ITLA
INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS
Las Americas Institute of Technology

ITLA SECURITY FEST 2019

CENTRO DE SEGURIDAD INFORMÁTICA Y COMPUTACIÓN FORENSE

TECNOLOGIA DE LA INFORMACION

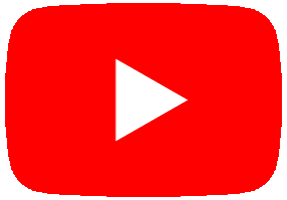
3RA FERIA ACADÉMICA DE REDES Y SEGURIDAD INFORMÁTICA
DEL 16 AL 18 DE OCTUBRE.

Pentesting Utilizando AI

Julio Ureña (PlainText)

net user plaintext

- Julio Ureña
- Cristiano / Esposo / Padre / Amigo
- Ingeniero en Sistemas
- OSCP
- Twitter: @JulioUrena
- Blog: https://plaintext.do
- YouTube: https://www.youtube.com/c/JulioUreña



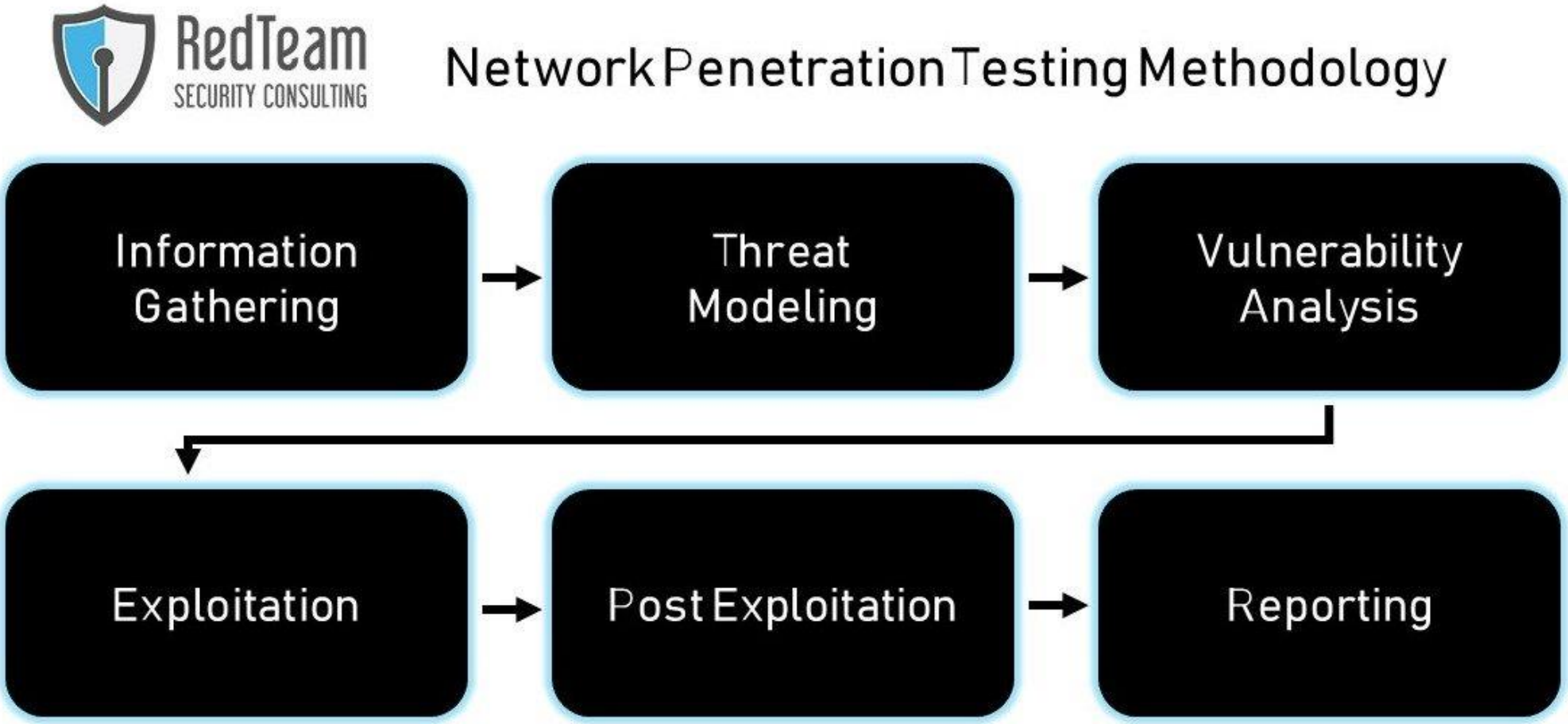
ITLA INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS
Las Americas Institute of Technology

ITLA SECURITY FEST 2019

Agenda

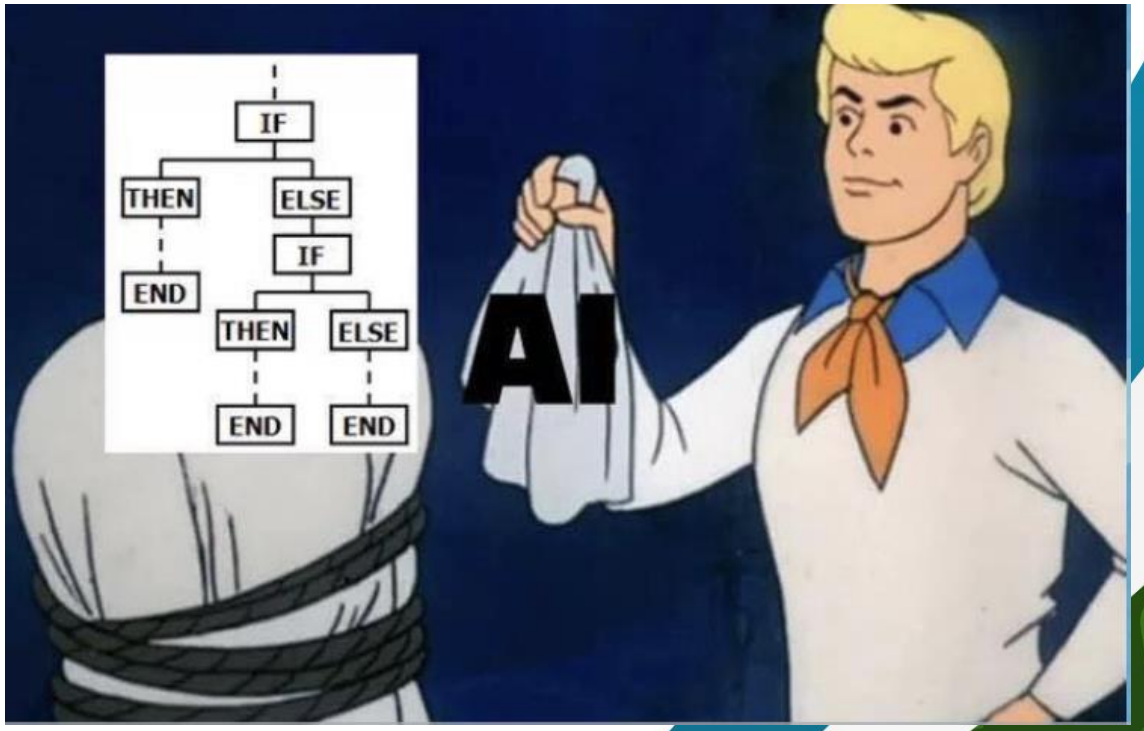
- ❑ Pentesting.
- ❑ ¿Qué es AI?
- ❑ Deep Learning 101
- ❑ Frameworks de AI
- ❑ Bypass CAPTCHA usando AI

¿Qué es Pentesting?



https://www.redteamsecure.com/network-penetration-testing-methodology/

¿Qué es AI?

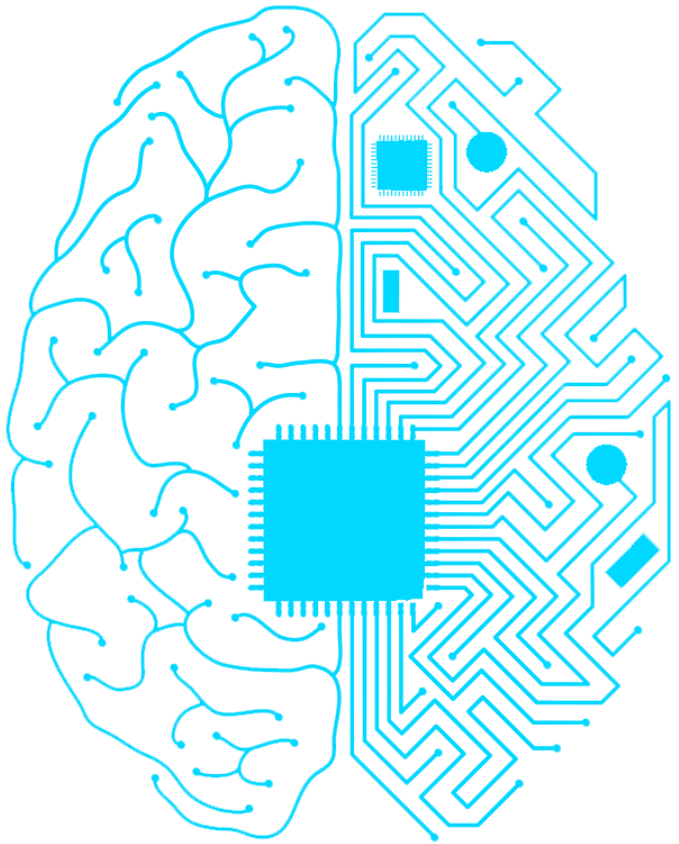


¿Qué realmente es AI?

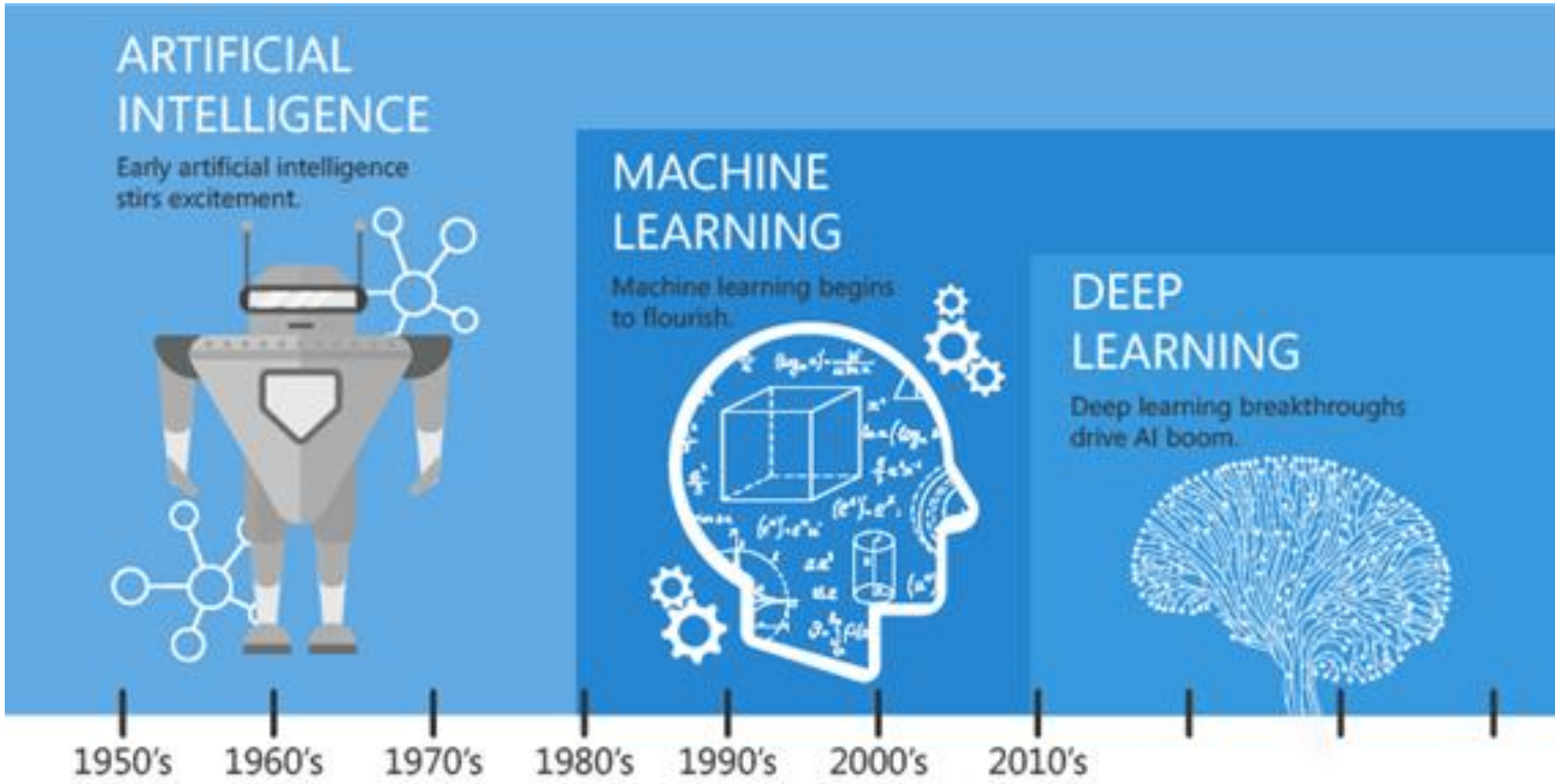
- Es la idea de crear una **computadora** que tenga la capacidad de **pensar** como un ser humano.

Cerebro vs **AI**

- Lógica, Cálculos, Análisis
- Contexto
- Emociones, Razón, Creencias



Historia de la Inteligencia Artificial

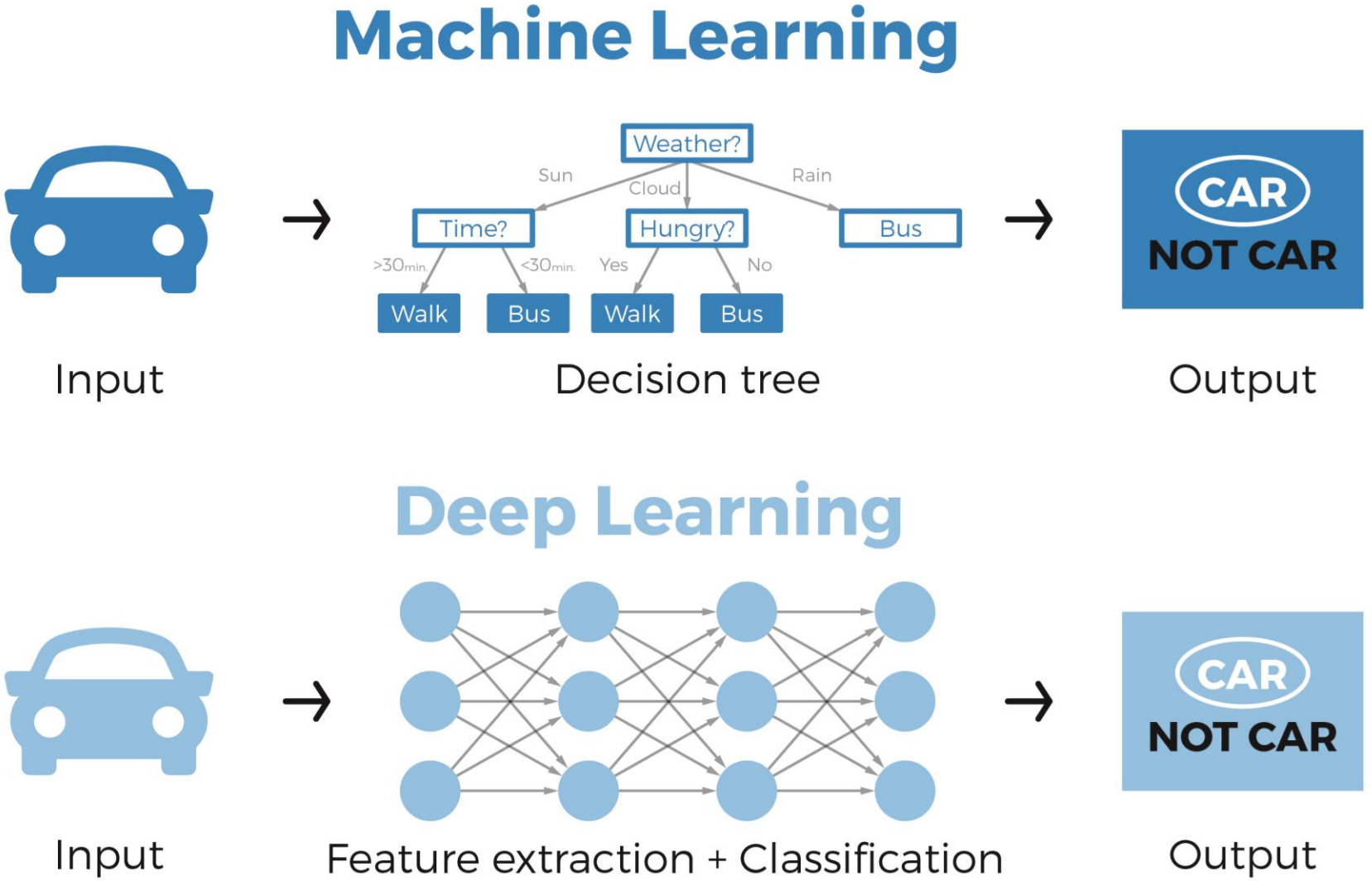


Since an early flush of optimism in the 1950's, smaller subsets of artificial intelligence - first machine learning, then deep learning, a subset of machine learning - have created ever larger disruptions.

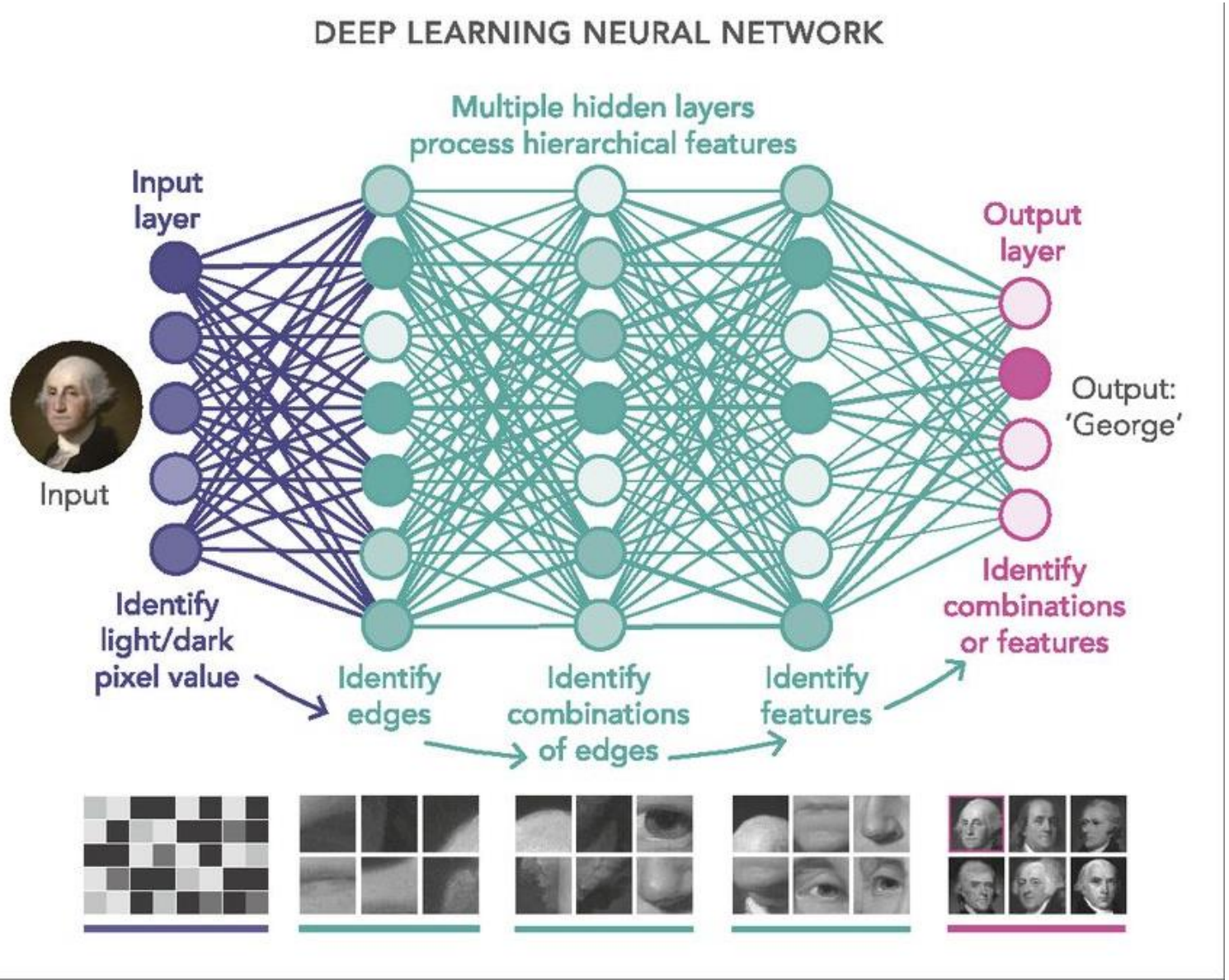
Expectativas…
AI / ML / DL – Toma tiempo entenderlo

Pero tendrán las herramientas y la tarea de hackear usando AI ☺

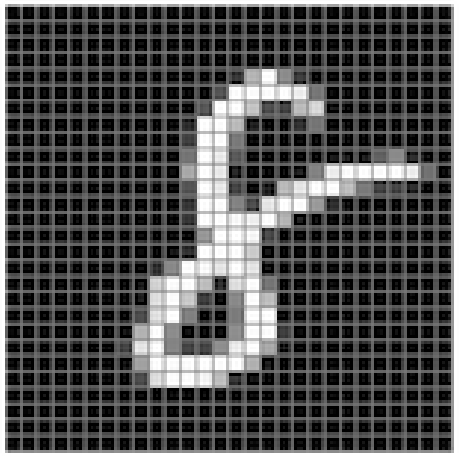
Deep Learning

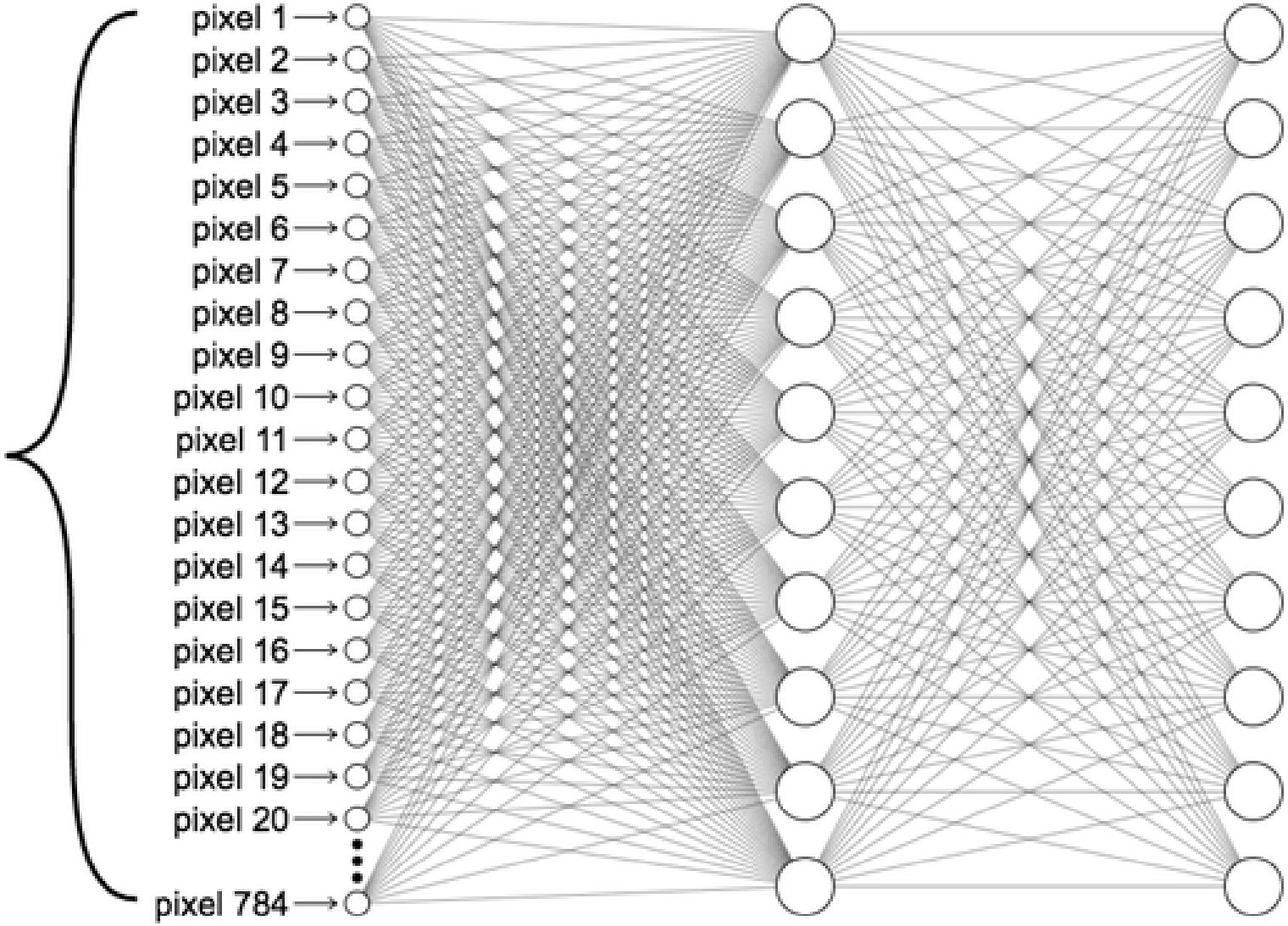


Deep Learning

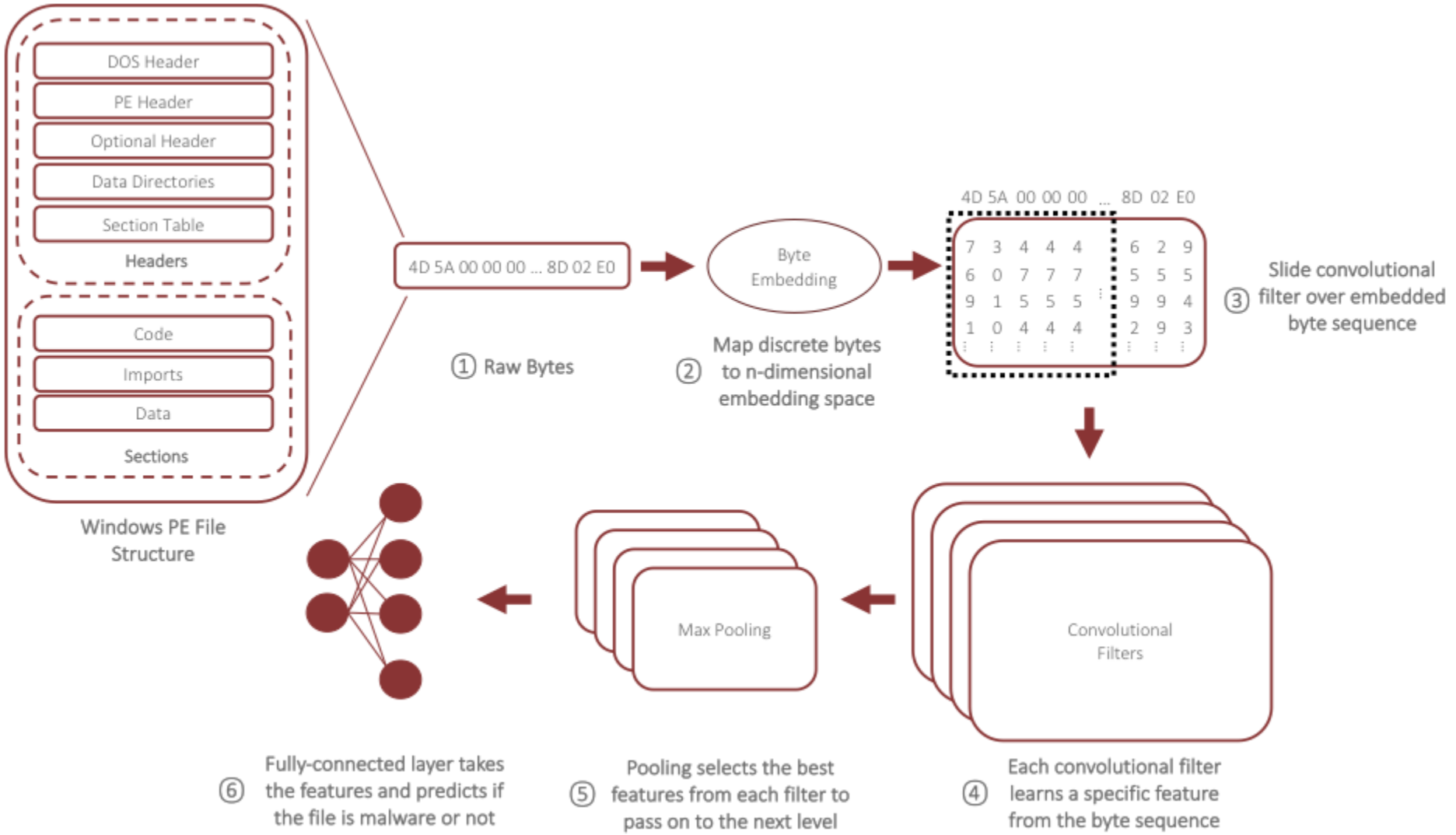


Deep Learning





Deep Learning

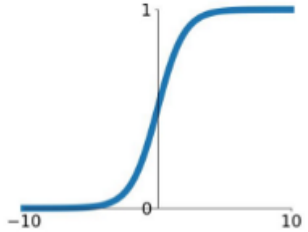


Deep Learning

Activation Functions

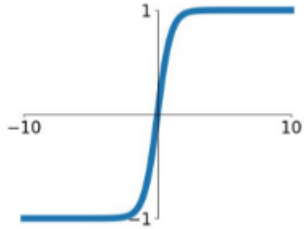
Sigmoid

$$\sigma(x) = \frac{1}{1+e^{-x}}$$



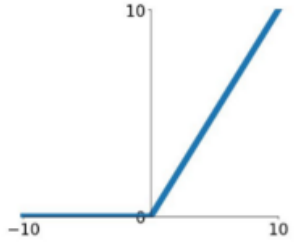
tanh

$$\tanh(x)$$



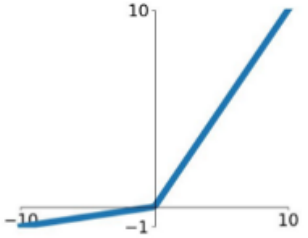
ReLU

$$\max(0, x)$$



Leaky ReLU

$$\max(0.1x, x)$$

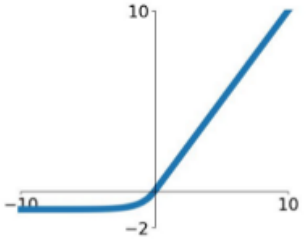


Maxout

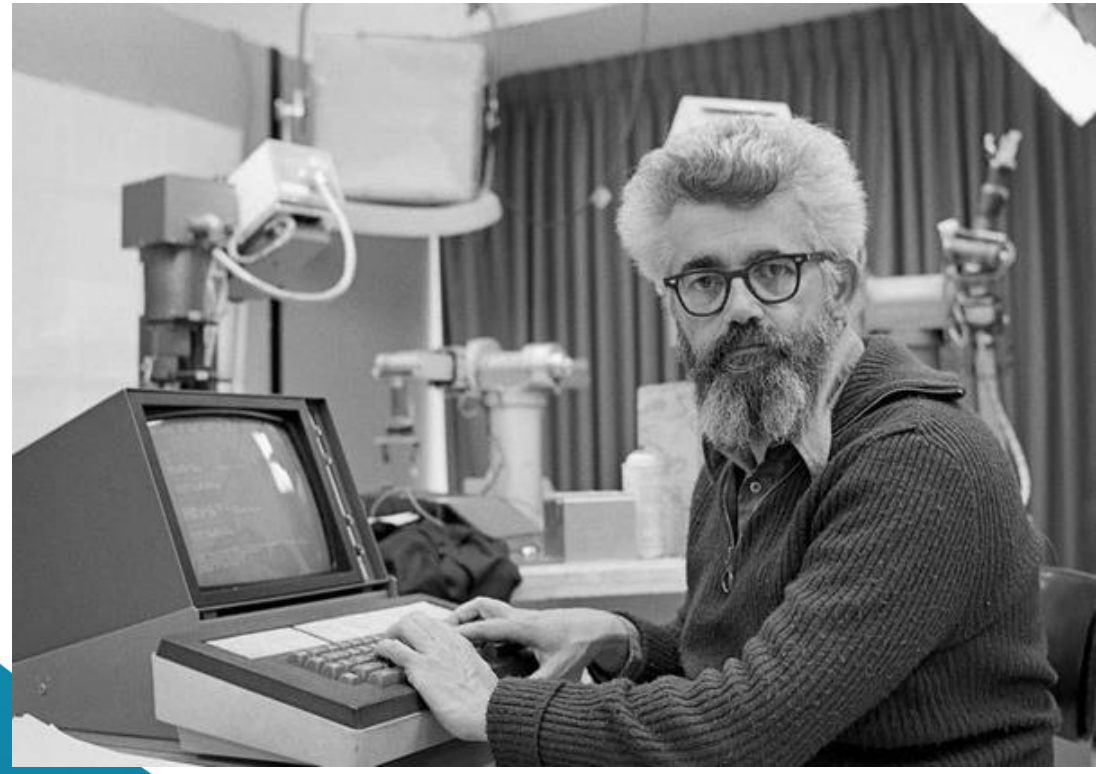
$$\max(w_1^T x + b_1, w_2^T x + b_2)$$

ELU

$$\begin{cases} x & x \geq 0 \\ \alpha(e^x - 1) & x < 0 \end{cases}$$



Deep Learning

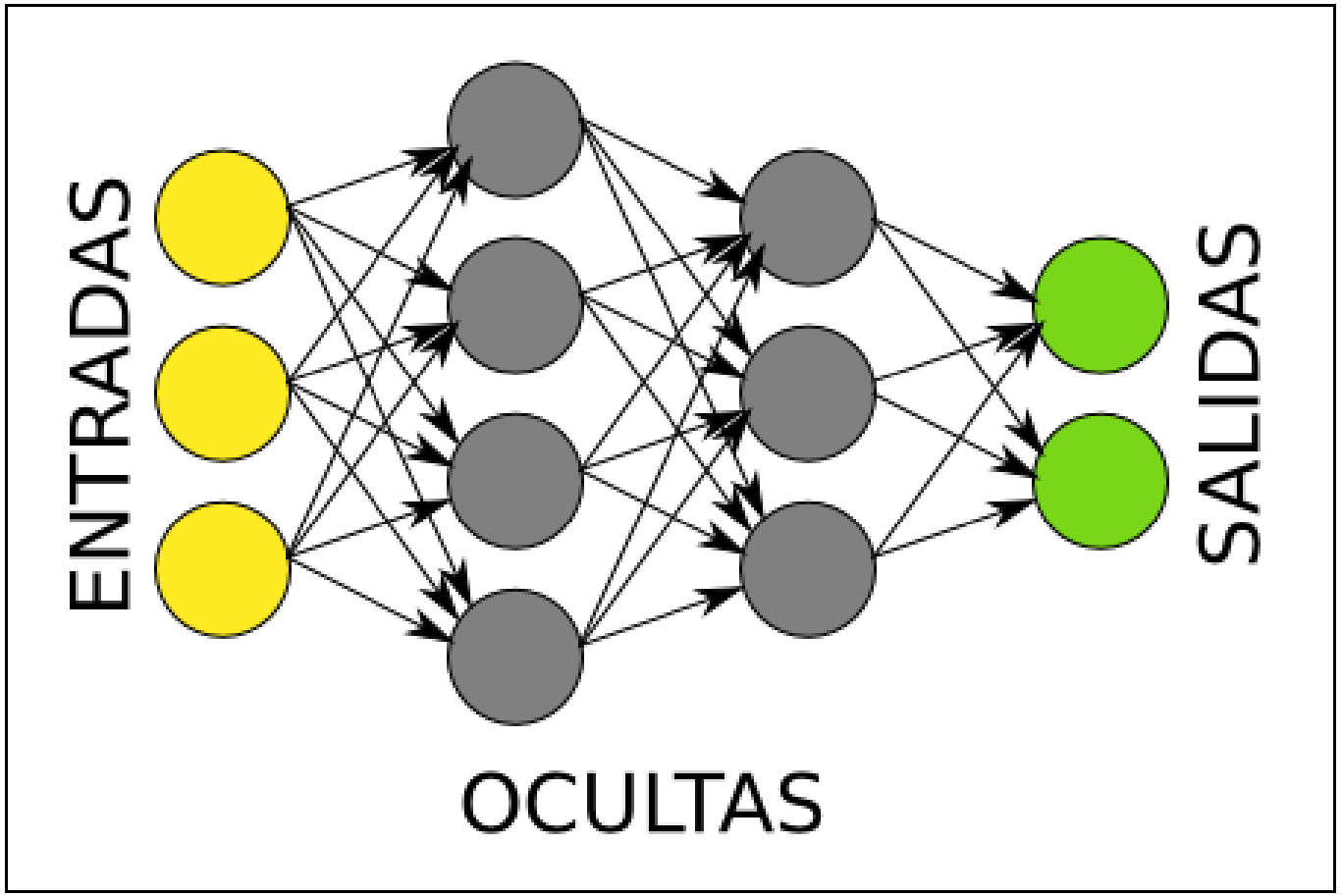


En 1956, John McCarthy, considerado el padre de la IA, organizó la conferencia Dartmount que reunió a los fundadores de la AI y las bases para el futuro de la investigación de la AI.

The Logic Theorist, considerado por muchos como el primer programa de IA, fue desarrollado en 1956.

Deep Learning 101

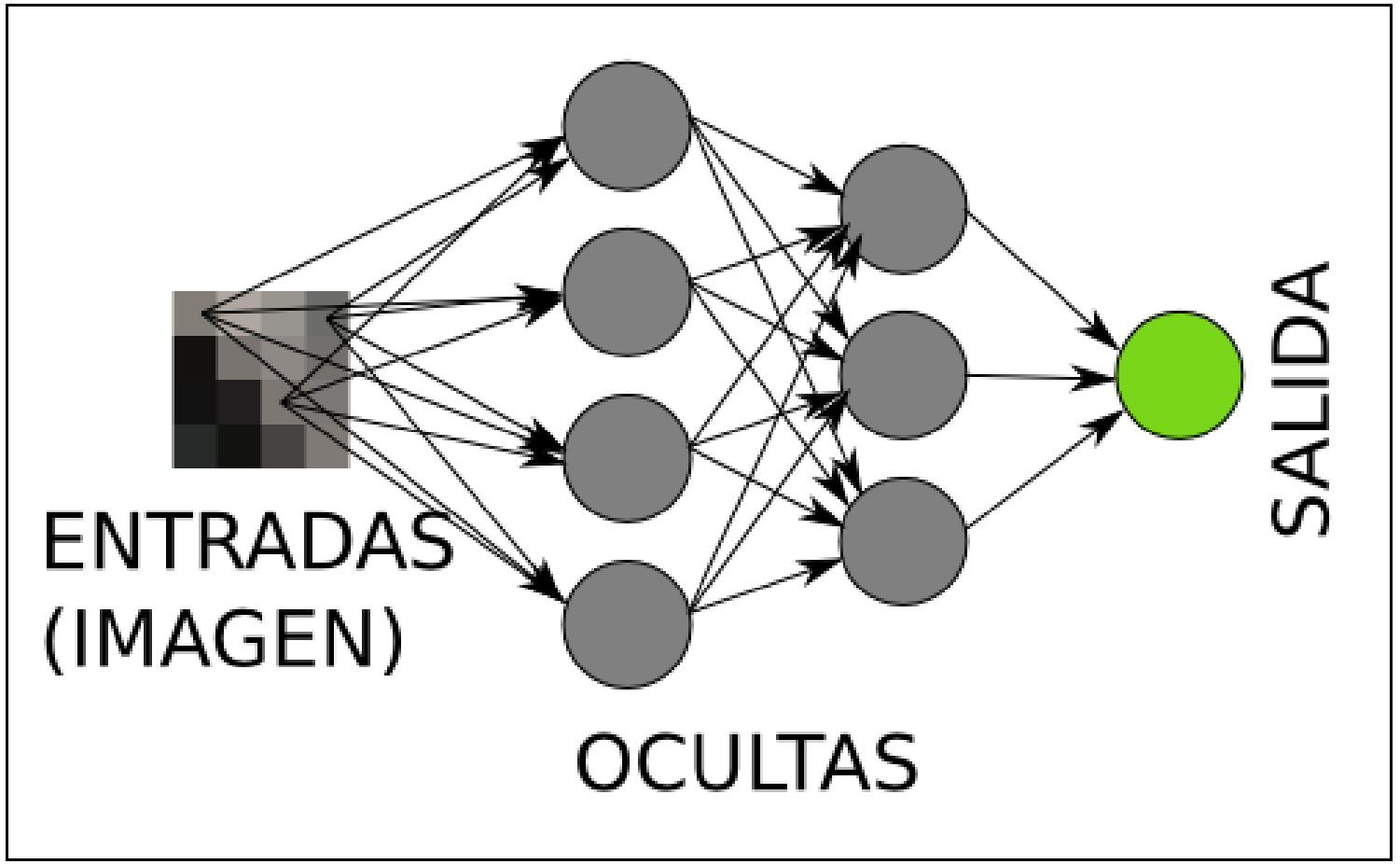
Arquitectura



- https://rubenlopezg.wordpress.com/2014/05/07/que-es-y-como-funciona-deep-learning

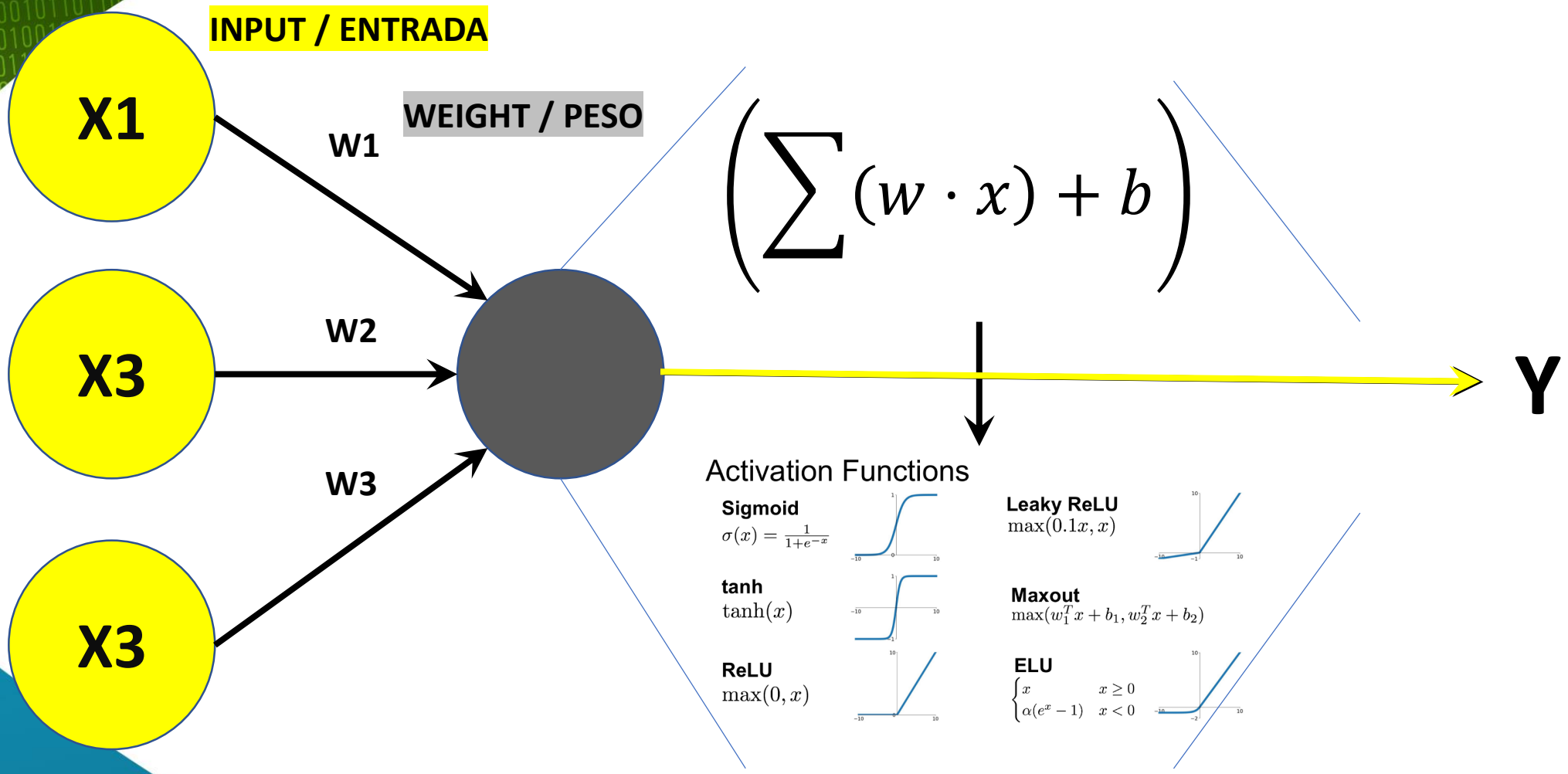
Deep Learning 101

Arquitectura

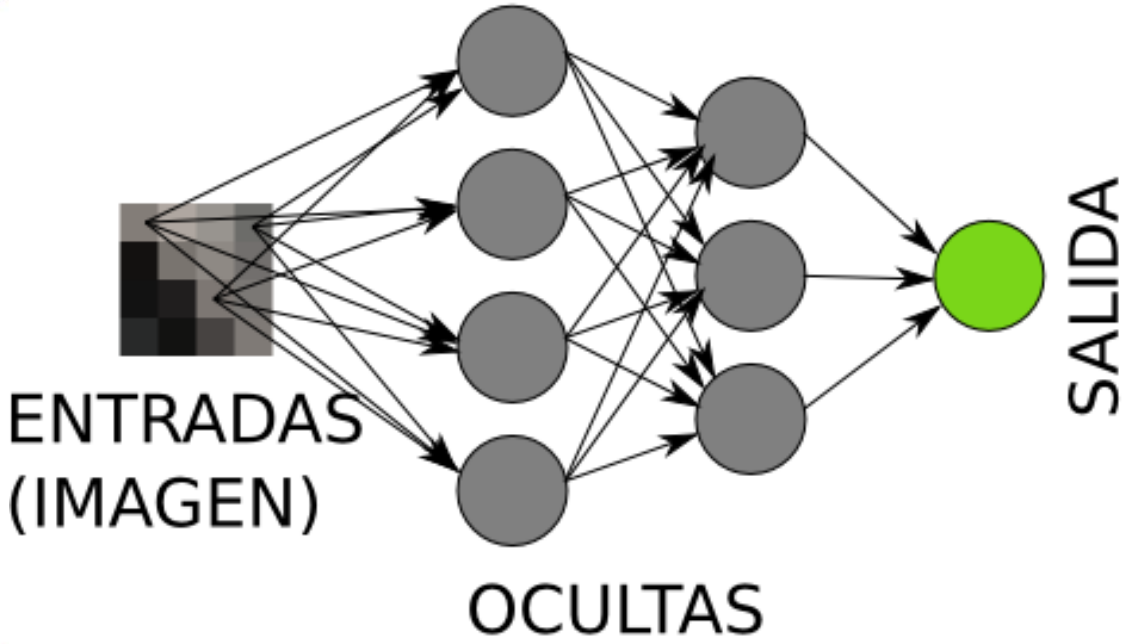


- https://medium.com/@adriaciurana/aprende-deep-learning-en-10-minutos-e4e9e8950cd8

Neurona Artificial

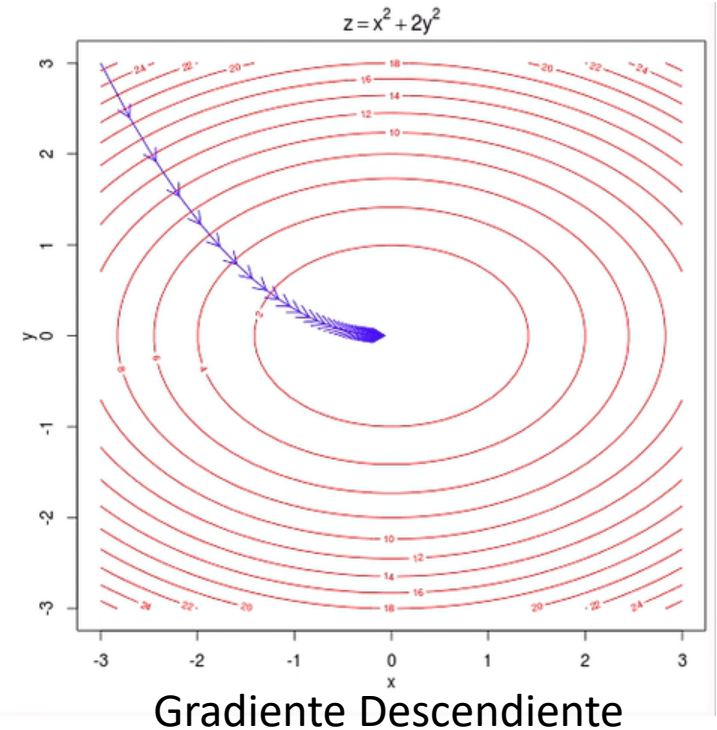


Entrenamiento de Red Neuronal



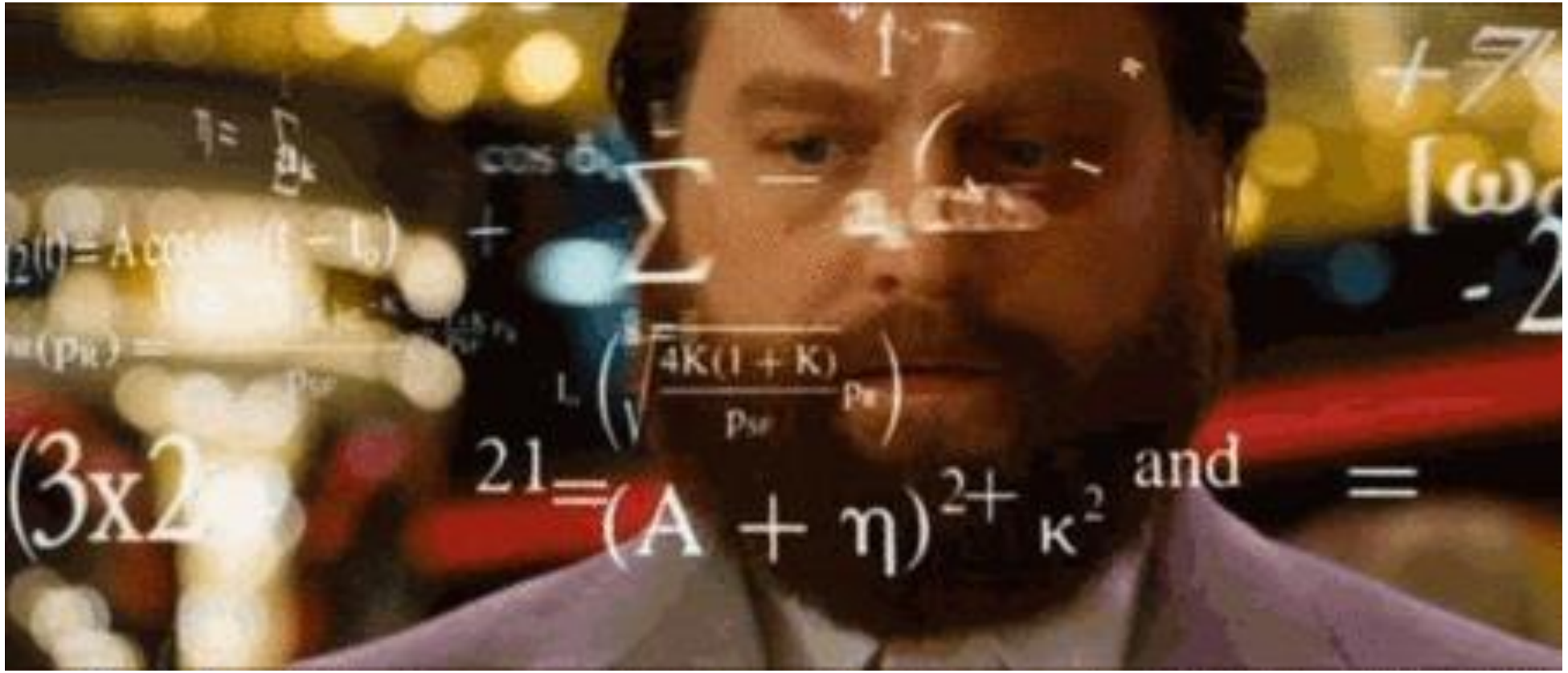
Error cuadrático medio

$$MSE = \frac{1}{M}\sum_{i=1}^{M}(real_i - estimado_i)^2$$

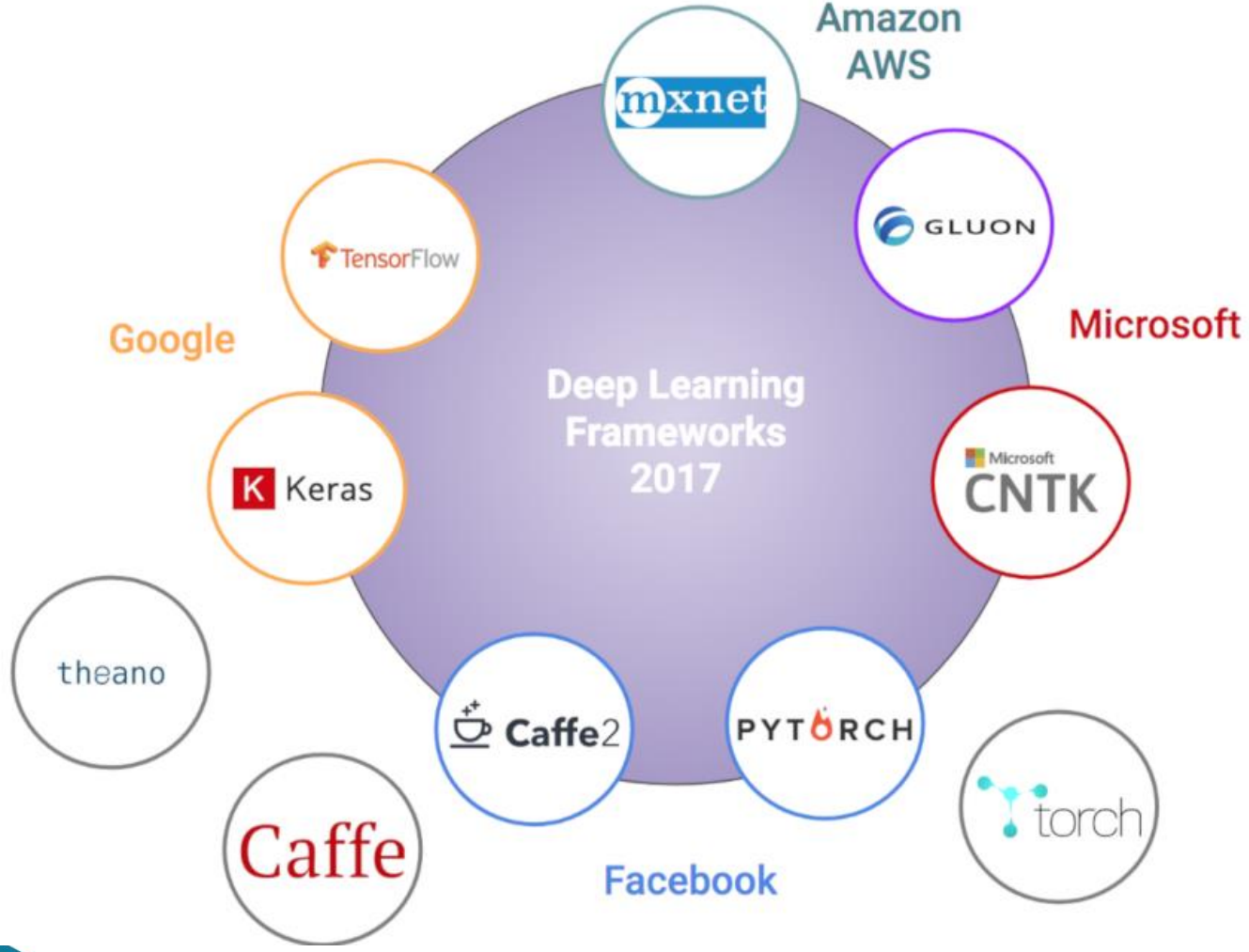


Gradiente Descendiente

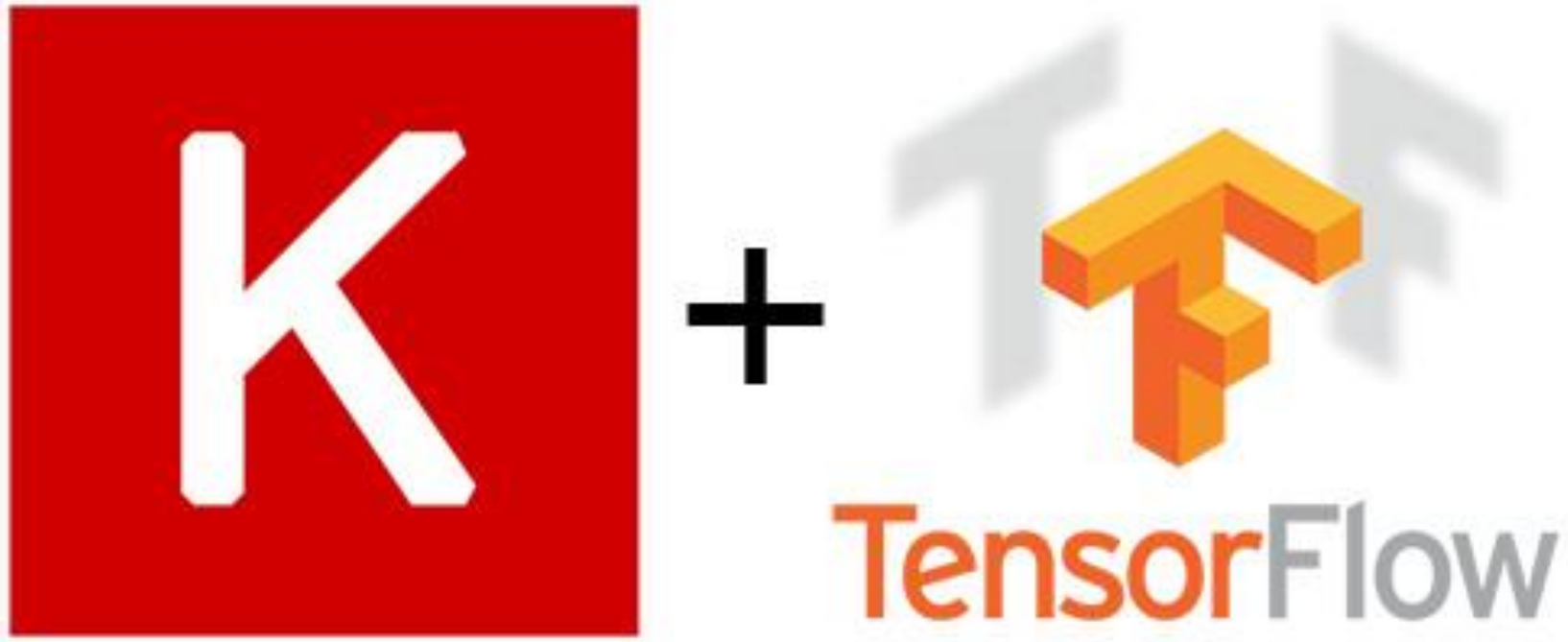
Ya soy un experto en AI



Deep Learning Frameworks



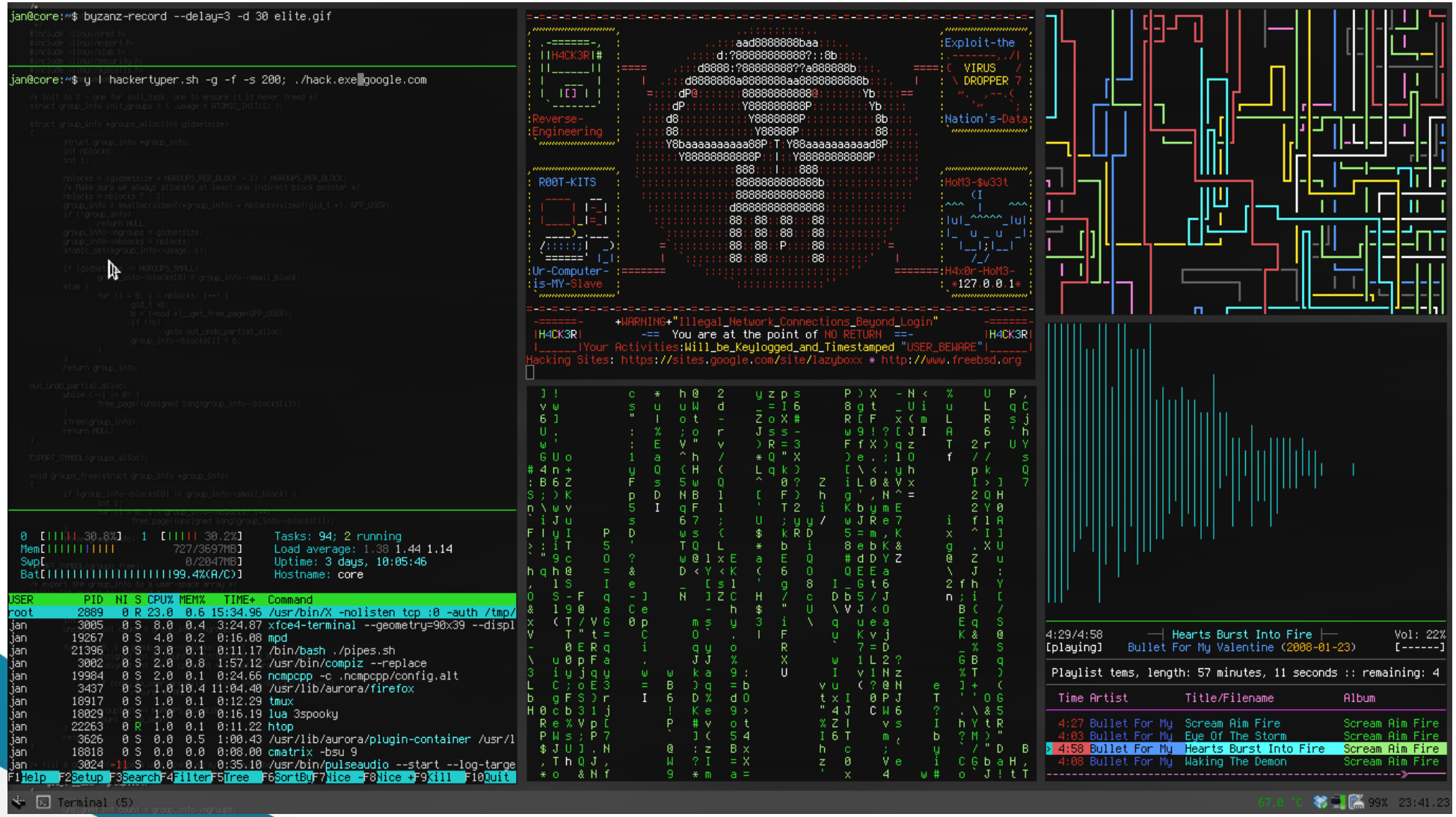
Keras & TensorFlow



ITLA INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS
Las Americas Institute of Technology

ITLA SECURITY FEST 2019

Pentesting & AI...



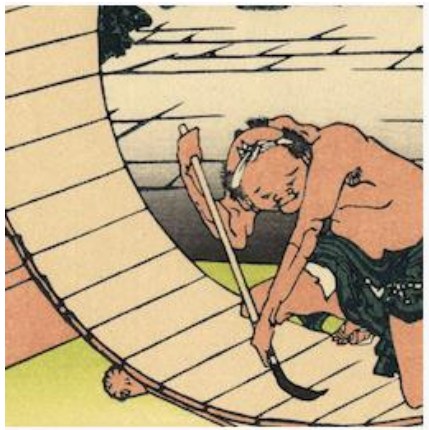
Pentesting & AI...

DEF CON 25 - Hyrum Anderson - Evading next gen AV using AI

DEF CON 24 - Machine Duping 101: Pwning Deep Learning Systems

DEF CON 25 (2017) - Weaponizing Machine Learning - Petro, Morris - Stream - 30July2017

Bypass de CAPTCHA



Really Simple CAPTCHA

★★★★½ (116)

Really Simple CAPTCHA is a CAPTCHA module intended to be called from other plugins. It is originally created for my Contact Form 7 plugin.

Takayuki Miyoshi

1+ million active installations Tested with 4.8.4

Adam Geitgey
https://twitter.com/ageitgey

https://medium.com/@ageitgey/how-to-break-a-captcha-system-in-15-minutes-with-machine-learning-dbebb035a710