ROBERT GORDON UNIVERSITY ABERDEEN

Machine Learning for Cyber Security Part 2

Dr Carlos Moreno Garcia

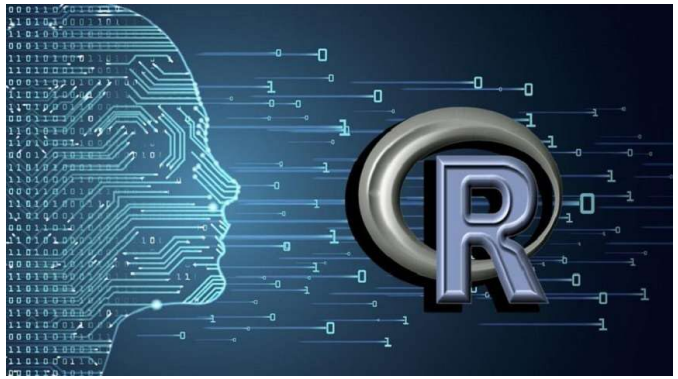
c.moreno-garcia@rgu.ac.uk

Senior Lecturer in Computing | Research Degrees Coordinator

Robert Gordon University, Aberdeen, Scotland, UK

Today's Activities (depending on time & interest)

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

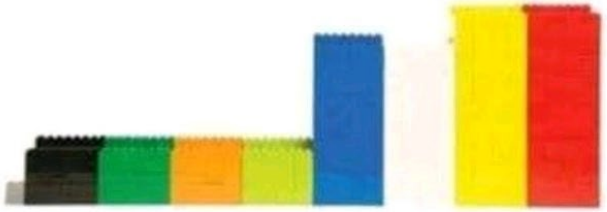


Data

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/1hXy9srPhVN9B7D2lrjZX9ltnemVrDPVz?usp=sharing

3. Bayesian Poisoning

https://colab.research.google.com/drive/1_6XFtMo0N63e3ULdsDCTZbPMKzB6MiPE?usp=sharing

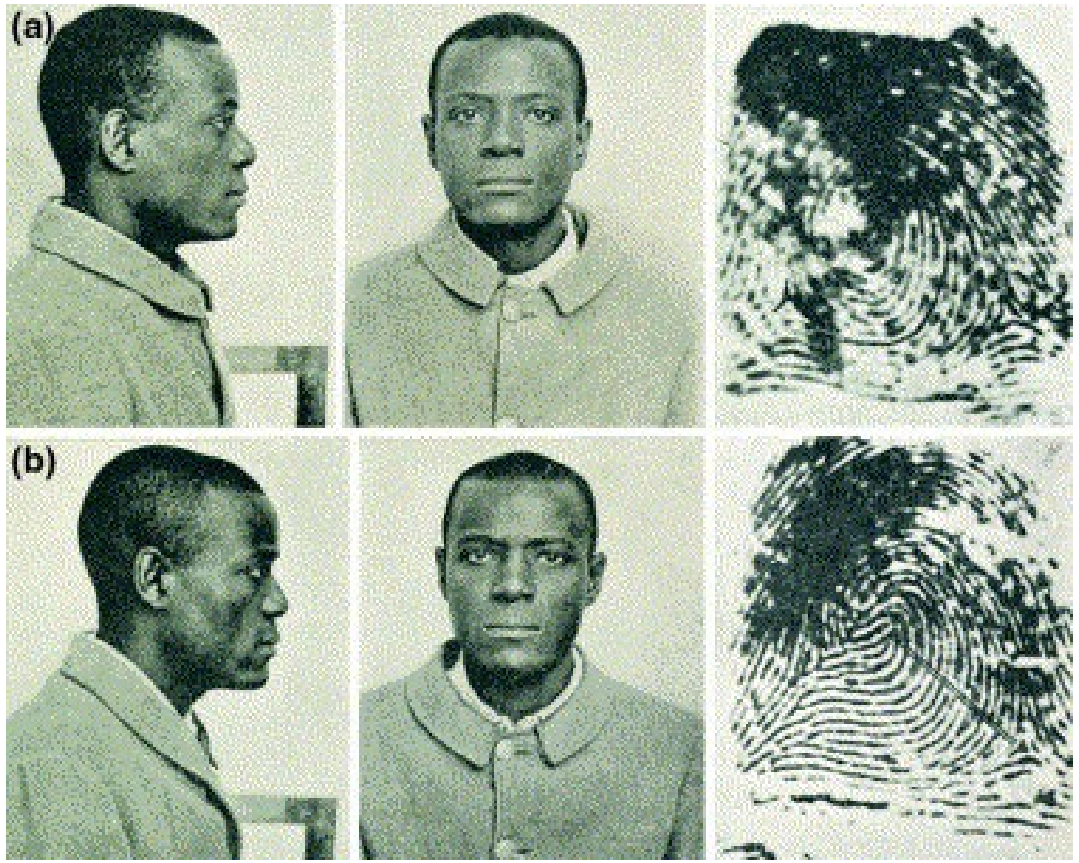
4. Biometrics

More Info:

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

Bertillionage

The Will and William West case



https://caasbrey.com/a-fingerprint-fable-the-will-and-william-west-case/

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

Final Considerations