Machine Learning for Cyber Security Part 2

Dr Carlos Moreno Garcia

c.moreno-garcia@rgu.ac.uk

Senior Lecturer in Computing

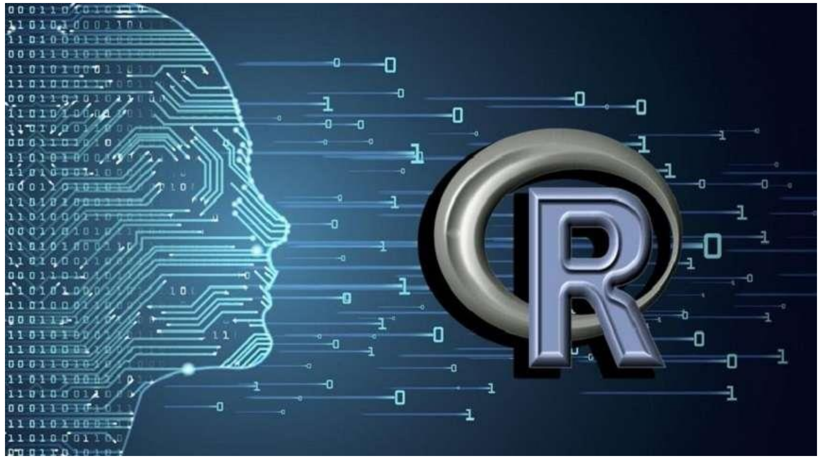
Robert Gordon University, Aberdeen, Scotland, UK

Today’s Activities

1. Malware Infection in Python
2. Bayesian poisoning in R
3. Face detection in Python
4. Image classification using CNNs in Python

ADDITIONAL PRACTICE

5. Password generation and cracking in Python
6. Fingerprint matching in Python

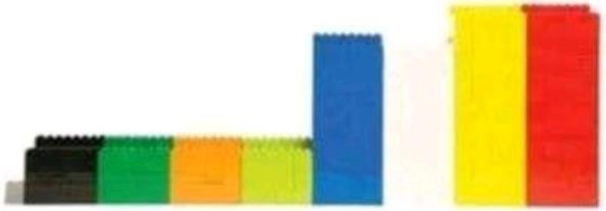


Data

Sorted

Arranged

Presented Visually



Explained With A Story

Actionable (Useful)

Ignored By Management And Tossed Out

1. Malware Infection

https://colab.research.google.com/drive/1hXy9srPhVN9B7D2lrjZX9ltnemVrDPVz?usp=sharing

2. Bayesian Poisoning

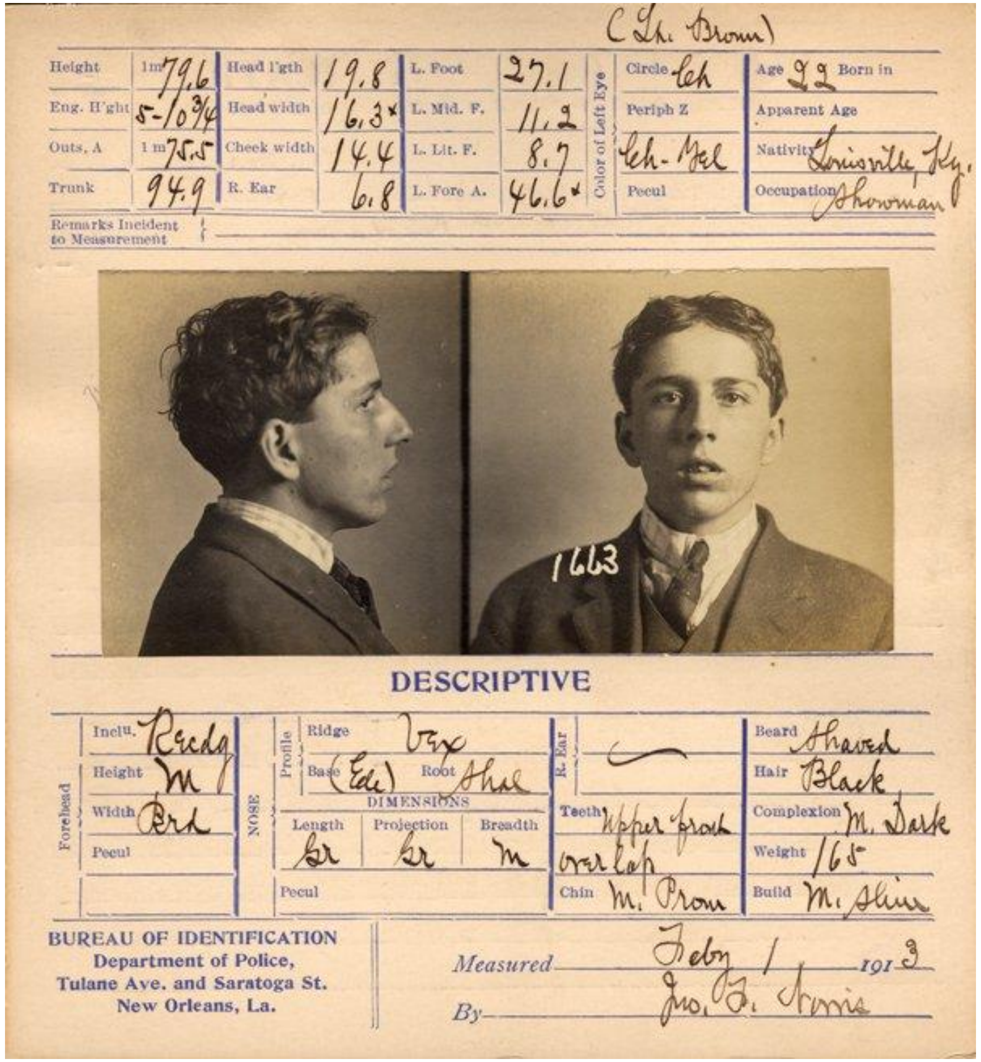
https://colab.research.google.com/drive/1UmTx0h-Tc6Prn9FQ1bjl-Zwbz9cq2lOK?usp=sharing

Biometrics

More Info:

https://www.biometricupdate.com/201802/history-of-biometrics-2

Bertillionage



(Th. Brown)

Height	1m 79.6	Head l'gth	19.8	L. Foot	27.1	Color of Left Eye	Circle Ch	Age 22	Born in
Eng. H'ght	5-10¾	Head width	16.3×	L. Mid. F.	11.2		Periph Z	Apparent Age	
Outs. A	1 m 75.5	Cheek width	14.4	L. Lit. F.	8.7		Ch-Yel	Nativity Louisville, Ky.	
Trunk	94.9	R. Ear	6.8	L. Fore A.	46.6×		Pecul	Occupation Showman	

Remarks Incident to Measurement

1663

DESCRIPTIVE

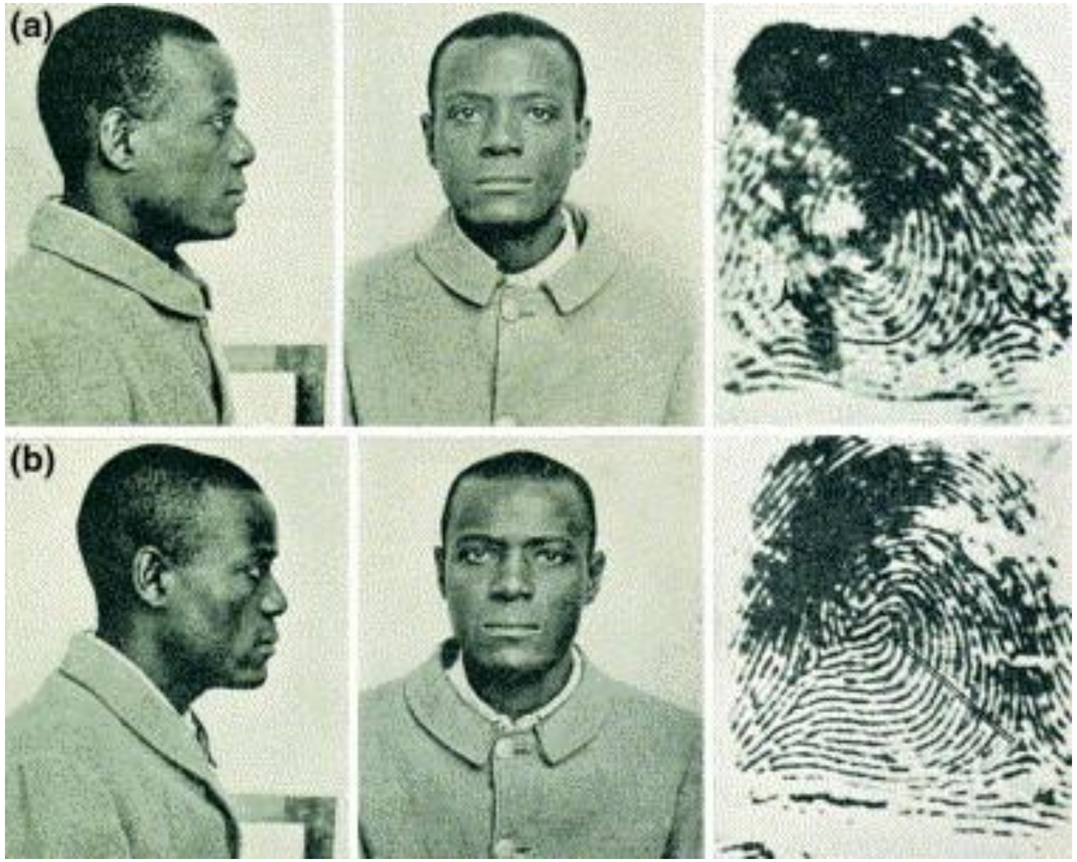
Forehead	Inclu. Recdg	NOSE	Profile	Ridge Vex		R. Ear	Beard Shaved
	Height M			Base (Ele)	Root Shal		Hair Black
	Width Brd		DIMENSIONS			Teeth Upper front	Complexion M. Dark
	Pecul		Length Gr	Projection Gr	Breadth M	over lap	Weight 165
			Pecul			Chin M. Prom	Build M. Slim

BUREAU OF IDENTIFICATION
Department of Police,
Tulane Ave. and Saratoga St.
New Orleans, La.

Measured Feby 1 1913

By Jno. F. Arnis

William West



https://dh.dickinson.edu/digitalmuseum/exhibit-artifact/babes-in-the-woods/fingerprints

Fundamentals

- Everything examined with enough detail can be distinguishable

- Humans have patterns that help secure systems (5 factors of authentication):
  - What you know
    - A password
  - What you have
    - Physical key
  - Where you are
    - Location
  - What you are
    - Biometrics
  - How you are
    - Behaviours (e.g. gait, handwriting, etc.)

3. Face detection

https://colab.research.google.com/drive/1qpk_hozXly_JTS4qarB6msGUuRdb-iVq?usp=sharing

4. Image Classification using Neural Networks

https://colab.research.google.com/drive/1p_r_buzwt0FBGEkVE1E91FKFrAIPDSZL?usp=sharing

Additional Practice

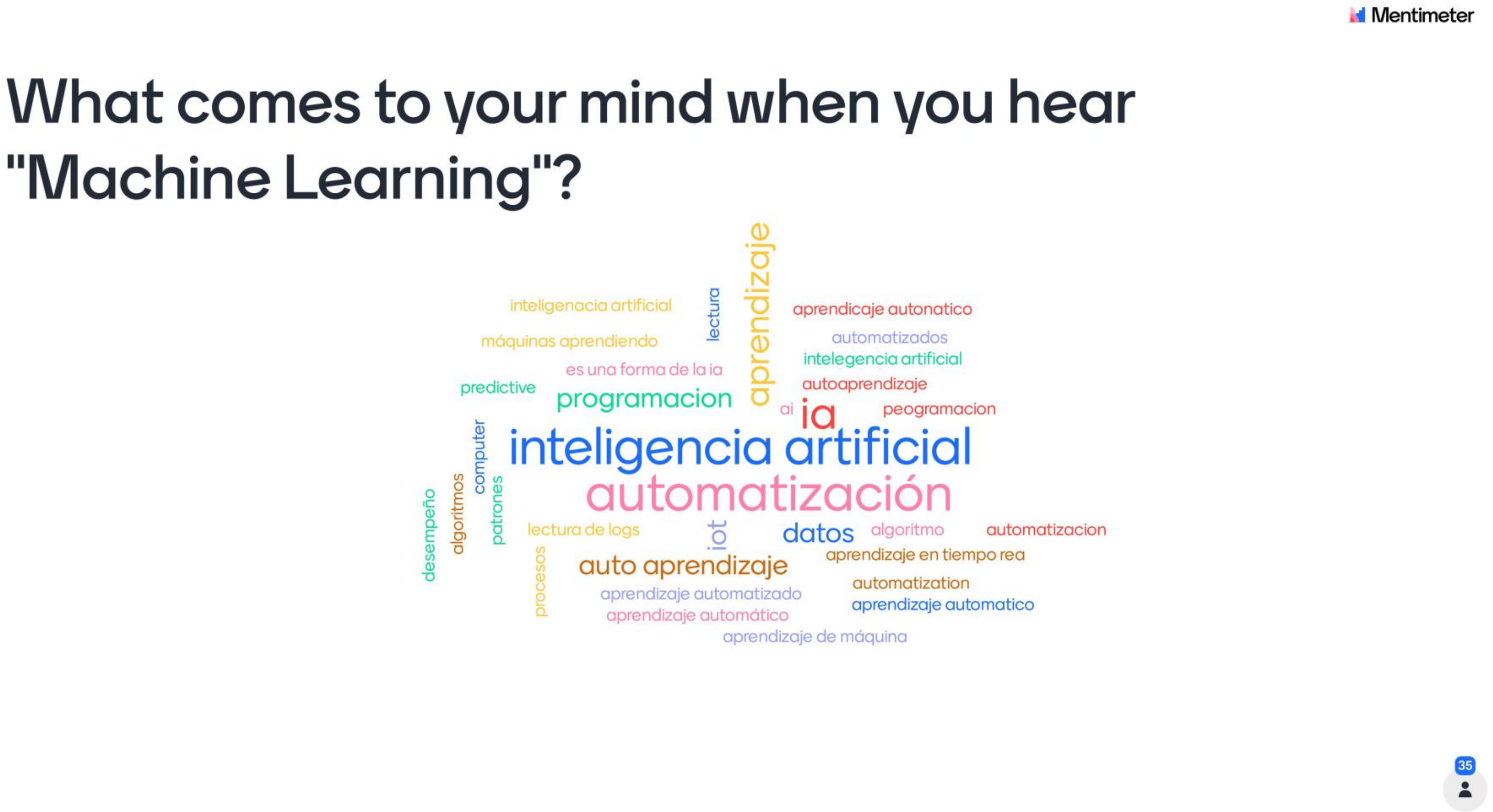
5. Password Generation and Cracking

https://colab.research.google.com/drive/1sLa1N09ul_RFLt0_ypAPUPZjMc_zNiR-?usp=sharing

6. Fingerprint Matching

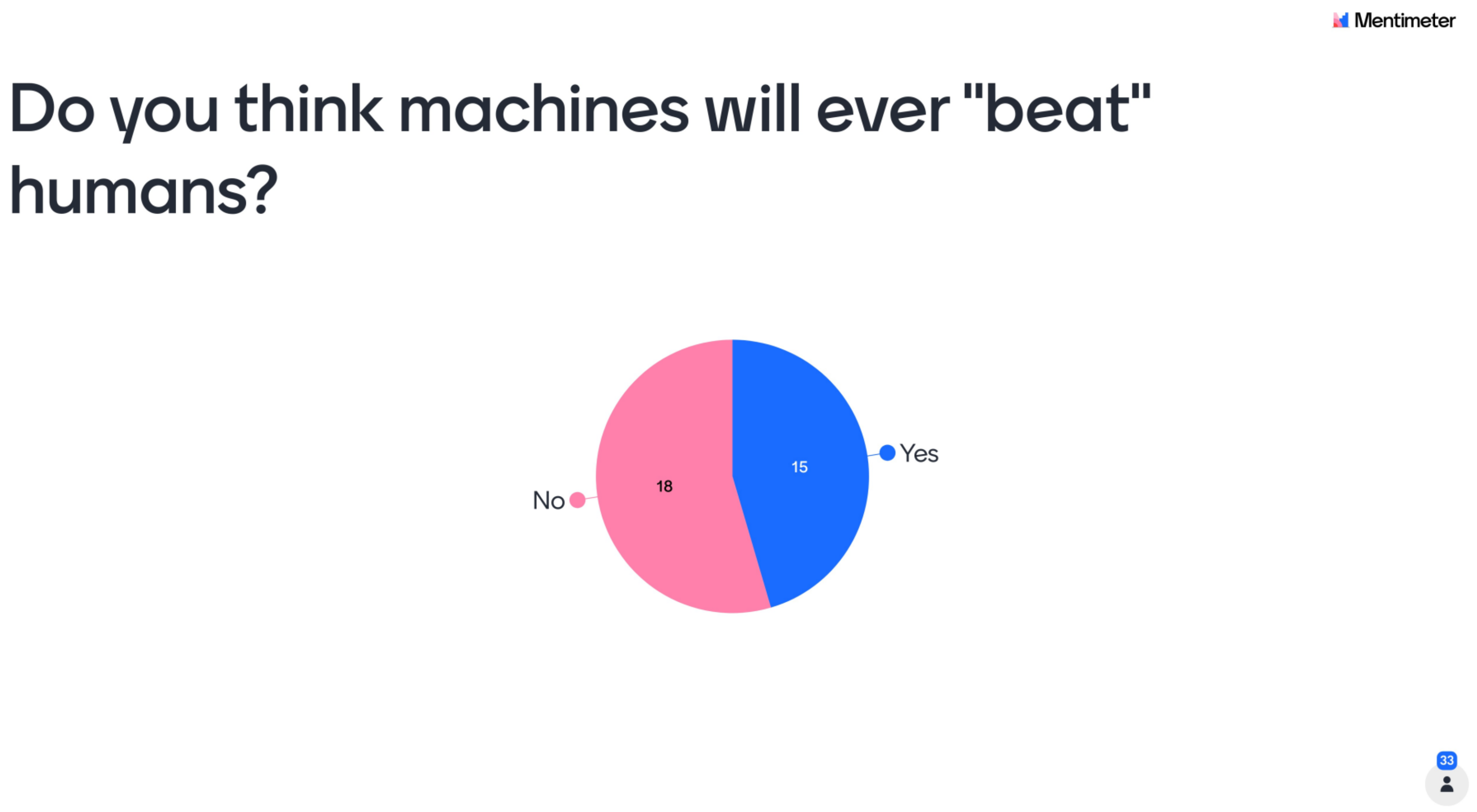
https://colab.research.google.com/drive/15mtlfOwuYygEwP9fpA1PMYJToUsnkKlh?usp=sharing

Results from last week’s polls



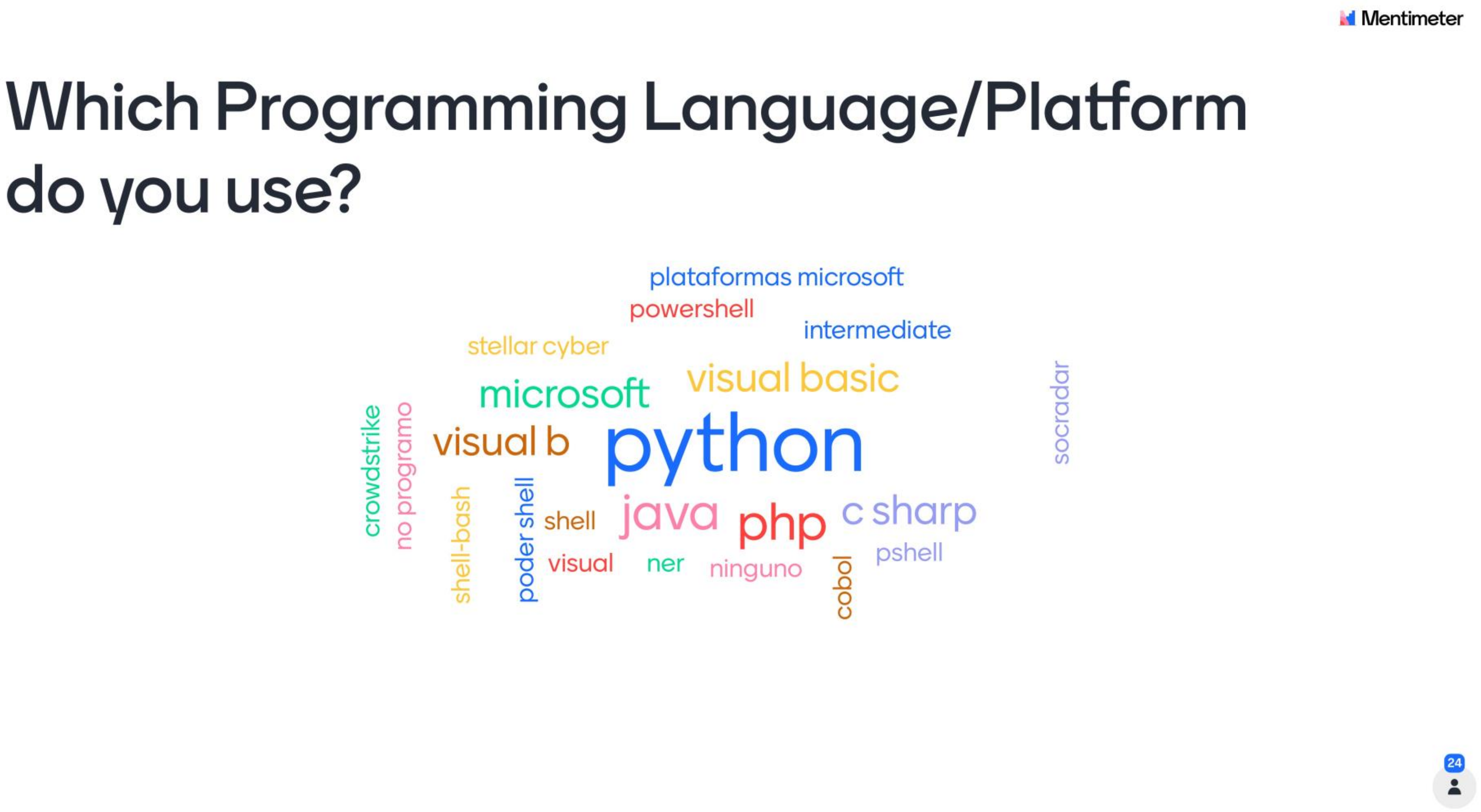
Mentimeter

What comes to your mind when you hear "Machine Learning"?



Mentimeter

Do you think machines will ever "beat" humans?



Mentimeter

Which Programming Language/Platform do you use?