Agentless crawler: <https://github.com/cloudviz/agentless-system-crawler>

Itemset Mining and related work: <https://github.com/fideliscyber/yalda>

<https://github.com/bartdag/pymining> (I sent to Prabhakar)

Prabhakar assigned task to me:

Please do this exercise for practice. It's not the focus of our algorithm, but we want to  
leverage some of the core mechanisms.  Think of a way you can add  
a non-standard actuation of a response based on your independent analysis of  
crawler data.  The actual algorithm of what we are analyzing, we can discuss next week.  
<https://www.stratoscale.com/blog/kubernetes/auto-healing-containers-kubernetes/>

**Crawler Codes and description:**

python crawler/crawler.py --crawlContainers test --url "file://output/before.csv" --features os

Metrics description

|  |  |
| --- | --- |
| Metrics | Description |
| Os | Os name, version. Kernel, architecture |
| disk | Partition name, freepct, fstype, mountpt, mountopts, partition size |
| Process | Details of process running inside container |
| Connection |  |
| Metric | Monitoring of light container (cpu, memory usage etc.) |
| package | Package name, size, verison, architecture |
| File | Details of all the files in container. The details contain atime, ctime, gid, links, mode, mtime, name, path, size, type, uid |
| config | Name, content and path of all the configuration files in container. For example: sshd\_config, /etc/hosts, /proc/19077/mounts etc. |

Comparing different way of extraction features. Different features from different containers. Find the better way. Look for new way of extracting features.

Kubernetes docker: <https://zwischenzugs.com/2015/04/06/play-with-kubernetes-quickly-using-docker/>

Kubernetes minikube: <https://github.com/kubernetes/minikube>

**Exercise: Classify container OS types.**

python crawler/crawler.py --crawlContainers 72d014d15513 --url "file://output/ubuntu\_mysql.csv" --features file --crawlmode OUTCONTAINER

Ubuntu releases are at: <https://wiki.ubuntu.com/Releases>

Centos releases: <https://wiki.centos.org/Download> <https://hub.docker.com/_/centos/>

Image fetching and container launching command: docker run -d --name=centos6.9 centos:6.9 bash -c "while true; do sleep 1; done"

**Crawling Script:**

python crawler/crawler.py --crawlContainers a0f8e1c9ede0 --url "file://output/centos5" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 558fa9c5643a --url "file://output/centos7.4.1708" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 90e3d7fbcc20 --url "file://output/centos7.3.1611" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 3396d9e7ba26 --url "file://output/centos7.2.1511" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 97bb3c044d41 --url "file://output/centos7.1.1503" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers f6175eb9936f --url "file://output/centos7.0.1406" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers a8b14a36fb59 --url "file://output/centos6" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 6a77cdcd4e51 --url "file://output/centos5.11" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 19494226358d --url "file://output/centos6.6" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 55c7f40f0eac --url "file://output/centos6.7" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 7f4c7d980794 --url "file://output/centos6.8" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers fc5fcc54e9be --url "file://output/centos6.9" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 59d57860f4ae --url "file://output/centos7" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers e11366eb15a4 --url "file://output/ubuntu10.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 1a0e573b9665 --url "file://output/ubuntu12.04.5" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 2c67f0261f71 --url "file://output/ubuntu12.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 7a838b8719e1 --url "file://output/ubuntu12.10" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 9588ae629aea --url "file://output/ubuntu13.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 86c64f9624e7 --url "file://output/ubuntu13.10" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 2a6b350b49f3 --url "file://output/ubuntu15.10" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers ec782ccc466e --url "file://output/ubuntu16.10" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 140e8fbad90b --url "file://output/ubuntu17.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 6a75aab4424d --url "file://output/ubuntu18.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers f26902038205 --url "file://output/ubuntu17.10" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 579859c874dc --url "file://output/ubuntu16.04" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 0db3a66d6794 --url "file://output/ubuntu14.04.5" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers c83e5a548c50 --url "file://output/ubuntu14.04.4" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers 9bd5b4d0cd69 --url "file://output/ubuntu14.04.3" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers fb4035e1c467 --url "file://output/ubuntu14.04.2" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers fdbe7226379e --url "file://output/ubuntu14.04.1" --features file,package --crawlmode OUTCONTAINER

python crawler/crawler.py --crawlContainers d9664eaca4a5 --url "file://output/ubuntu14.04" --features file,package --crawlmode OUTCONTAINER

Whitelisted Profile: <https://www.twistlock.com/2017/05/31/twistlock-uses-machine-learning/>

One class SVM: <http://scikit-learn.org/stable/modules/generated/sklearn.svm.OneClassSVM.html>

<http://scikit-learn.org/stable/auto_examples/svm/plot_oneclass.html#sphx-glr-auto-examples-svm-plot-oneclass-py>