photo: Utah

Współczesne wyzwania z zakresu cyberbezpieczeństwa

Artificial Intelligence

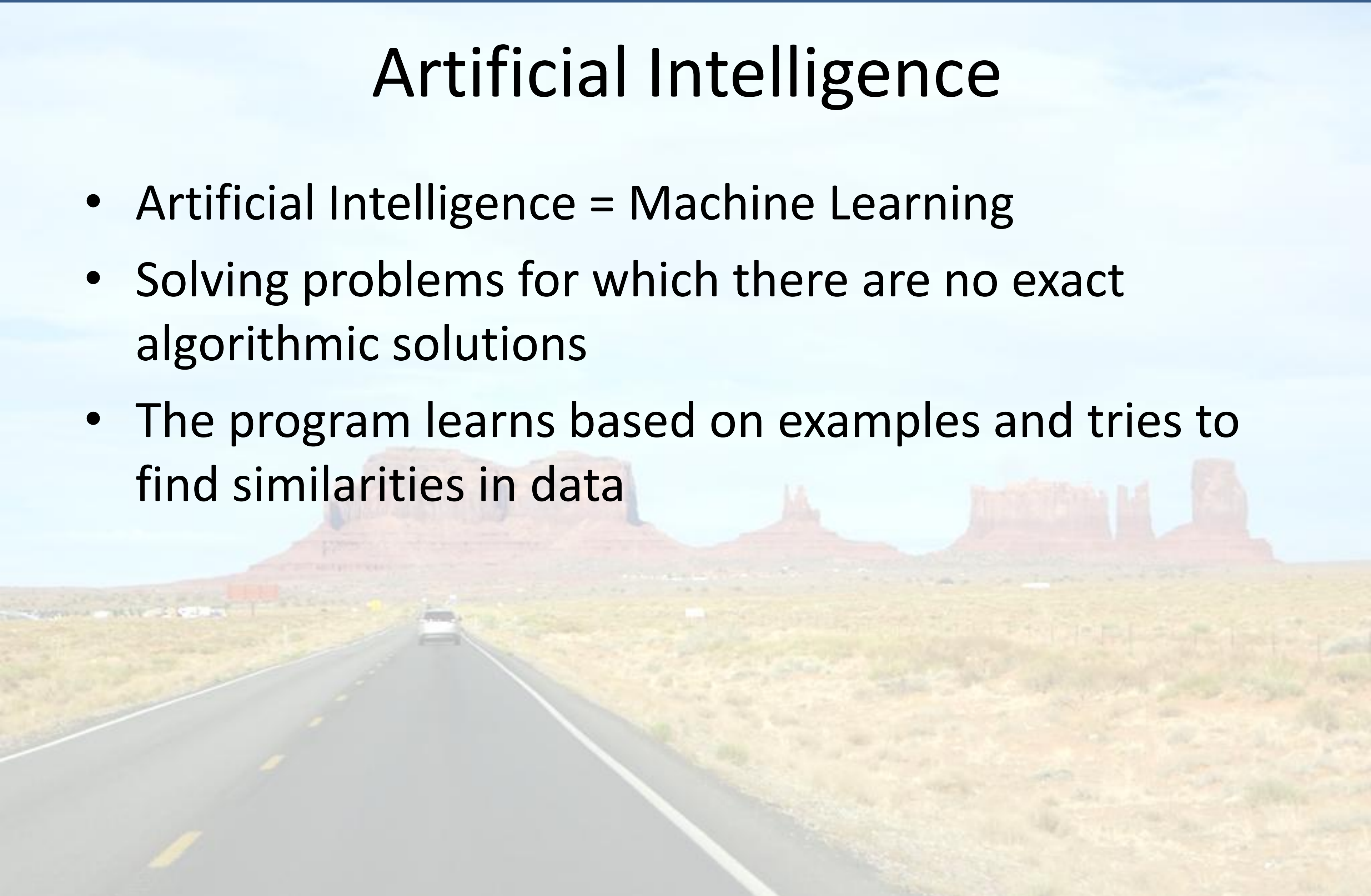
Paweł Kasprowski, PhD, DSc.

O mnie

- dr hab. inż. Paweł Kasprowski, prof. PŚ
  - zastępca kierownika Katedry Informatyki Stosowanej
  - uczelniany koordynator Priorytetowego Obszaru Badawczego Sztuczna Inteligencja i Przetwarzanie Danych
  - uczelniany koordynator kierunku informatyka
- Wiele lat doświadczenia
  - bazy danych
  - uczenie maszynowe
  - uczenie głębokie
  - analiza ruchu oka

About me

- Paweł Kasprowski, PhD, DSc, SUT Professor
  - vice-head of Applied Informatics Department
  - university coordinator of Artificial Intelligence and Data Processing Priority Research Area
  - university coordinator of informatics degree course
- A lot of experience in
  - databases
  - machine learning
  - deep learning
  - eye movement analysis



Artificial Intelligence

- Artificial Intelligence = Machine Learning
- Solving problems for which there are no exact algorithmic solutions
- The program learns based on examples and tries to find similarities in data

AI in Cybersecurity

- For defenders:
  - finding untypical and suspicious behavior
  - threat detection, anomaly detection
  - identification of attacks
- For attackers:
  - creating artificial data that misleads systems
  - fake faces, fake requests
  - automated attempts to break security

Content of the course

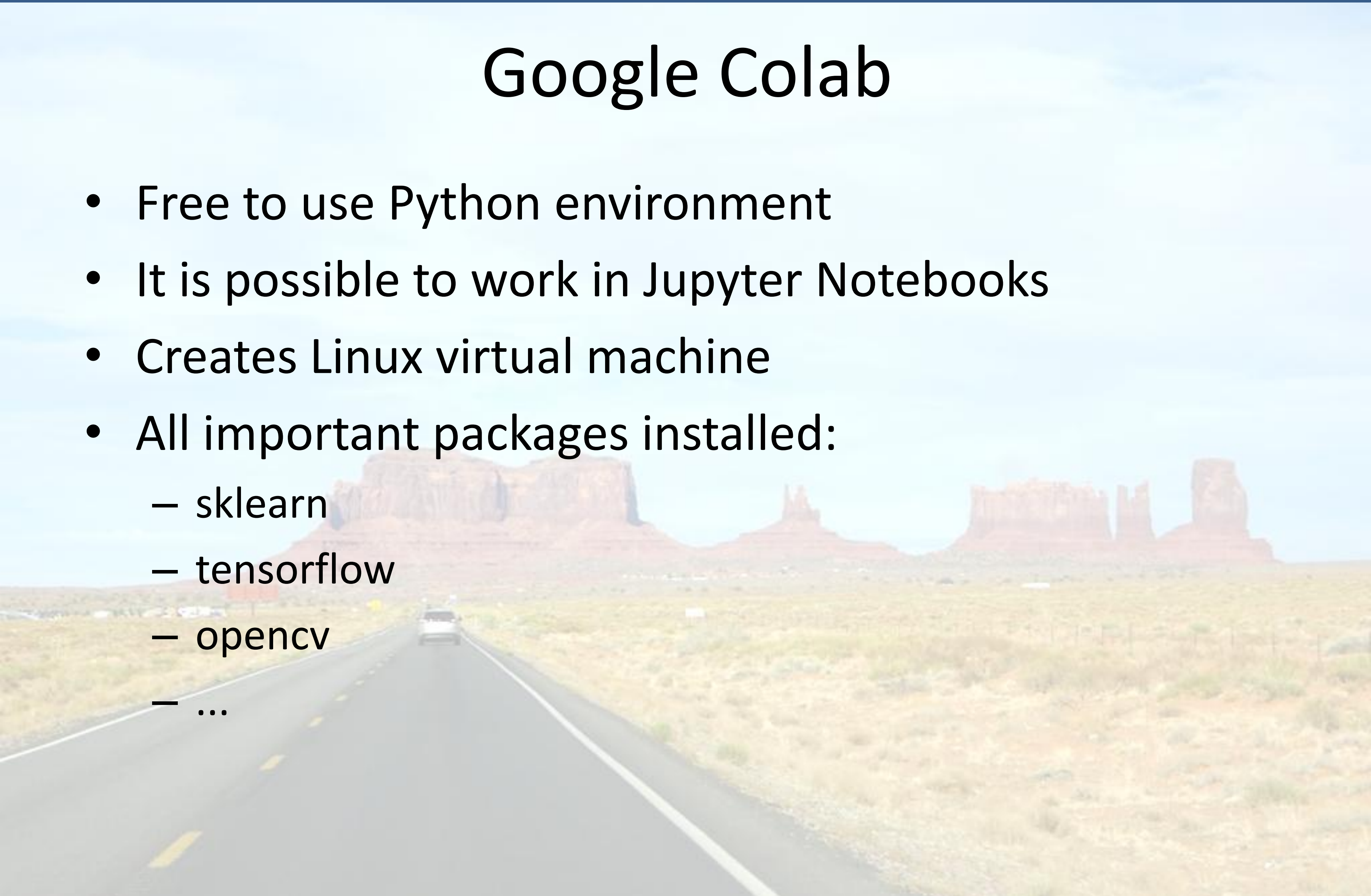
1. Introduction to Machine Learning
2. Regression
3. Neural Networks
4. Convolutional Neural Networks
5. Adversarial Attacks
6. Generative Adversarial Networks

About 30 min per module (one shorter and one longer)

Materials

- Presentations and code available at GitHub:
  - https://www.github.com/kasprowski/cyber2022
- Jupyter Notebooks that may be started e.g. in Google Colab
  - https://colab.research.google.com/
- It is also possible to start examples on your own computer
  - e.g. in Anaconda environment

Google Colab



- Free to use Python environment
- It is possible to work in Jupyter Notebooks
- Creates Linux virtual machine
- All important packages installed:
  - sklearn
  - tensorflow
  - opencv
  - ...

Local installation

- Install Miniconda
  - https://docs.conda.io/en/latest/miniconda.html
- Run „Anaconda prompt”
- Create a new environment:
  - conda create --name myname
- Activate the environment: activate myname
- Install packages using the conda tool:
  - conda install <package> - jupyterlab, pandas, matplotlib, scikit-learn, tensorflow, pip
- Install packages using pip
  - pip install <package> - opencv-contrib-python, pygame, thorpy

Code analysis

- All examples are runnable!
- I will not explain ALL details
- If you have questions – there will be a QA session
- You can also always ask by email

- Enjoy listening!
- Try to execute
- Try to change and see what happens – it is the best way to learn!

photo: Utah

Współczesne wyzwania z zakresu cyberbezpieczeństwa

Artificial Intelligence

Paweł Kasprowski, PhD, DSc.