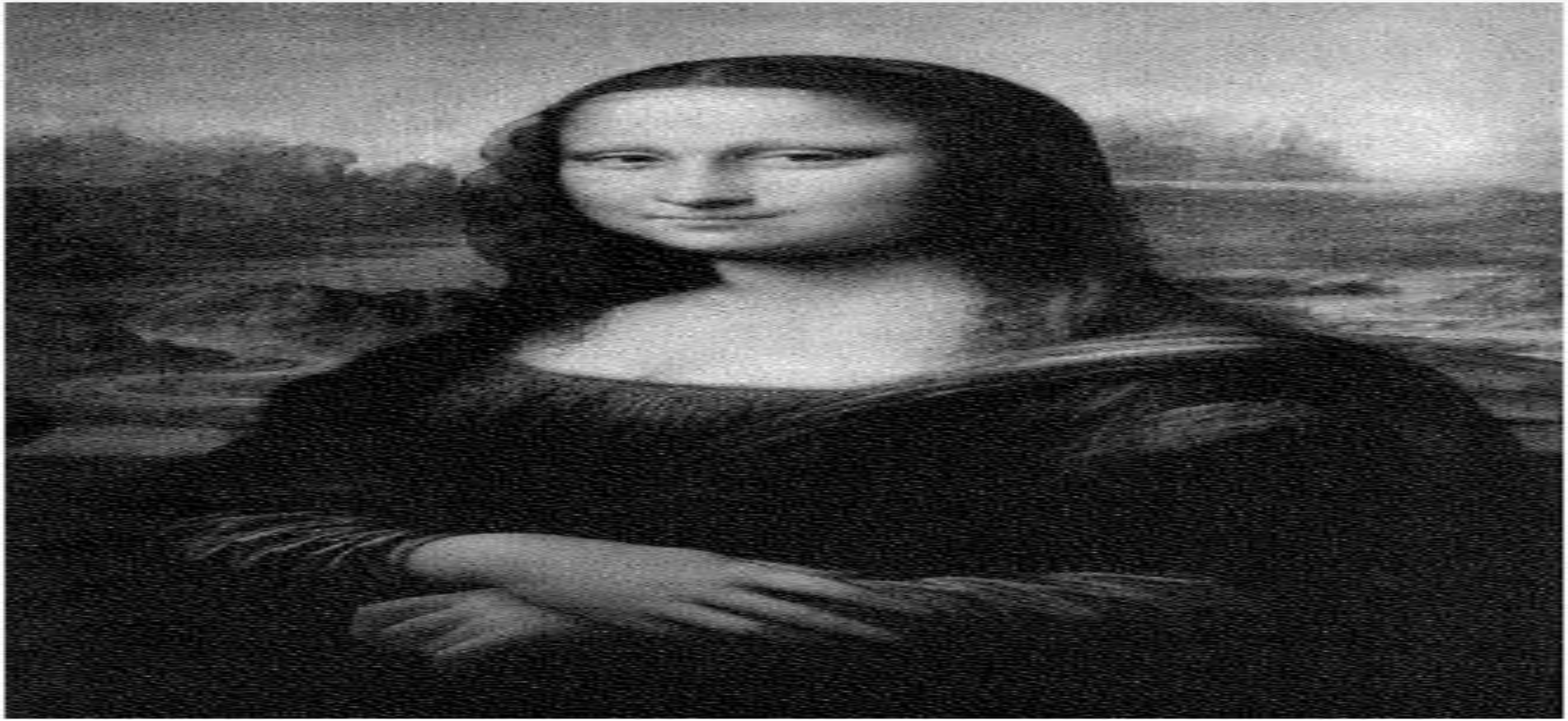


-196° C

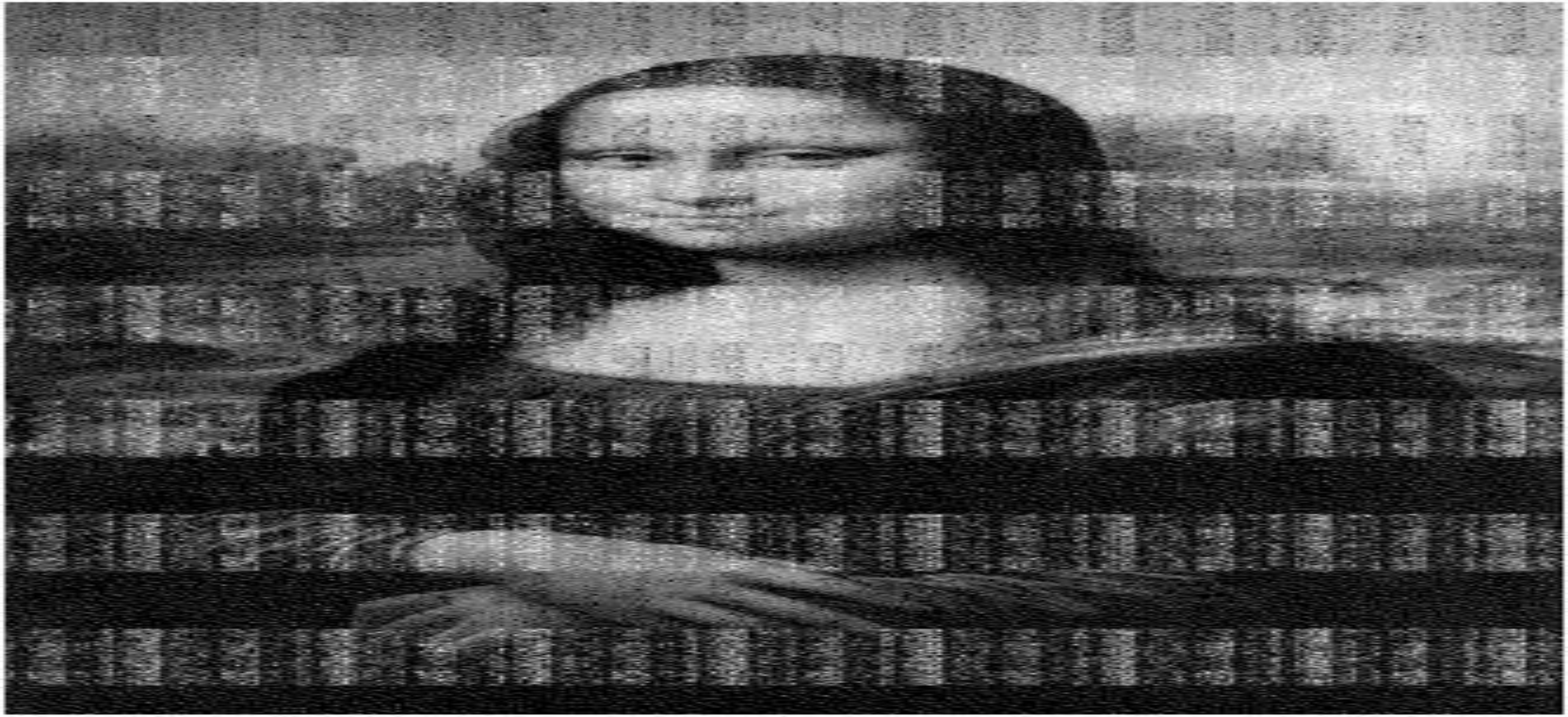
Your Password ☺

Machine	Seconds w/out power	Error % at operating temp	Error % at -50° C
A	60	41	No errors
A	300	50	0.000095
B	360	50	No errors
C	600	50	0.000036
C	120	41	0.00105
C	360	42	0.00144
D	40	50	0.025
D	80	50	0.18

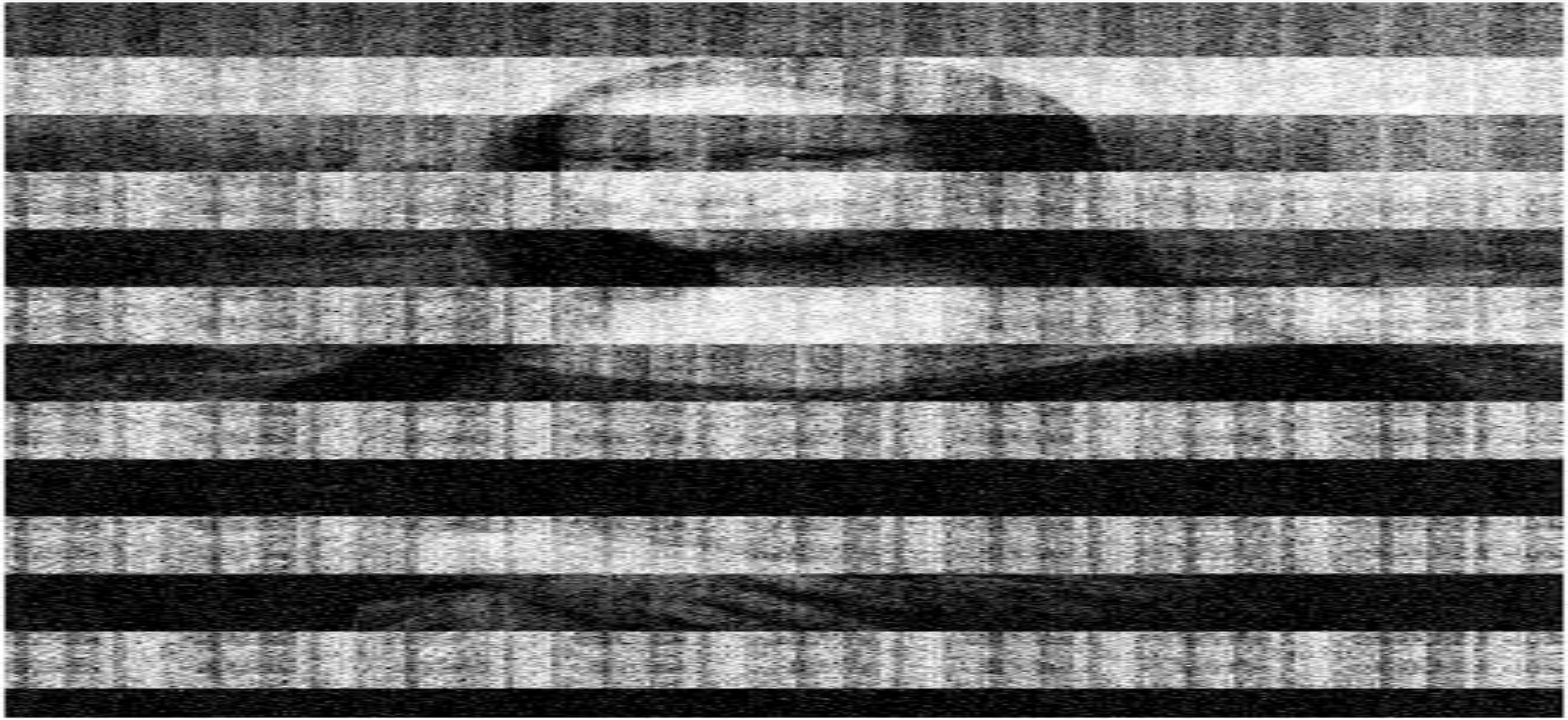
After 5 Seconds [SEC ‘08]



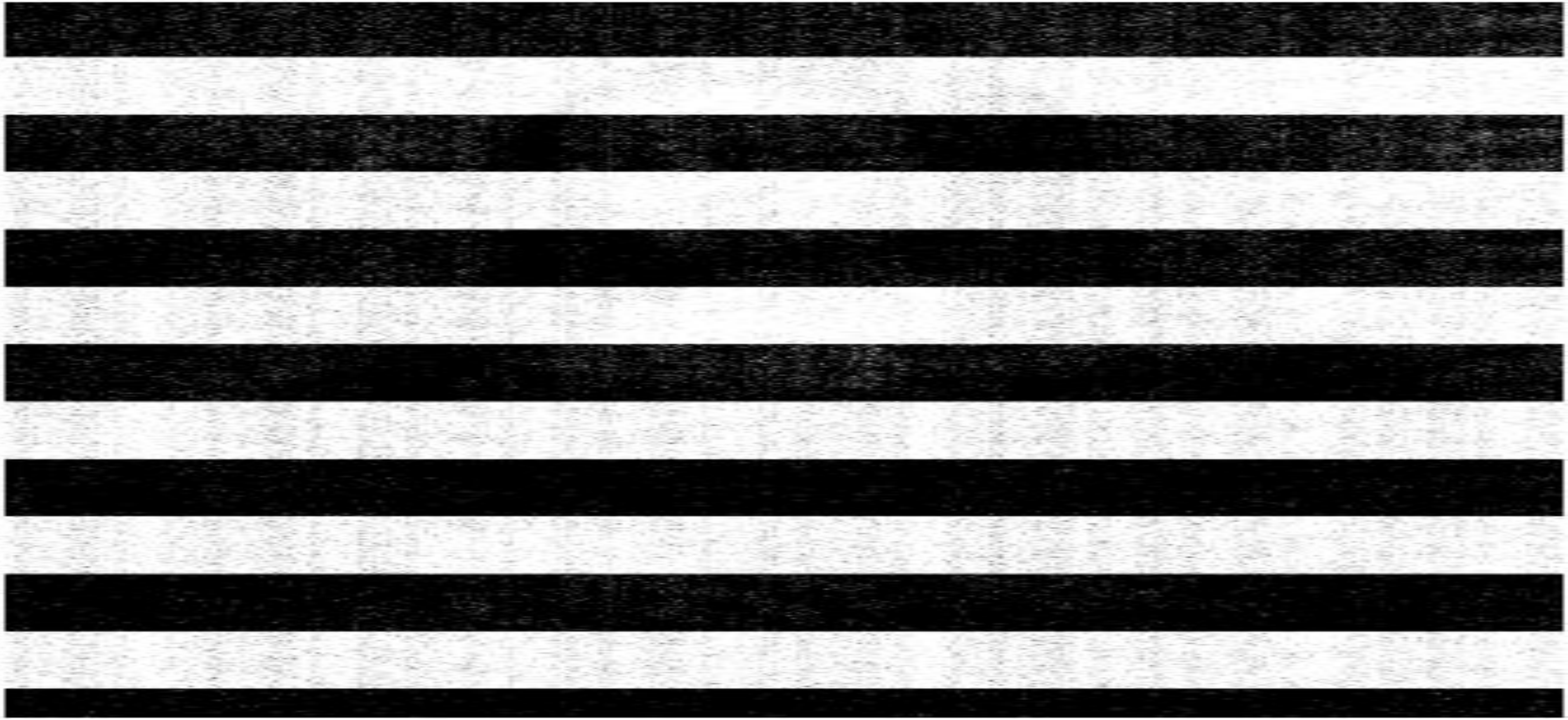
30 Seconds [SEC '08]



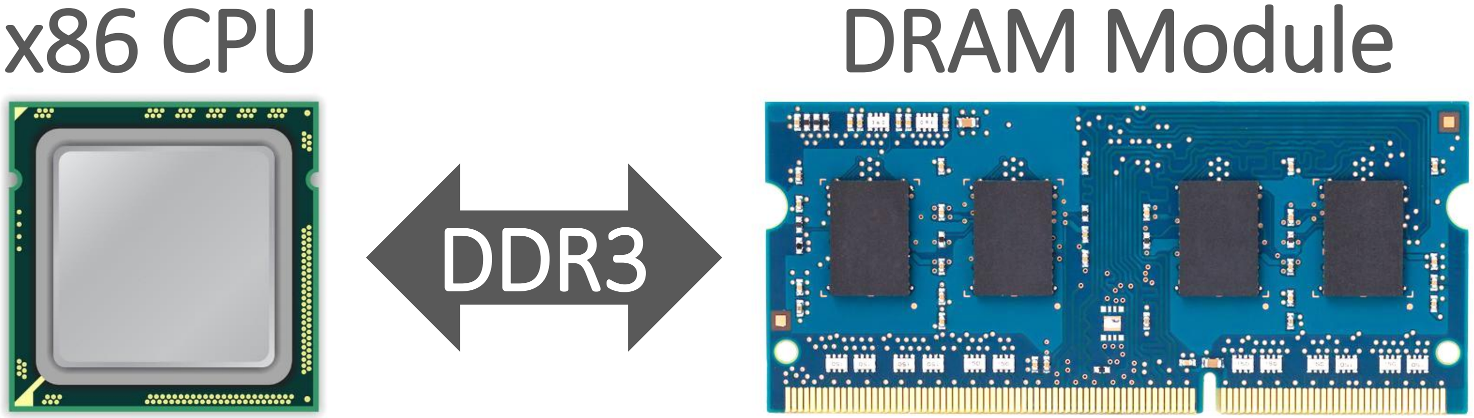
60 Seconds [SEC ‘08]



300 Seconds [SEC ‘08]

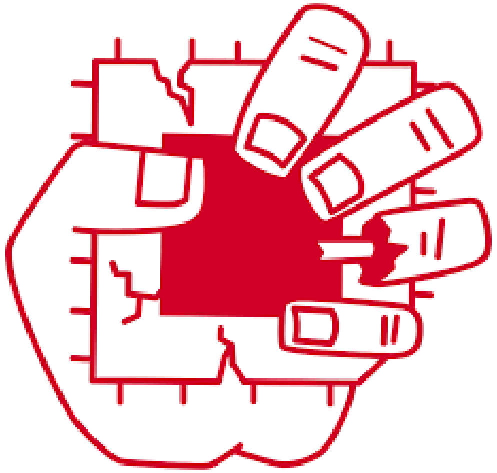


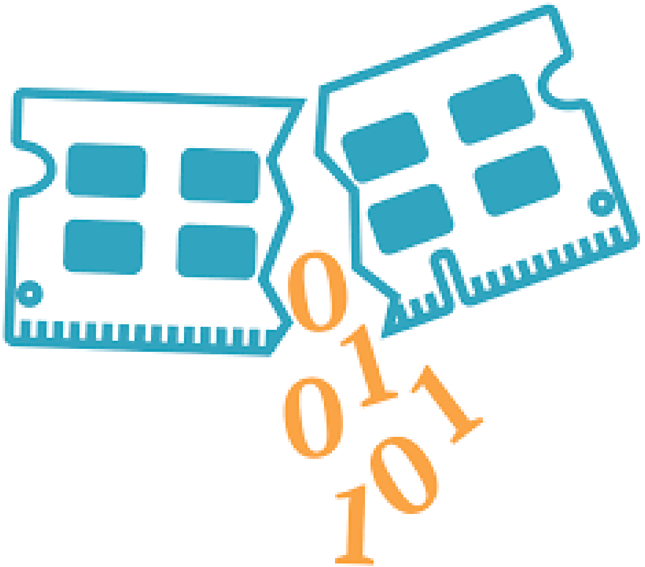
Row Hammer

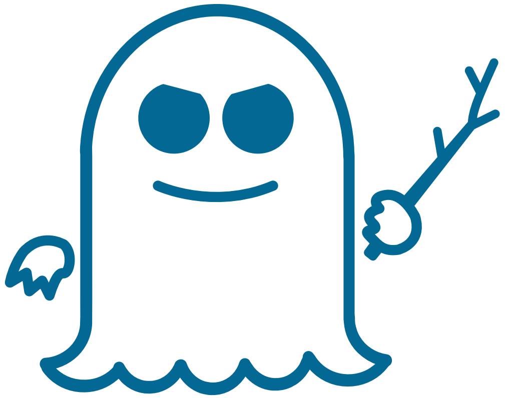


```
     111111111
x →  111111111
     111111111
     111111111
     111111111
     111111111
```

And 2018 Jan onwards







Even with the self-driving cars!! Who is Responsible? Your Memory Stupid ☺

10K feet view of CS665-Assignments

Understand different parts of memory systems

Attack different parts of memory systems

Detect these attacks

Mitigate these attacks

PS: The assignments are well-prepared this time.
We will be there ☺

Programming Assignments (Need to bring your laptop)

See for yourself an attack on a real machine

Code and build a variant of an attack

Code to reverse-engineer

Code to detect these attacks

OR ideas to mitigate these attacks

Finally:

CS665: We will learn (not you or me)

CS665: There will not be competition for exam scores
(small class, we will learn as a group (not as an individual))
Bonus points, Late submissions, learning and not racing ☺

CS665: Discussions + Hands-ons (no lectures and exams)

CS665: Discussion of basics + SOTA on secure memory systems

CS665:Have fun while learning

Next Lecture: Basics first

Autobiography of Memory Read/Write

Long long ago, …… there was a memory read named LOAD …….

Then Caches

So Brush up your basics

Few Non-maskable interrupts

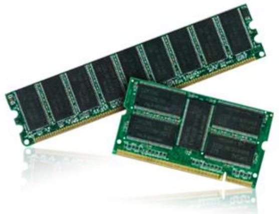
- A trip in August : 10 to 12 days (personal NMI) : two to three lectures
- A trip to US in Sept. : five to seven days (professional NMI): two lectures
- A trip to IIX in October: one to two days (professional again, trying my best to make CS665 unaffected)
- Can we get one or two within next 10 days? Academic load will be lighter compared to later. This Saturday for an hour on hands-on?

Assignment-0

ASSIGNMENT-0

Submit it by tomorrow night (11:59 PM)

Have fun !! I am excited !! What about you ?

May the secure  be with you

“It takes two to speak the truth - one to speak and another to hear” - **Henry David Thoreau**

Thank You &

Have a Good day