Python Forensics

Authored by: girish ramnani

What this talk is all about?

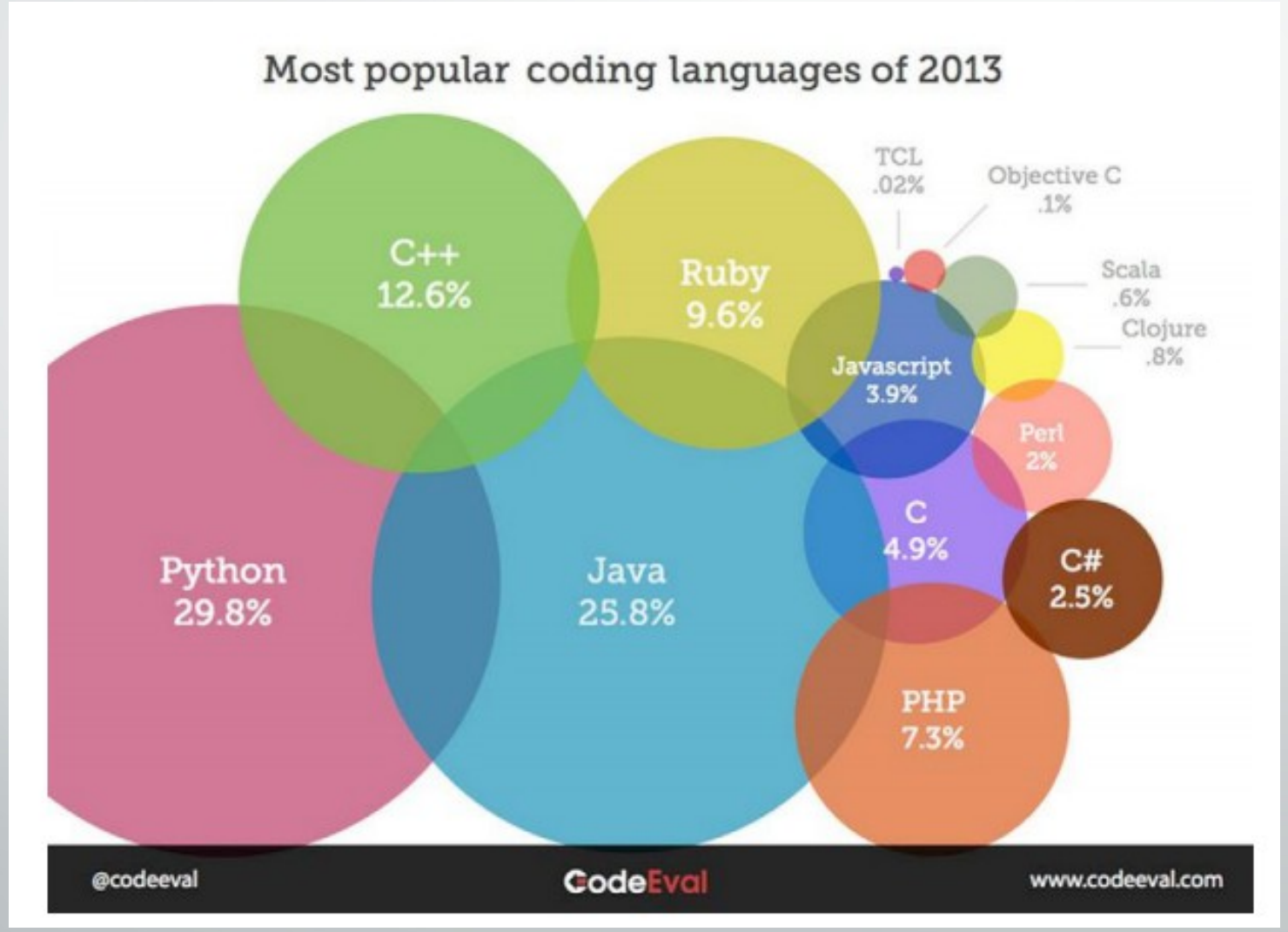
- Learning python for creating forensic tools
- Learning some great extra concepts such as natural language analysis
- Having fun

Table of Content

Why python?

- Syntactic sugar
- Large community
- due to Python’s intrinsic extensibility , copious amount of third-party libraries and modules exist.

Survey


Most popular coding languages of 2013
C++
12.6%
Ruby
9.6%
TCL
.02%
Objective C
.1%
Scala
.6%
Clojure
.8%
Javascript
3.9%
Perl
2%
C
4.9%
C#
2.5%
Python
29.8%
Java
25.8%
PHP
7.3%
@codeeval
CodeEval
www.codeeval.com

Python quick review

- print(“hello”)
- [1,2,3,4]
- for e , value in enumerate(range(4))
- Print the reverse of a number

APP1 : Socket Scanner

- A basic script to find the open sockets

APP 2: FILE HASHER

- File hasher is a command line tool which has following functionality
  - Finds the hash of any given file
  - Supports 3 hashing algorithm (md5, sha256,sha512)
  - Generates a .csv file with the report of processed file

Modules used

- Argparse
- Csv
- Hashlib

And some other standard libraries

the division of classes

CSV writer

__init__
(filename,hashtype)

Writerow(variable arguments)

Walk_path()

Walks the path given

Hash_file(filename , csv writer)

Ur Part

- The template consists of incomplete code , ur part would be to bring together those parts and complete the code.

Thank you