



ITLA SECURITY FEST 2019



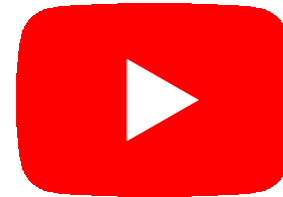
3^{RA} FERIA ACADÉMICA DE REDES Y SEGURIDAD INFORMÁTICA
DEL 16 AL 18 DE OCTUBRE.

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
SECURITY
FEST 2019



Agenda

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

¿Qué es Pentesting?

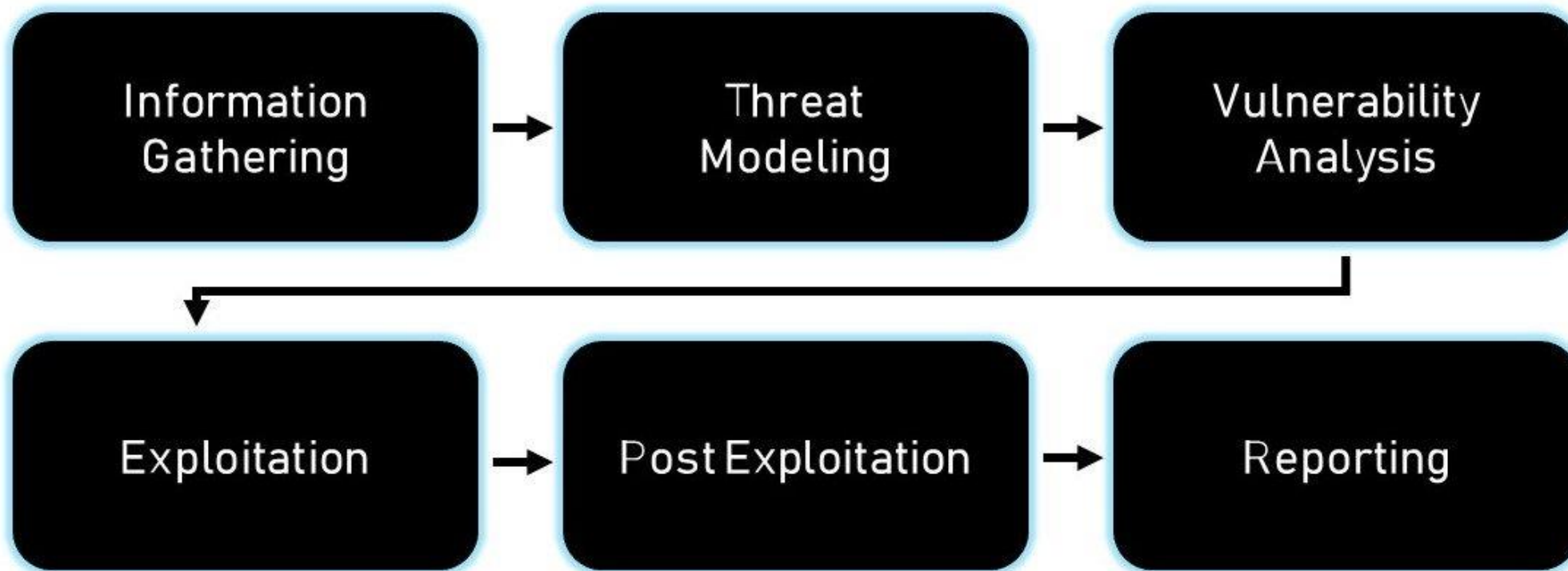


ITLA
SECURITY
FEST 2019



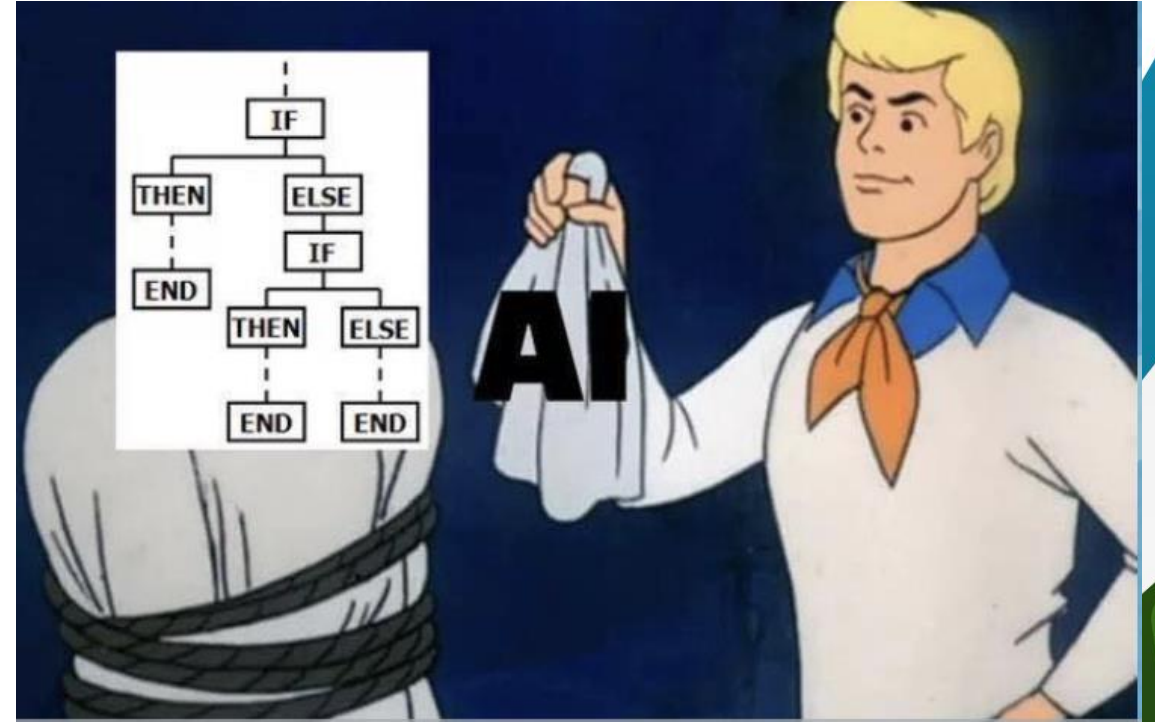


Network Penetration Testing Methodology



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

¿Qué es AI?

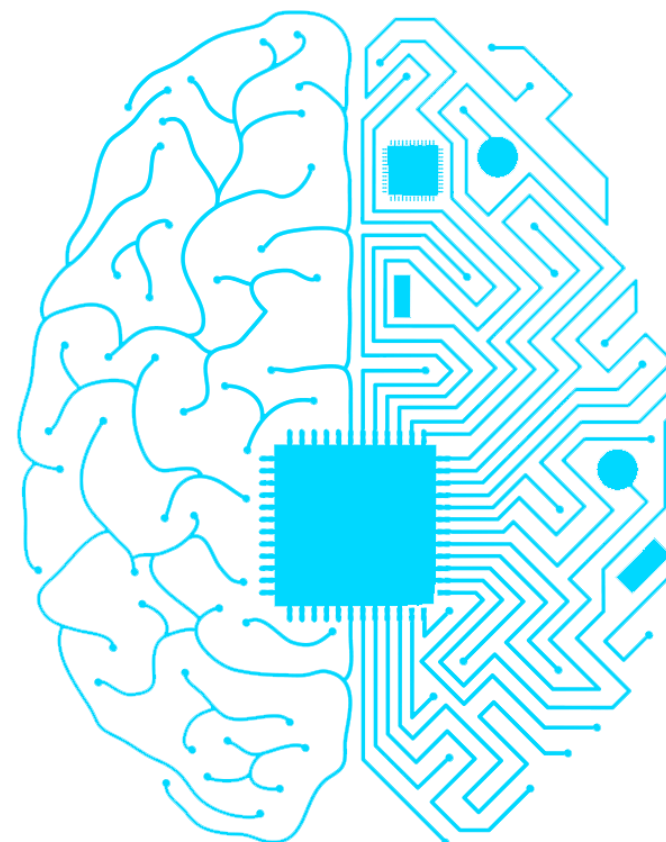


¿Qué realmente es AI?

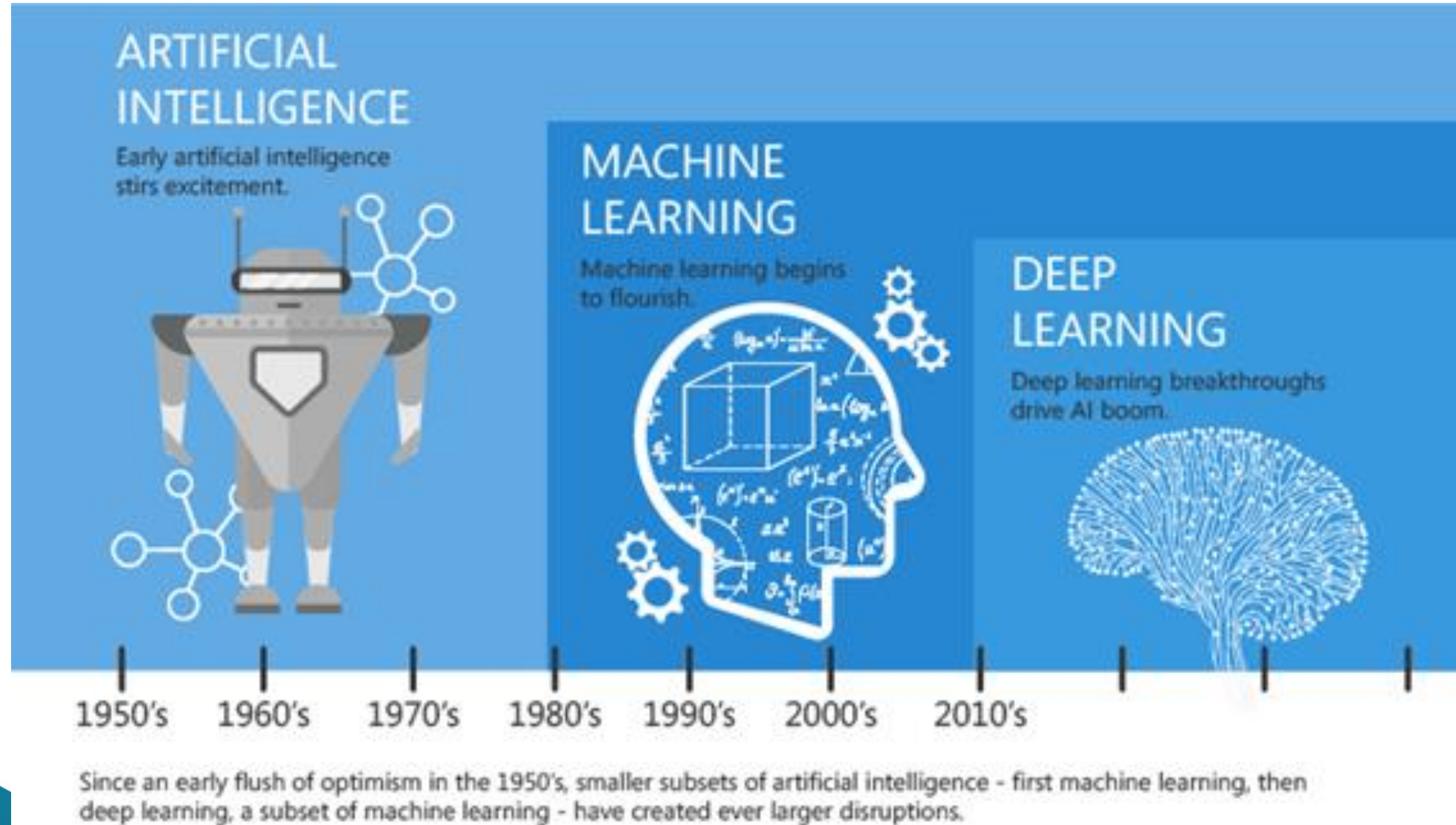
- Es la idea de crear una **computadora** que tenga la capacidad de **pensar** como un ser humano.

Cerebro vs AI

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



Historia de la Inteligencia Artificial



Expectativas...

AI / ML / DL – Toma tiempo entenderlo



ITLA
SECURITY
FEST 2019



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

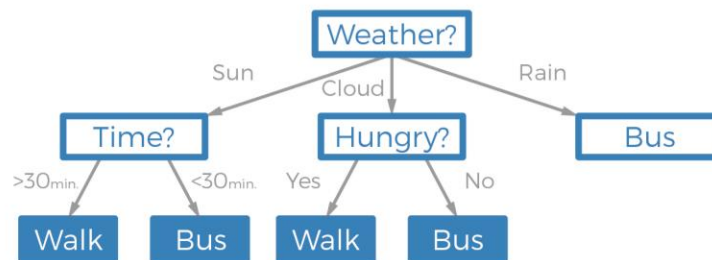


Deep Learning

Machine Learning



Input



Decision tree

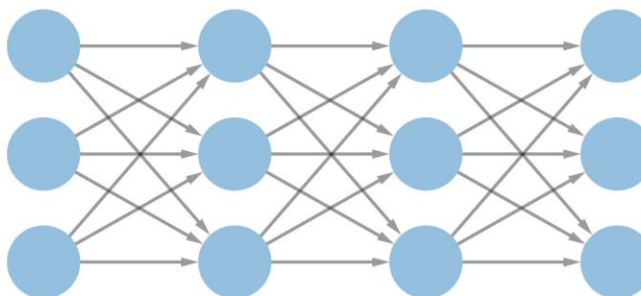


Output

Deep Learning



Input



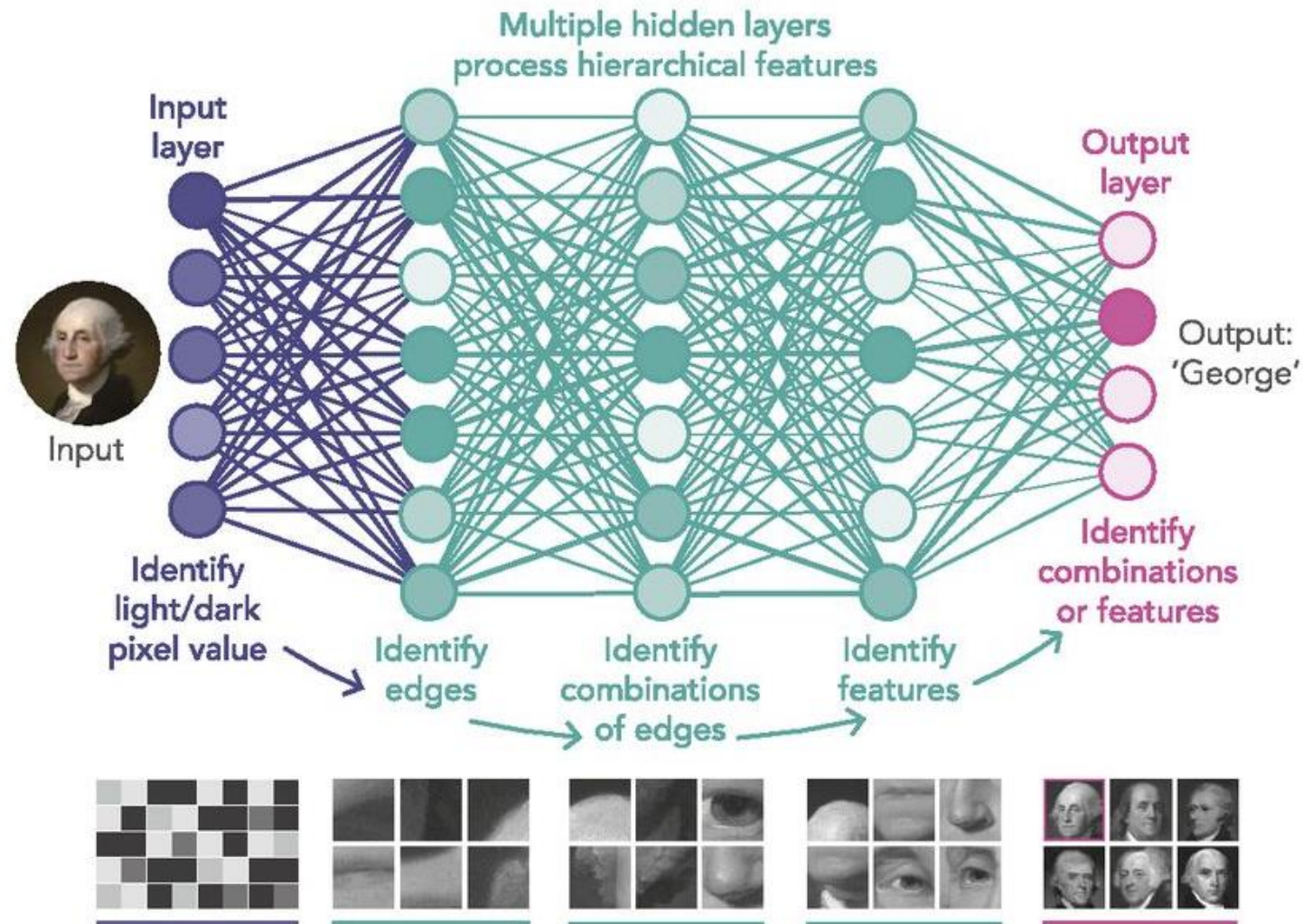
Feature extraction + Classification



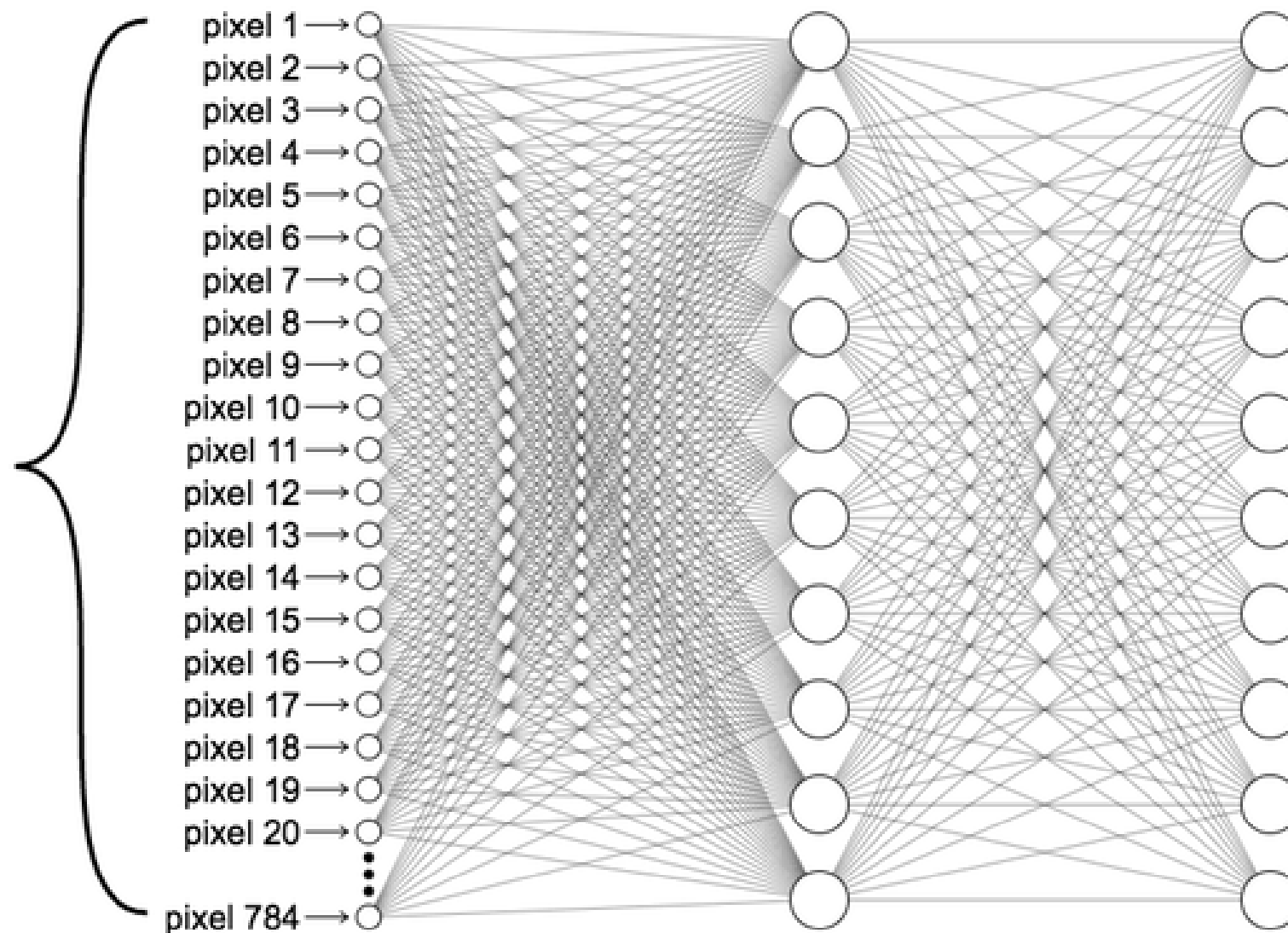
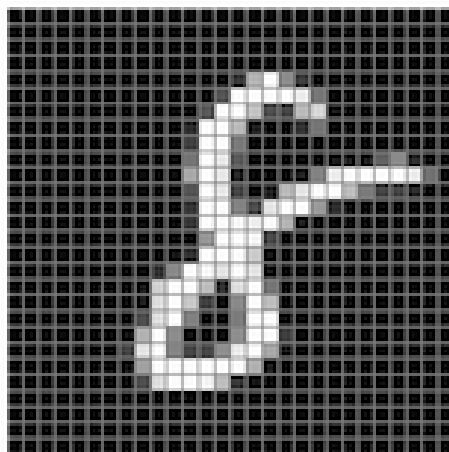
Output

Deep Learning

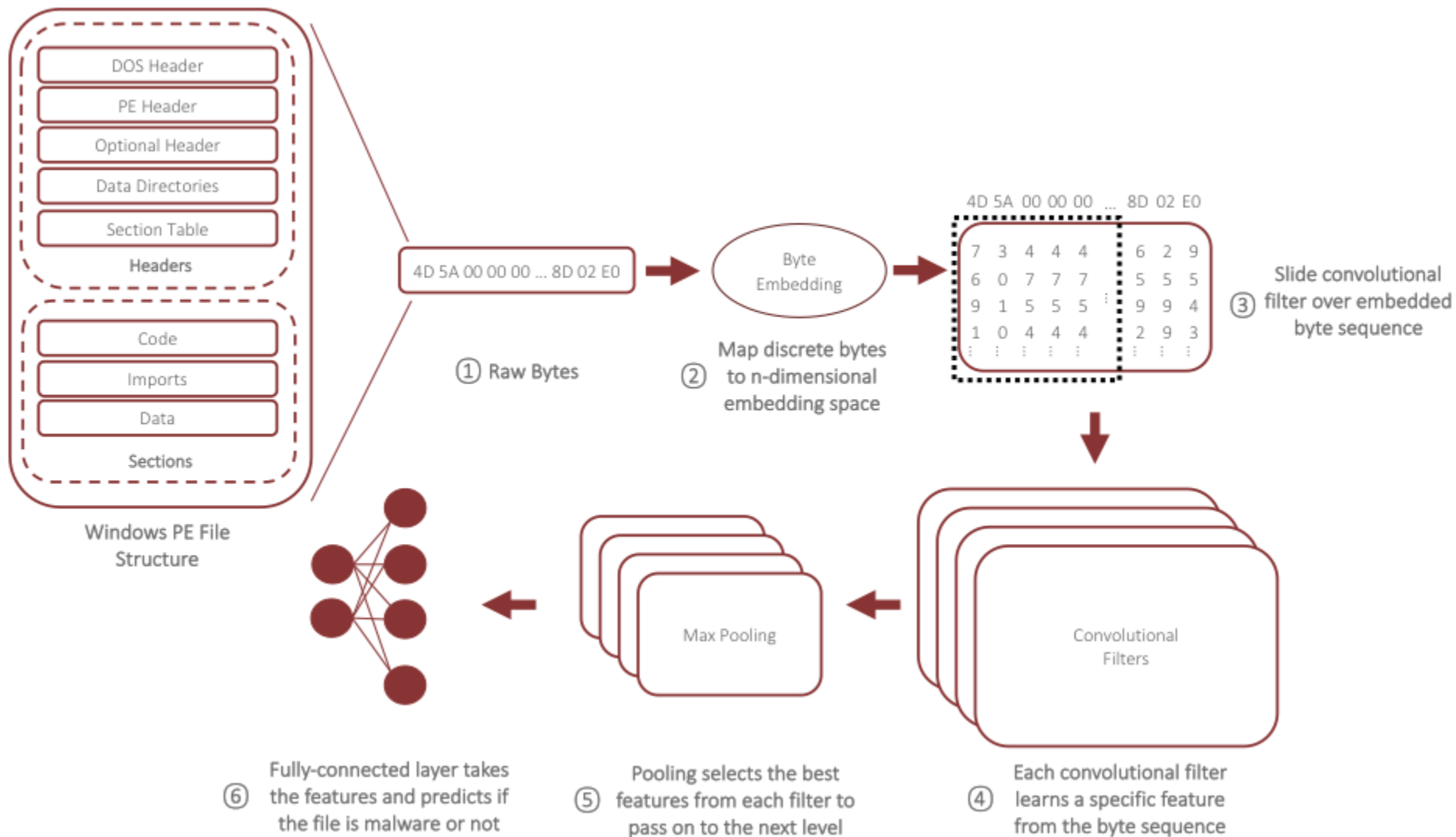
DEEP LEARNING NEURAL NETWORK



Deep Learning



Deep Learning

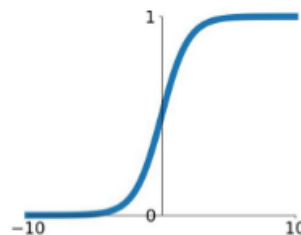


Deep Learning

Activation Functions

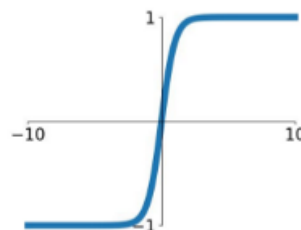
Sigmoid

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



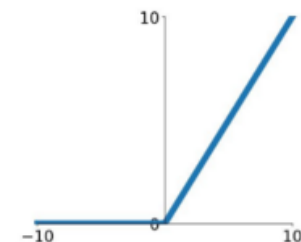
tanh

$$\tanh(x)$$



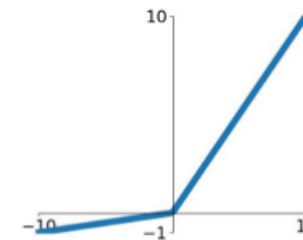
ReLU

$$\max(0, x)$$



Leaky ReLU

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

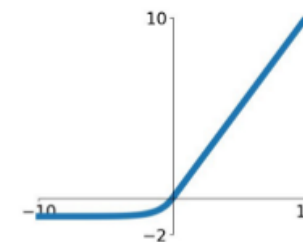


Maxout

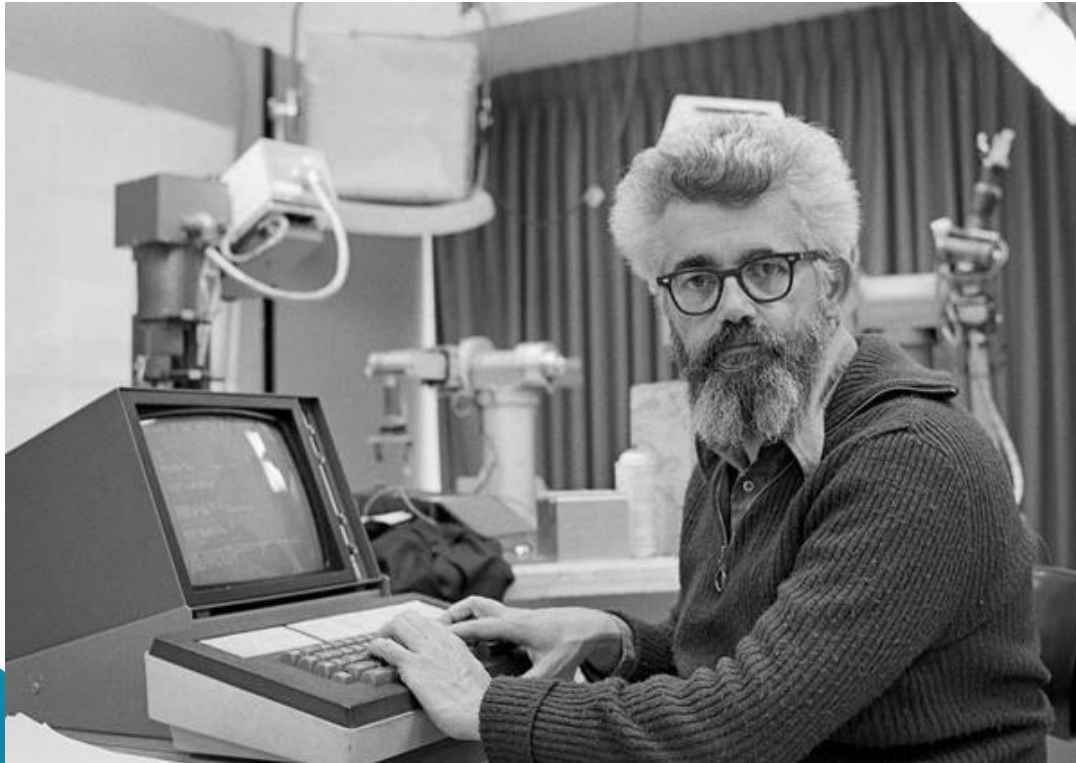
$$\max(w_1^T x + b_1, w_2^T x + b_2)$$

ELU

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



Deep Learning

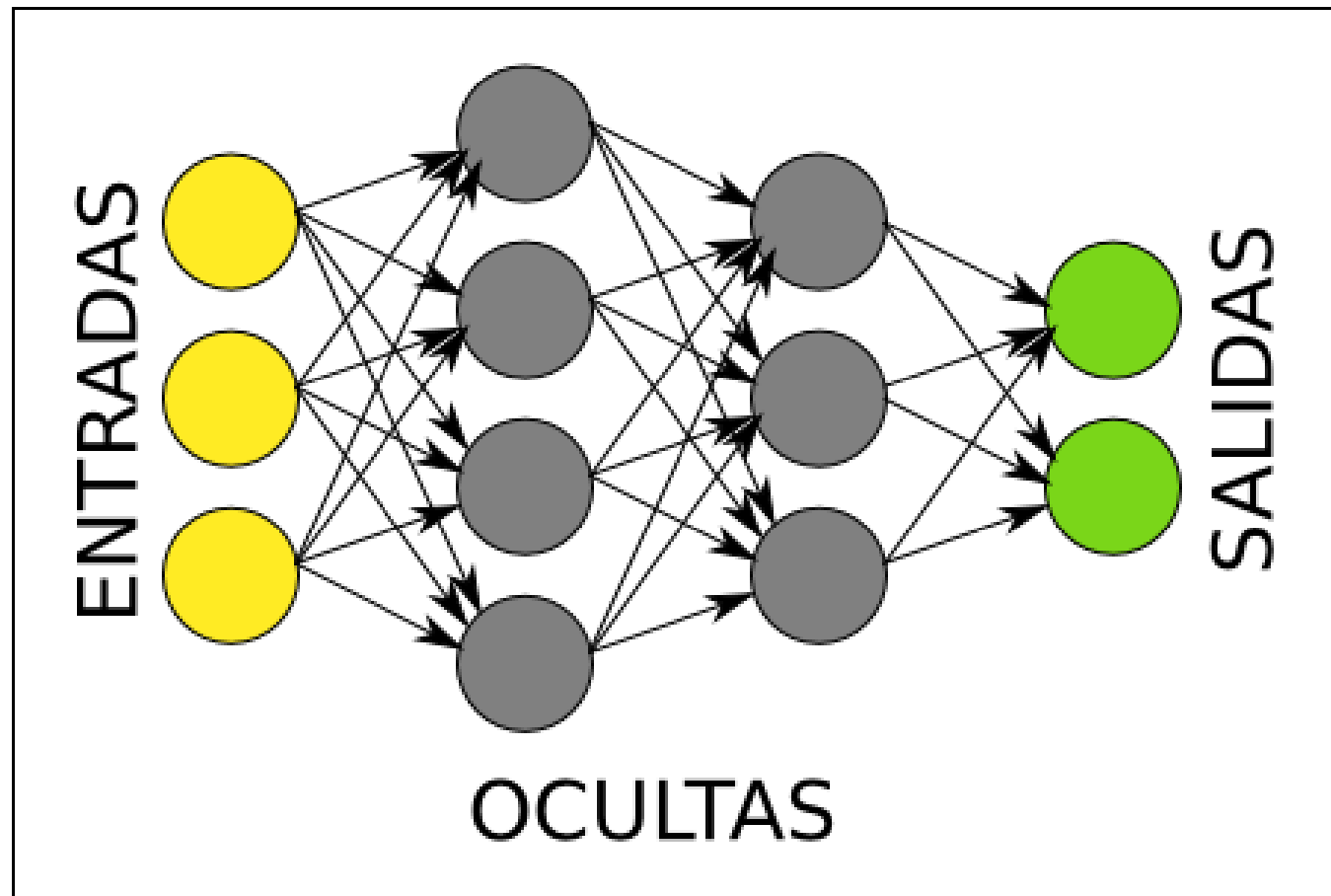


En 1956, John McCarthy, considerado el padre de la IA, organizó la conferencia Dartmouth que reunió a los fundadores de la AI y las bases para el futuro de la investigación de la AI.

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

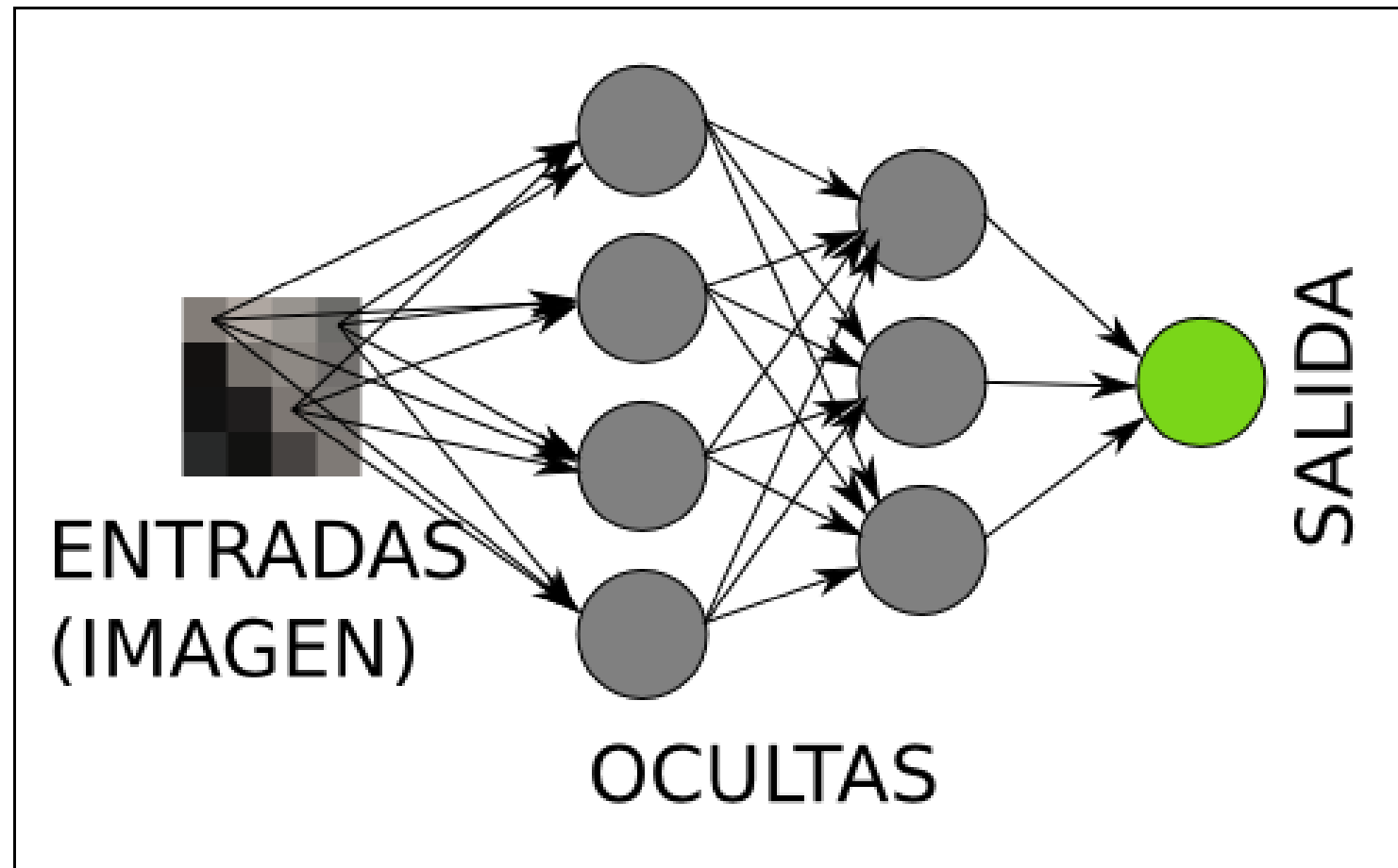
Deep Learning 101

Arquitectura



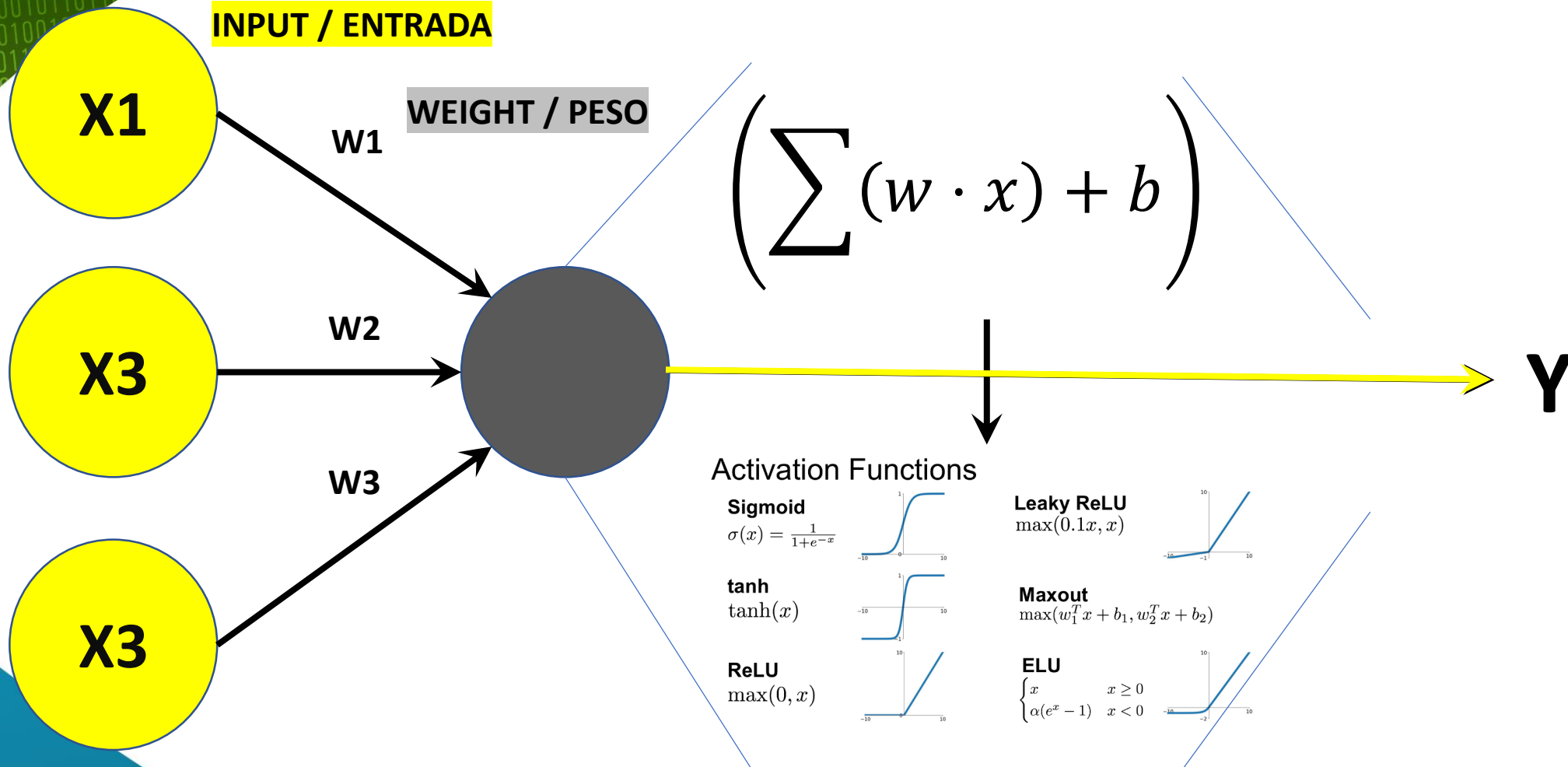
Deep Learning 101

Arquitectura

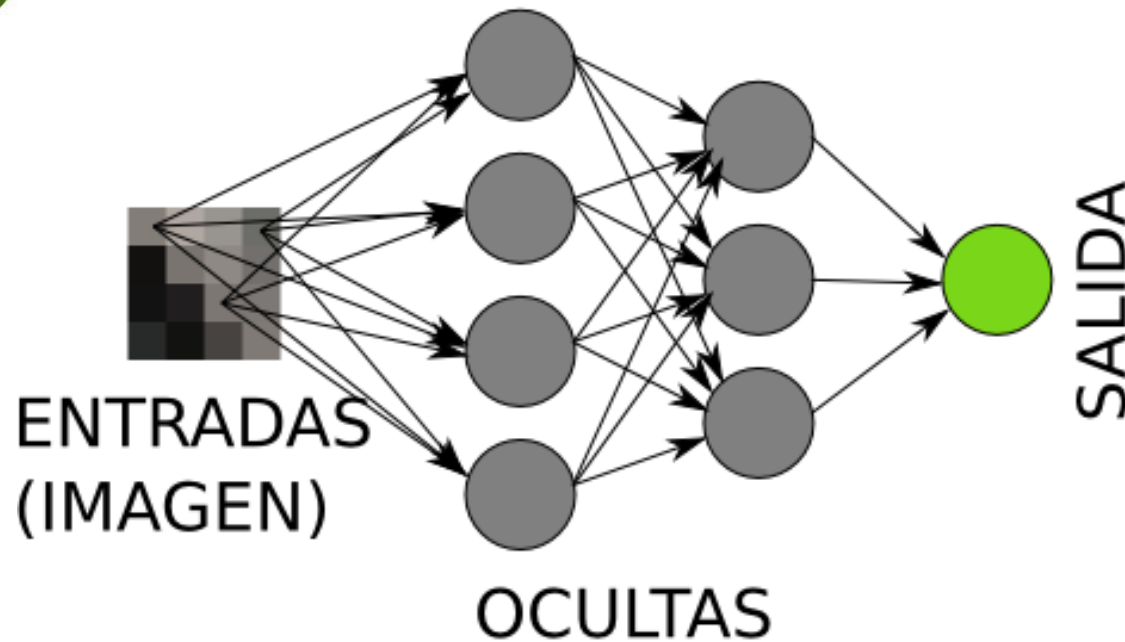


- <https://medium.com/@adriaciurana/aprende-deep-learning-en-10-minutos-e4e9e8950cd8>

Neurona Artificial

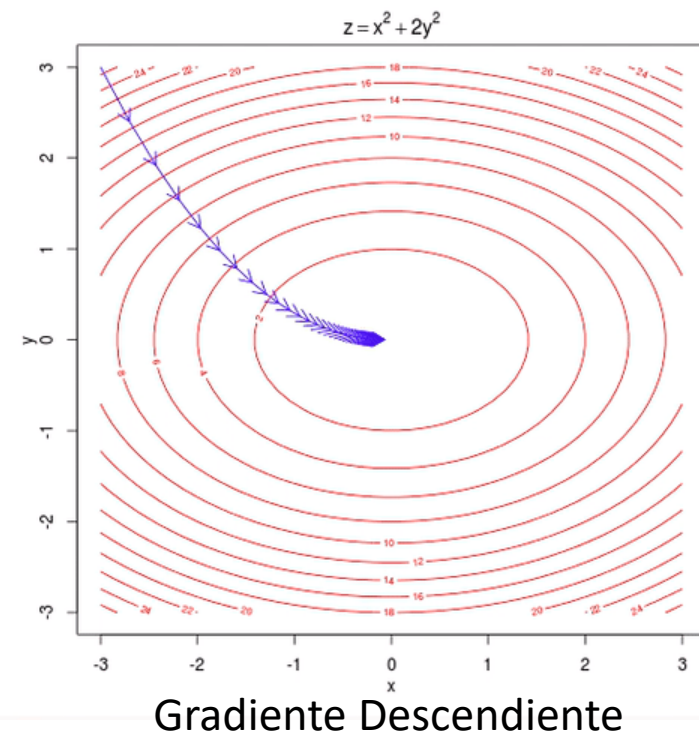


Entrenamiento de Red Neuronal

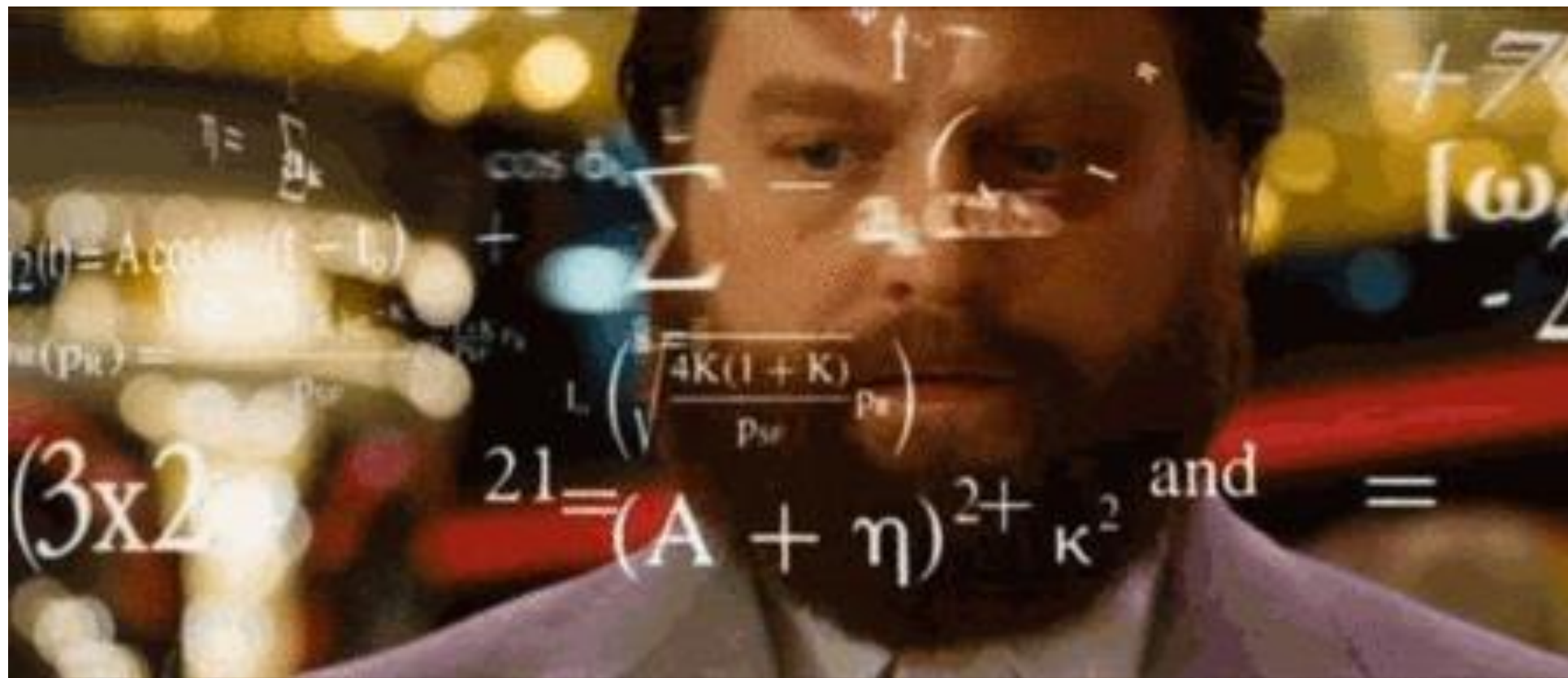


Error cuadrático medio

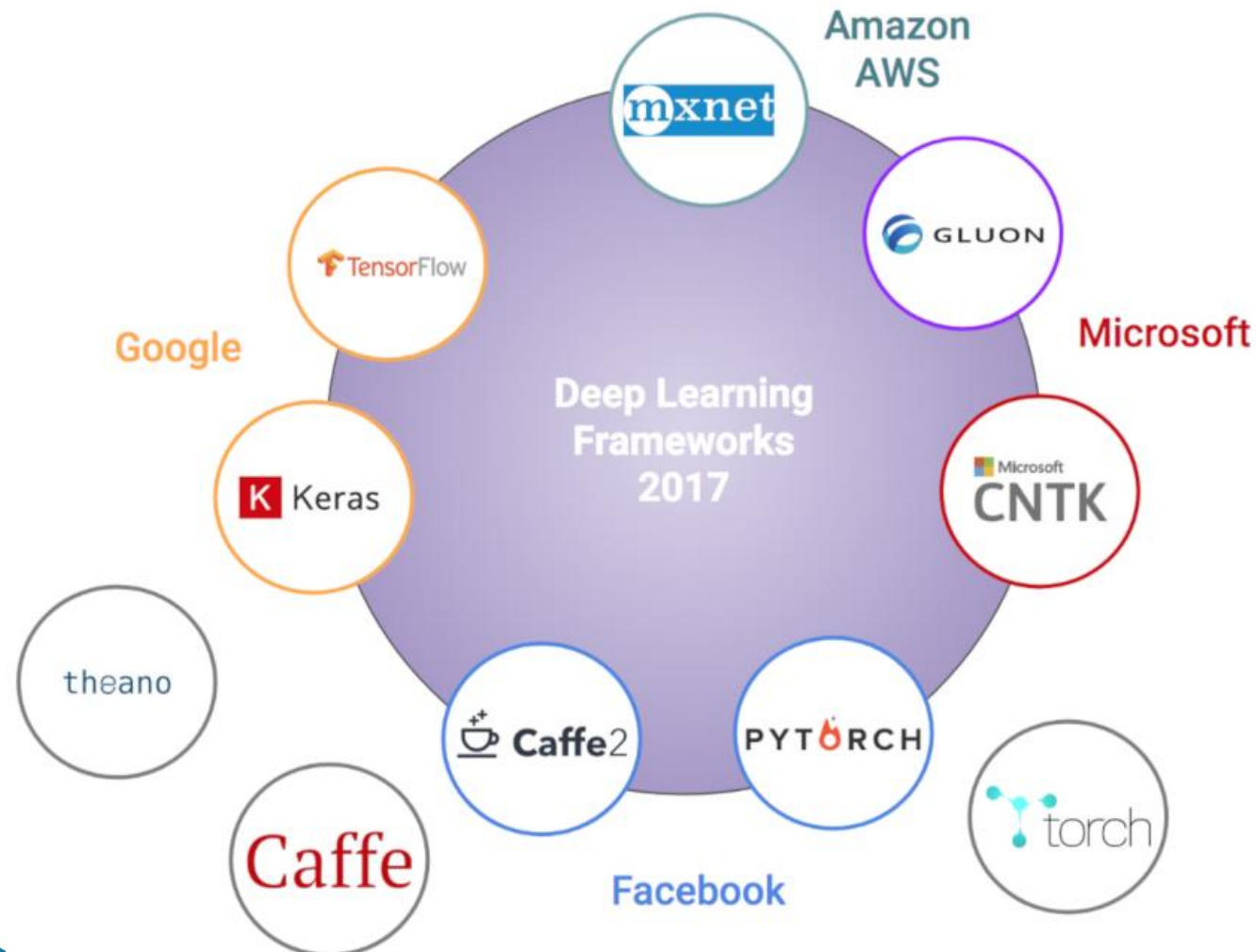
$$MSE = \frac{1}{M} \sum_{i=1}^M (real_i - estimado_i)^2$$



Ya soy un experto en AI



Deep Learning Frameworks



Keras & TensorFlow



+



Pentesting & AI...

```
jan@core:*$ %byzanz-record --delay=3 -d 30 elite.gif
```

```
#include <stdio.h>  
#include <unistd.h>  
#include <iomanip.h>  
#include <sys/types.h>
```

```
jan@core:$ y l hacker typer.sh -g -f -s 200; ./hack.exe google.com  
  
/* int i = 0 is one for initblock, one to ensure it is never freed */  
struct group_info init_group = { .usage = RTPMT_INIT(2) };
```

```
struct group_info *group_alloc(int gblsize)  
{  
    struct group_info *group_info;  
    int nblocks;  
  
    nblocks = (gblsize + NBLOCKS_PER_BLOCK - 1) / NBLOCKS_PER_BLOCK;  
    /* Take care we always allocate at least one indirect block pointer */  
    nblocks = nblocks + 1;  
    group_info = malloc(sizeof(struct group_info) * nblocks+sizeof(pid_t *) * GFP_USER);  
    if (!group_info)  
        return NULL;  
    group_info->nblocks = gblsize/  
    group_info->nblocks = nblocks;  
    memset(group_info,&usage, 1);  
  
    if (nblocks == NBLOCKS_PER_BLOCK)  
        info=>blocks[0] = group_info->mail_block;  
else {  
    for (i = 0; i < nblocks; i++) {  
        add_i_4e  
        void **l_get_free(GFP_USER);  
        if (!bi)  
            goto write_indirect_malloc;  
        group_info->blocks[i] = bi;  
    }  
    return group_info;  
write_indirect_malloc:  
while (i-->0){  
    free_page(unaligned_long/group_info->blocks[i]);  
}  
return group_info;  
}
```

```
CPRINT_WARN(groups_alloc);  
  
void group_free(struct group_info *group_info)  
{  
    if (group_info->blocks[0] != group_info->mail_block) {  
        int i;  
for(i = 0; i < group_info->nblocks; i++){  
free_page(unaligned_long/group_info->blocks[i]);  

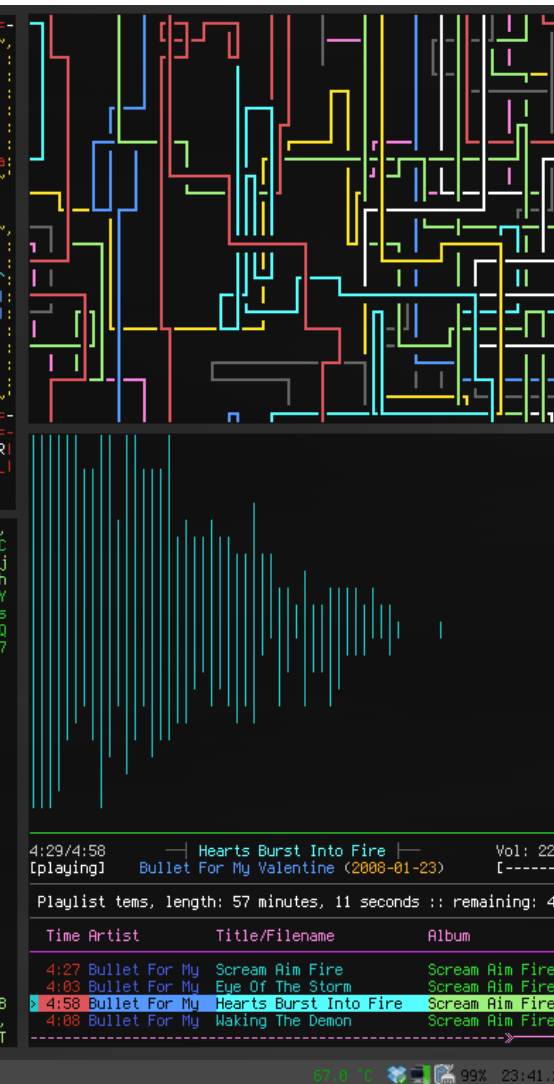
```

```
0 [||||| 30.8%]      1 [||||| 30.2%] Tasks: 94; 2 running  
Mem[|||||||       ]          727/3697MB Load average: 1.38 1.44 1.14  
Swp[]              |         0/2847MB   Uptime: 3 days, 10:05:46  
Bat[||||||||||||| ]     109.4%(A/C) Hostname: core
```

```
USER PID NI S CPUX MEM% TIME+ Command  
root 2889 0 R 23.0 0.6 15:34.96 /usr/bin/X -nolisten tcp :0 -auth /tmp/.  
jan 3095 0 S 0.0 0.4 3:24.87 xfce-terminal --geometry=98x39 --displ  
jan 19267 0 S 0.0 0.2 0:16.08 npd  
jan 21396 0 S 0.0 0.1 0:11.17 /bin/bash ./pipes.sh  
jan 3082 0 S 2.0 0.8 1:57.12 /usr/lib/compliz --replace  
jan 19984 0 S 2.0 0.1 0:24.66 ncmapcpp -c .ncmapp/config.alt  
jan 3437 0 S 1.0 10.4 11:04.40 /usr/lib/aurora/firefox  
jan 18917 0 S 1.0 0.1 0:12.29 tmux  
jan 18829 0 S 1.0 0.0 0:15.19 lua 3spooky  
jan 22263 0 R 1.0 0.1 0:11.22 http  
jan 3626 0 S 0.0 0.5 1:00.43 /usr/lib/aurora/plugin-container /usr/l  
jan 18818 0 S 0.0 0.0 0:08.00 cmatrix-bsu 9  
jan 3024 -1 I 0.0 0.1 0:35.10 /usr/bin/pulseaudio --start --log-tau
```

```
F1 Help F2 Setup F3 Search F4 Filter F5 Tree F6 Sort By F7 Nice F8 Nice F9 Kill F10 Quit
```

```
[Terminal (S)]
```

[illegible]

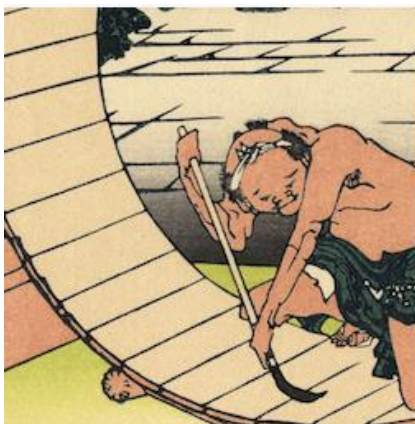
Pentesting & AI...

[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

★★★★★ (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>