

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. Password generation and cracking in Python
2. Malware Infection in Python
3. Bayesian poisoning in R
4. Biometrics
 - a. Face detection in Python
 - b. Fingerprint matching in Python
5. Image classification using CNNs in Python



Data



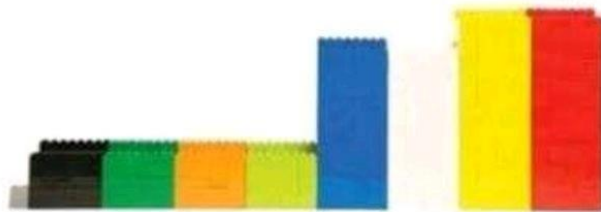
Sorted



Arranged



Presented
Visually



Explained
With A Story



Actionable
(Useful)



Ignored By
Management
And Tossed
Out



1. Password Generation and Cracking

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

2. Malware Infection

<https://colab.research.google.com/drive/1hXy9srPhVN9B7D2lrjZX9ltmemVrDPVz?usp=sharing>

3. Bayesian Poisoning

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

4. Biometrics

More Info:

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

Bertillionage

(L. Brown)

Height	1m 79.6	Head l'gth	19.8	L. Foot	27.1	Circle	leh	Age	22	Born in	
Eng. H'ght	5-10 3/4	Head width	16.3	L. Mid. F.	11.2	Periph Z		Apparent Age			
Outs. A	1m 75.5	Cheek width	14.4	L. Lit. F.	8.7	leh-Mel		Nativity	Louisville, Ky.		
Trunk	94.9	R. Ear	6.8	L. Fore A.	46.6	Pecul		Occupation	Shoemaker		

Remarks Incident to Measurement: {



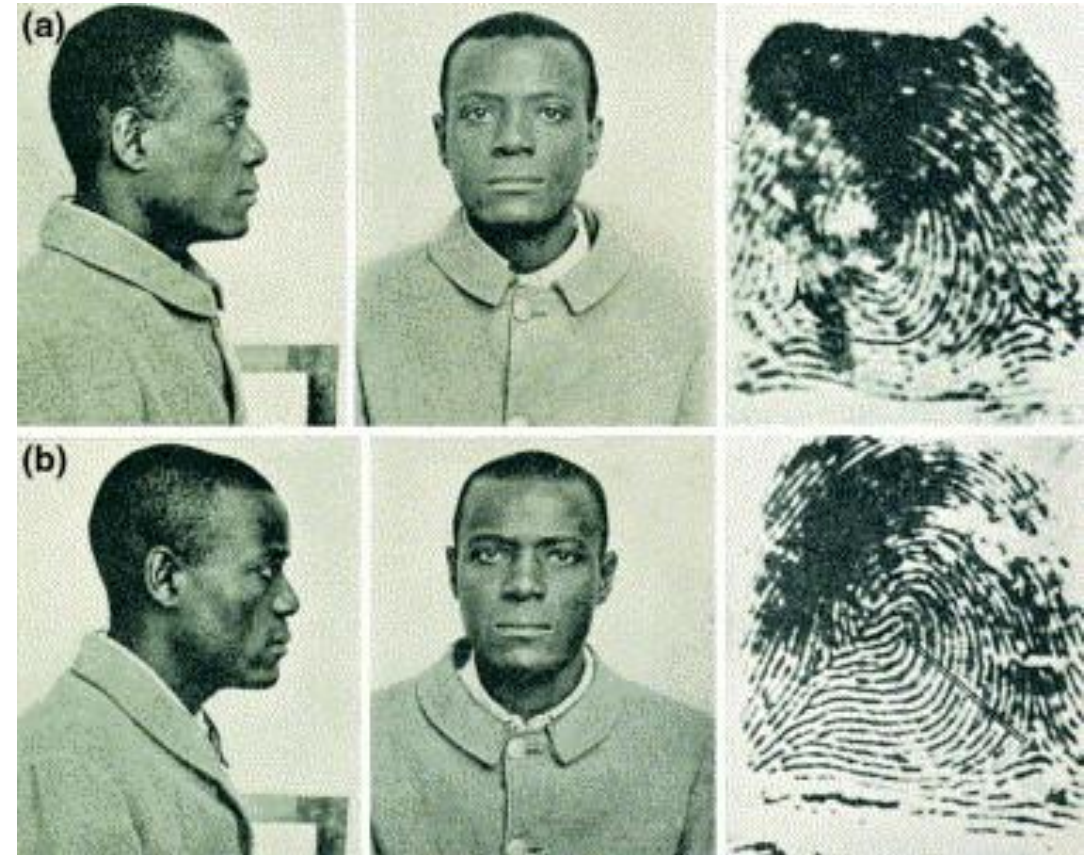
DESCRIPTIVE

Incl.	Recd	Ridge	Vex	Beard	Shaved
Height	M	Base	(Eu) Root	Hair	Black
Width	Br	DIMENSIONS			Complexion
Pecul		Length	Projection	Breadth	M. Dark
		br	br	m	Weight
		Pecul			165
					Build
					M. Slim

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

Measured July 1 1913
By Geo. B. Harris

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.)

4a. Fingerprint Matching

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

4b. Face detection

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

5. Image Classification using Neural Networks

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