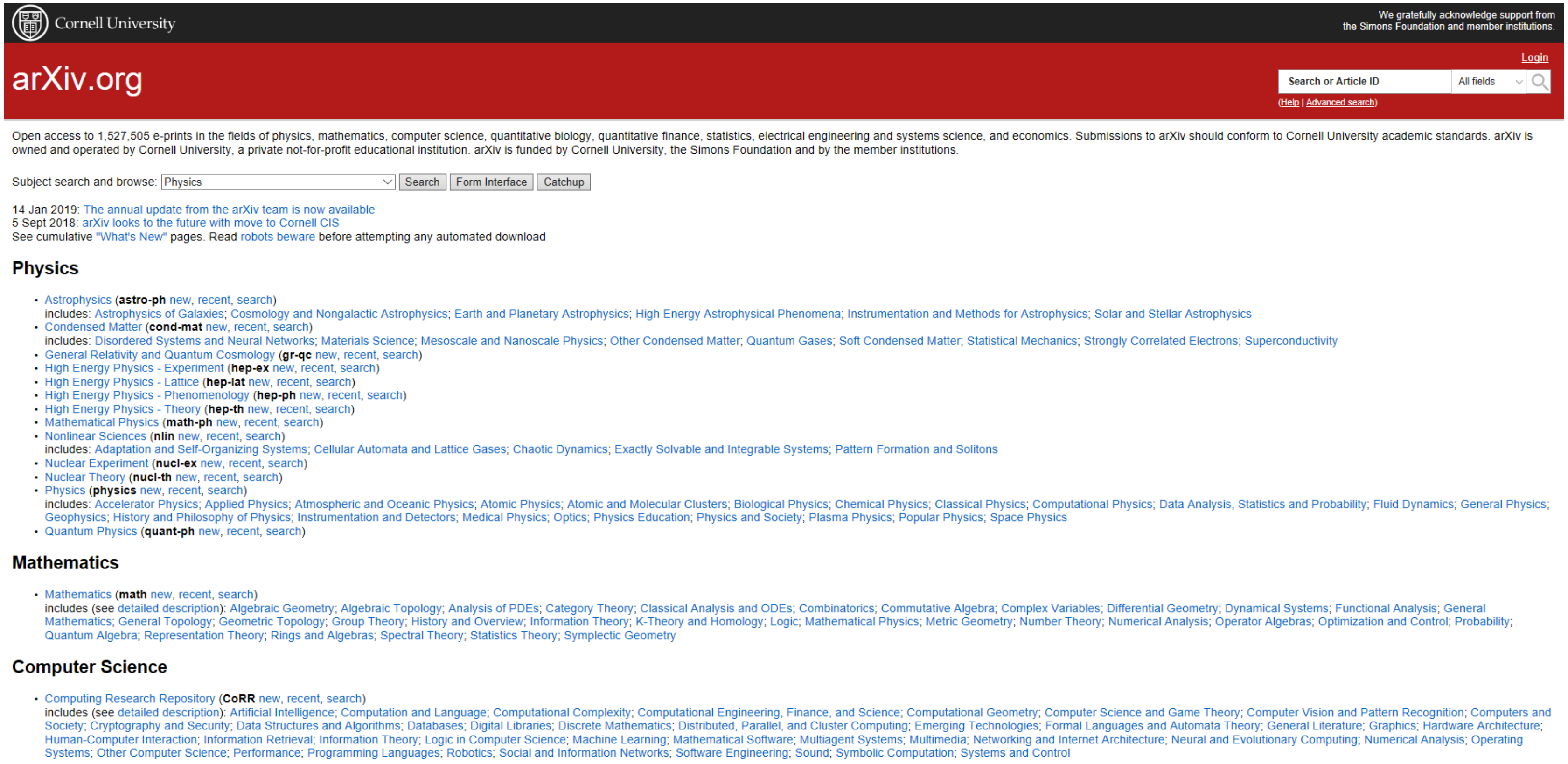
Homework 2

Regular Expression with Python

Parsing the Paper

arXiv (https://arxiv.org/)

- a repository of electronic preprints



Open access to 1,527,505 e-prints in the fields of physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics. Submissions to arXiv should conform to Cornell University academic standards. arXiv is owned and operated by Cornell University, a private not-for-profit educational institution. arXiv is funded by Cornell University, the Simons Foundation and by the member institutions.

Subject search and browse: Physics [Search] [Form Interface] [Catchup]

14 Jan 2019: The annual update from the arXiv team is now available
5 Sept 2018: arXiv looks to the future with move to Cornell CIS
See cumulative "What's New" pages. Read robots beware before attempting any automated download

Physics

- Astrophysics (**astro-ph** new, recent, search)
  includes: Astrophysics of Galaxies; Cosmology and Nongalactic Astrophysics; Earth and Planetary Astrophysics; High Energy Astrophysical Phenomena; Instrumentation and Methods for Astrophysics; Solar and Stellar Astrophysics
- Condensed Matter (**cond-mat** new, recent, search)
  includes: Disordered Systems and Neural Networks; Materials Science; Mesoscale and Nanoscale Physics; Other Condensed Matter; Quantum Gases; Soft Condensed Matter; Statistical Mechanics; Strongly Correlated Electrons; Superconductivity
- General Relativity and Quantum Cosmology (**gr-qc** new, recent, search)
- High Energy Physics - Experiment (**hep-ex** new, recent, search)
- High Energy Physics - Lattice (**hep-lat** new, recent, search)
- High Energy Physics - Phenomenology (**hep-ph** new, recent, search)
- High Energy Physics - Theory (**hep-th** new, recent, search)
- Mathematical Physics (**math-ph** new, recent, search)
- Nonlinear Sciences (**nlin** new, recent, search)
  includes: Adaptation and Self-Organizing Systems; Cellular Automata and Lattice Gases; Chaotic Dynamics; Exactly Solvable and Integrable Systems; Pattern Formation and Solitons
- Nuclear Experiment (**nucl-ex** new, recent, search)
- Nuclear Theory (**nucl-th** new, recent, search)
- Physics (**physics** new, recent, search)
  includes: Accelerator Physics; Applied Physics; Atmospheric and Oceanic Physics; Atomic Physics; Atomic and Molecular Clusters; Biological Physics; Chemical Physics; Classical Physics; Computational Physics; Data Analysis, Statistics and Probability; Fluid Dynamics; General Physics; Geophysics; History and Philosophy of Physics; Instrumentation and Detectors; Medical Physics; Optics; Physics Education; Physics and Society; Plasma Physics; Popular Physics; Space Physics
- Quantum Physics (**quant-ph** new, recent, search)

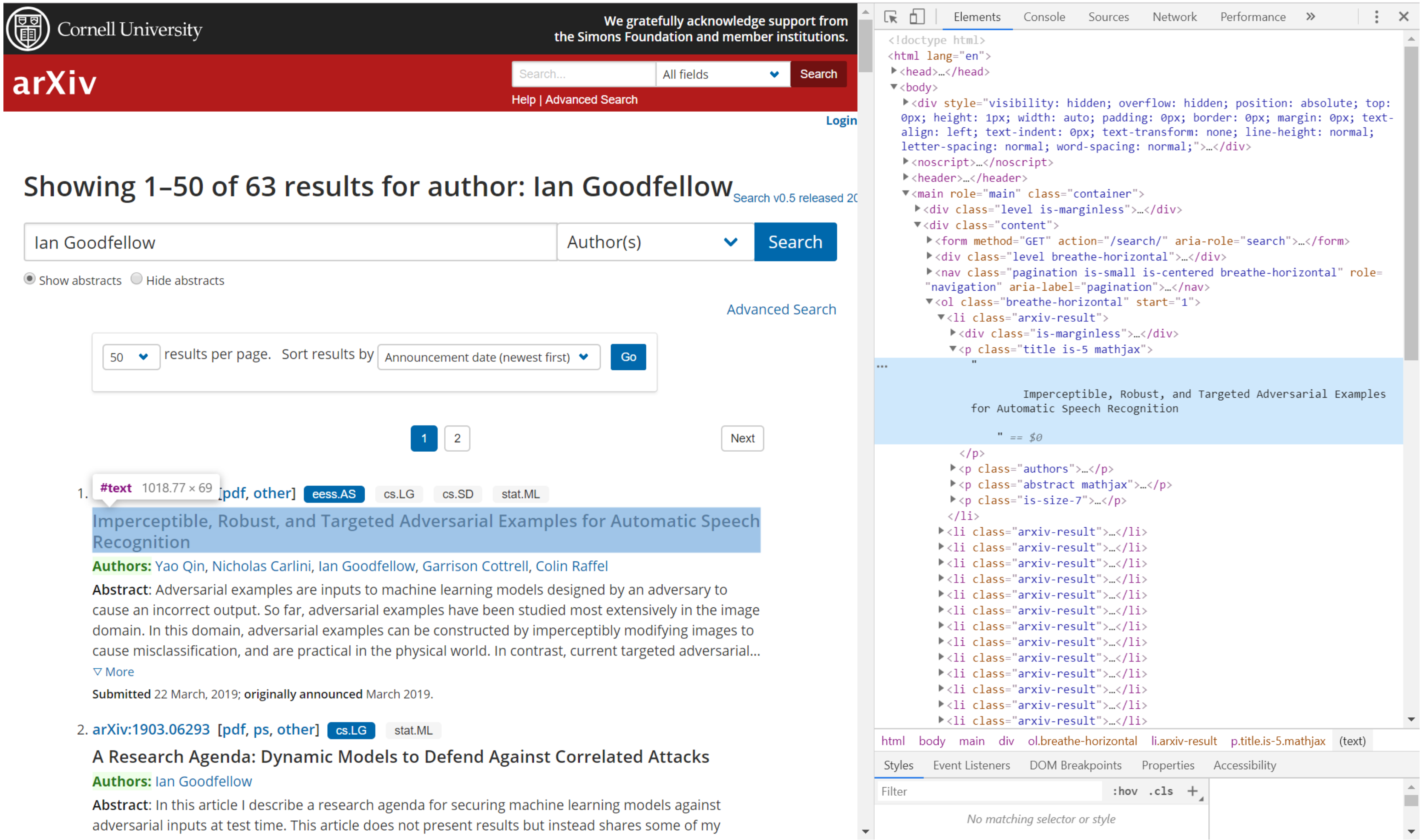
Mathematics

- Mathematics (**math** new, recent, search)
  includes (see detailed description): Algebraic Geometry; Algebraic Topology; Analysis of PDEs; Category Theory; Classical Analysis and ODEs; Combinatorics; Commutative Algebra; Complex Variables; Differential Geometry; Dynamical Systems; Functional Analysis; General Mathematics; General Topology; Geometric Topology; Group Theory; History and Overview; Information Theory; K-Theory and Homology; Logic; Mathematical Physics; Metric Geometry; Number Theory; Numerical Analysis; Operator Algebras; Optimization and Control; Probability; Quantum Algebra; Representation Theory; Rings and Algebras; Spectral Theory; Statistics Theory; Symplectic Geometry

Computer Science

- Computing Research Repository (**CoRR** new, recent, search)
  includes (see detailed description): Artificial Intelligence; Computation and Language; Computational Complexity; Computational Engineering, Finance, and Science; Computational Geometry; Computer Science and Game Theory; Computer Vision and Pattern Recognition; Computers and Society; Cryptography and Security; Data Structures and Algorithms; Databases; Digital Libraries; Discrete Mathematics; Distributed, Parallel, and Cluster Computing; Emerging Technologies; Formal Languages and Automata Theory; General Literature; Graphics; Hardware Architecture; Human-Computer Interaction; Information Retrieval; Information Theory; Logic in Computer Science; Machine Learning; Mathematical Software; Multiagent Systems; Multimedia; Networking and Internet Architecture; Neural and Evolutionary Computing; Numerical Analysis; Operating Systems; Other Computer Science; Performance; Programming Languages; Robotics; Social and Information Networks; Software Engineering; Sound; Symbolic Computation; Systems and Control

Browser Tools



Cornell University

We gratefully acknowledge support from
the Simons Foundation and member institutions.

arXiv

Search... | All fields | Search

Help | Advanced Search

Login

Showing 1–50 of 63 results for author: Ian Goodfellow

Search v0.5 released 20

Ian Goodfellow | Author(s) | Search

● Show abstracts ○ Hide abstracts

Advanced Search

50 results per page. Sort results by Announcement date (newest first) Go

1 2 Next

1. #text 1018.77 × 69 [pdf, other] eess.AS cs.LG cs.SD stat.ML

Imperceptible, Robust, and Targeted Adversarial Examples for Automatic Speech Recognition

Authors: Yao Qin, Nicholas Carlini, Ian Goodfellow, Garrison Cottrell, Colin Raffel

Abstract: Adversarial examples are inputs to machine learning models designed by an adversary to cause an incorrect output. So far, adversarial examples have been studied most extensively in the image domain. In this domain, adversarial examples can be constructed by imperceptibly modifying images to cause misclassification, and are practical in the physical world. In contrast, current targeted adversarial...

▽ More

Submitted 22 March, 2019; **originally announced** March 2019.

2. arXiv:1903.06293 [pdf, ps, other] cs.LG stat.ML

A Research Agenda: Dynamic Models to Defend Against Correlated Attacks

Authors: Ian Goodfellow

Abstract: In this article I describe a research agenda for securing machine learning models against adversarial inputs at test time. This article does not present results but instead shares some of my

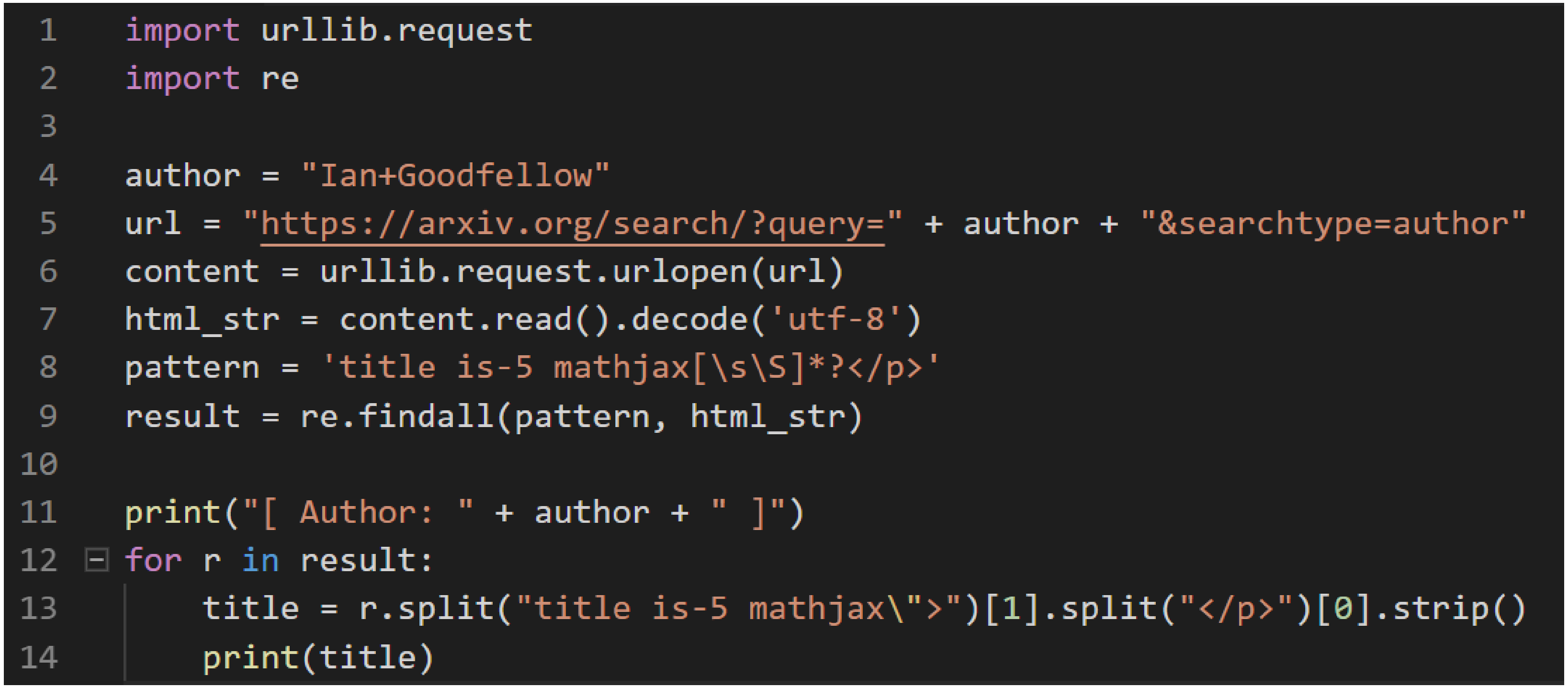
```
<!doctype html>
<html lang="en">
 ▶<head>…</head>
 ▼<body>
   ▶<div style="visibility: hidden; overflow: hidden; position: absolute; top:
   0px; height: 1px; width: auto; padding: 0px; border: 0px; margin: 0px; text-
   align: left; text-indent: 0px; text-transform: none; line-height: normal;
   letter-spacing: normal; word-spacing: normal;">…</div>
   ▶<noscript>…</noscript>
   ▶<header>…</header>
   ▼<main role="main" class="container">
     ▶<div class="level is-marginless">…</div>
     ▼<div class="content">
       ▶<form method="GET" action="/search/" aria-role="search">…</form>
       ▶<div class="level breathe-horizontal">…</div>
       ▶<nav class="pagination is-small is-centered breathe-horizontal" role=
       "navigation" aria-label="pagination">…</nav>
       ▼<ol class="breathe-horizontal" start="1">
         ▼<li class="arxiv-result">
           ▶<div class="is-marginless">…</div>
           ▼<p class="title is-5 mathjax">
...          "

                   Imperceptible, Robust, and Targeted Adversarial Examples
             for Automatic Speech Recognition

                 " == $0
           </p>
           ▶<p class="authors">…</p>
           ▶<p class="abstract mathjax">…</p>
           ▶<p class="is-size-7">…</p>
         </li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
         ▶<li class="arxiv-result">…</li>
```

html body main div ol.breathe-horizontal li.arxiv-result p.title.is-5.mathjax (text)

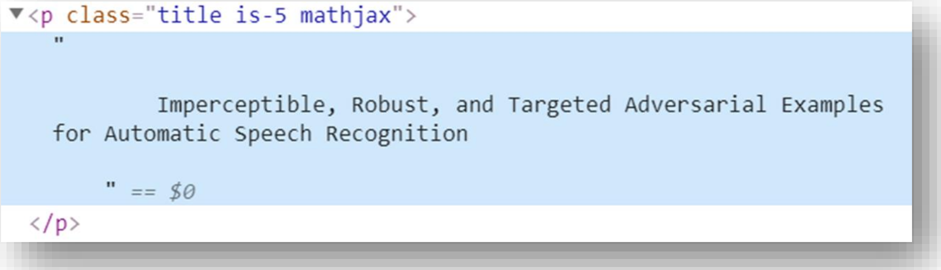
No matching selector or style

Python Example

- Get the title of each papers of an author



```python
import urllib.request
import re

author = "Ian+Goodfellow"
url = "https://arxiv.org/search/?query=" + author + "&searchtype=author"
content = urllib.request.urlopen(url)
html_str = content.read().decode('utf-8')
pattern = 'title is-5 mathjax[\s\S]*?</p>'
result = re.findall(pattern, html_str)

print("[ Author: " + author + " ]")
for r in result:
    title = r.split("title is-5 mathjax\">")[1].split("</p>")[0].strip()
    print(title)
```



```html
▼<p class="title is-5 mathjax">
   "

          Imperceptible, Robust, and Targeted Adversarial Examples
   for Automatic Speech Recognition

       " == $0
 </p>
```

Python Example

```
pattern = 'title is-5 mathjax[\s\S]*?</p>'
```

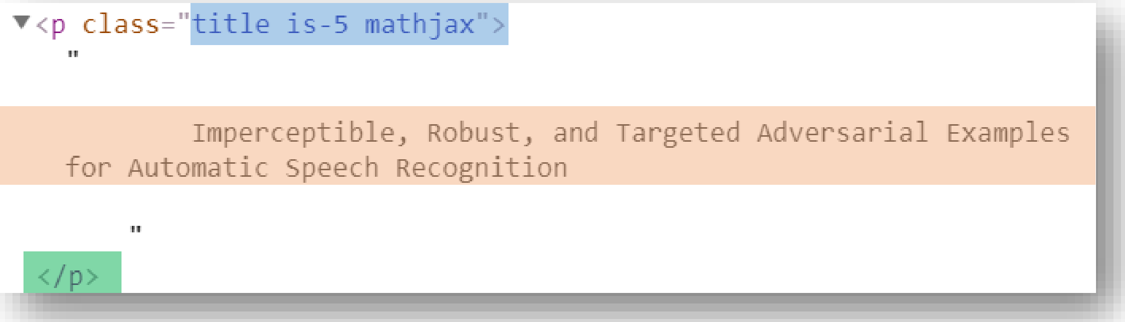
\s: whitespace characters

\S: non-whitespace character

* : repeat several times

? : matches either once or zero times

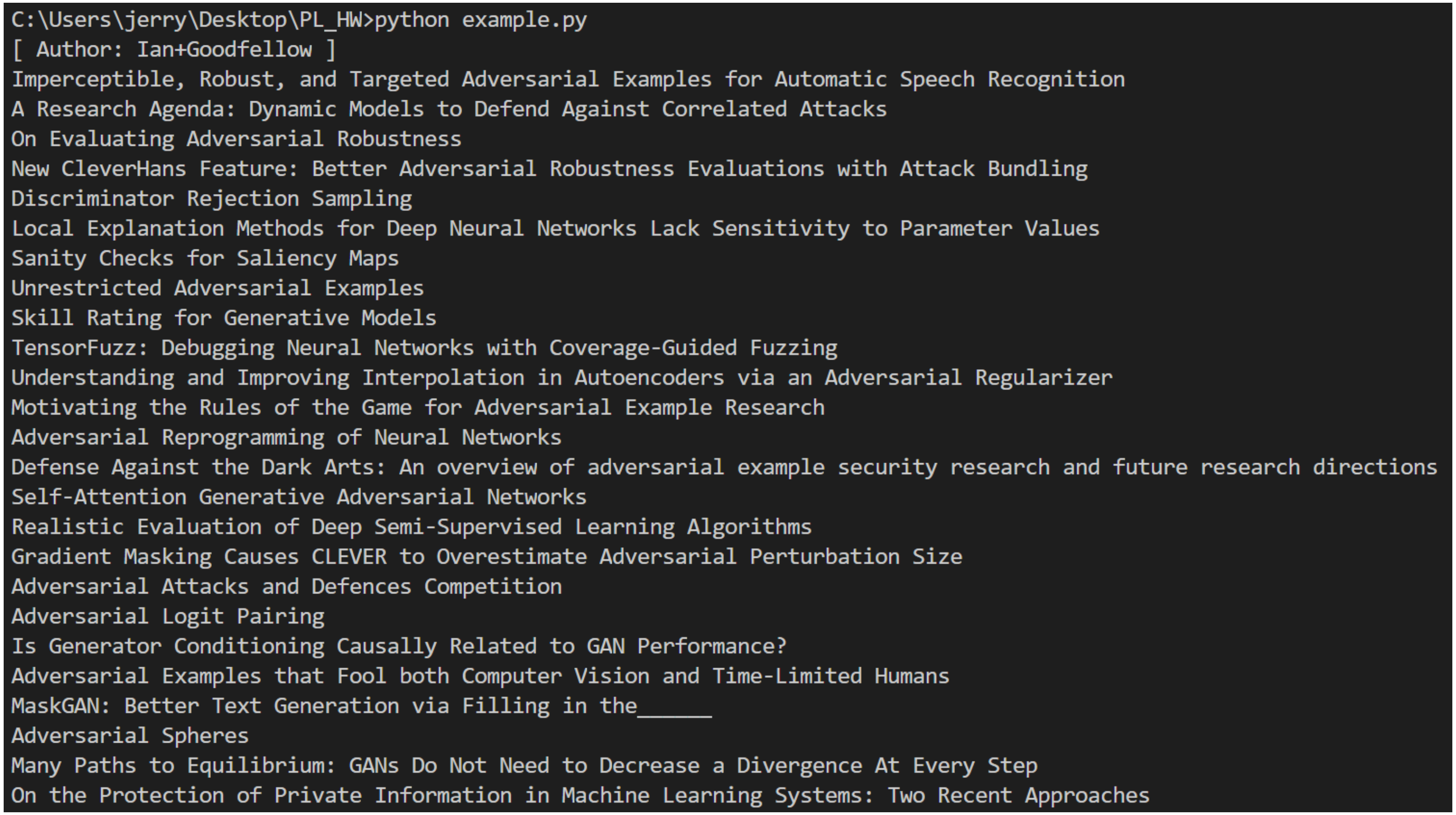
```
title = r.split("title is-5 mathjax\">")[1].split("</p>")[0].strip()
```



```
▼<p class="title is-5 mathjax">
   "
            Imperceptible, Robust, and Targeted Adversarial Examples
   for Automatic Speech Recognition

       "
  </p>
```

Python Example

- Result



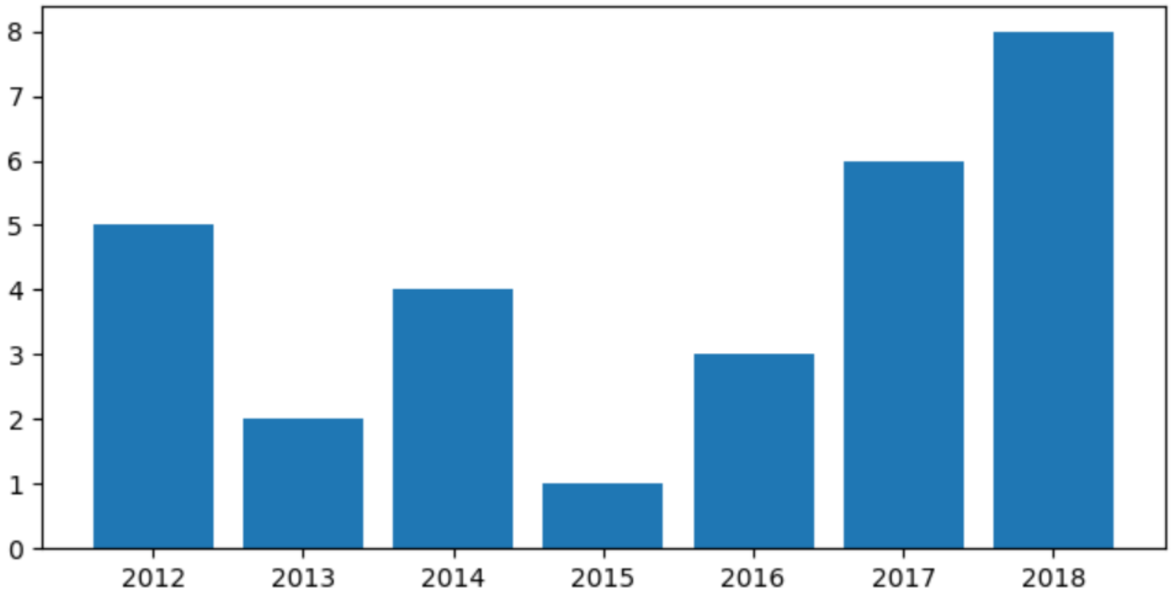
```
C:\Users\jerry\Desktop\PL_HW>python example.py
[ Author: Ian+Goodfellow ]
Imperceptible, Robust, and Targeted Adversarial Examples for Automatic Speech Recognition
A Research Agenda: Dynamic Models to Defend Against Correlated Attacks
On Evaluating Adversarial Robustness
New CleverHans Feature: Better Adversarial Robustness Evaluations with Attack Bundling
Discriminator Rejection Sampling
Local Explanation Methods for Deep Neural Networks Lack Sensitivity to Parameter Values
Sanity Checks for Saliency Maps
Unrestricted Adversarial Examples
Skill Rating for Generative Models
TensorFuzz: Debugging Neural Networks with Coverage-Guided Fuzzing
Understanding and Improving Interpolation in Autoencoders via an Adversarial Regularizer
Motivating the Rules of the Game for Adversarial Example Research
Adversarial Reprogramming of Neural Networks
Defense Against the Dark Arts: An overview of adversarial example security research and future research directions
Self-Attention Generative Adversarial Networks
Realistic Evaluation of Deep Semi-Supervised Learning Algorithms
Gradient Masking Causes CLEVER to Overestimate Adversarial Perturbation Size
Adversarial Attacks and Defences Competition
Adversarial Logit Pairing
Is Generator Conditioning Causally Related to GAN Performance?
Adversarial Examples that Fool both Computer Vision and Time-Limited Humans
MaskGAN: Better Text Generation via Filling in the______
Adversarial Spheres
Many Paths to Equilibrium: GANs Do Not Need to Decrease a Divergence At Every Step
On the Protection of Private Information in Machine Learning Systems: Two Recent Approaches
```

Question 1 (40%)

- Draw the bar graph of the number of papers been published each year of an author

Ex.

```
Input Author: [Name of author]
```



Question 2 (60%)

- Count the number of papers written together of each co-author
- The name of co-authors have to be sorted according to alphabet (i.e. a-z)

Ex.

```
Input Author: [Name of author]
[Name of co-author 1]: XX times
[Name of co-author 2]: XX times
[Name of co-author 3]: XX times
```

Notice

Deadline: 2019/05/1 22:00

Only the URL Library (urllib) and Regular Expression Library (re) are allowed to be used.