Traffic analysis via Pacumen

Zanin, Flávio E. G.

Dalhousie University

flavio.zanin@dal.ca

Surpervisor: Dr. Nur Zincir-Heywood

Abstract: This document gives a summary of the author's experiences on the installation and the usage of a tool called Pacumen [1, 2] for network traffic analysis. All the installation and experimentation done in this work are performed on a 64 bit Ubuntu-16.04 machine.

1) Installation

Note: Every time a command starts with "sudo" (Super User DO), it will request your password.

1.1) Python, setuptools and pip

Python 2.7.11 was already installed in the operational system.

Run both commands:

```
$ sudo apt-get install python-pip

$ pip install setuptools
```

1.2) Pyparsing

Python comes with pyparsing 2.0.3. Pacumen requires pyparsing 1.5.7.

In order to fix the version problem, it is necessary to run the following commands in the command window:

```
$ sudo apt-get install python-numpy python-scipy python-
matplotlib ipython ipython-notebook python-pandas python-
sympy python-nose

$ pip uninstall pyparsing
```

```
$ pip install pyparsing==1.5.7

$ pip install pydot
```

It is worth noting that if you had pyparsing installed through setup.py, you'll need to uninstall the package in a different manner. Read more here.

If you find the error: Not uninstalling pyparsing at (path), outside environment (path).

Go to your local files (mine was /home/flavio/.local/lib/python2.7/site-packages). Run:

```
$ pip install pyparsing==1.5.7

$ sudo cp ./pyparsing-1.5.7.dist-info
/usr/lib/python2.7/dist-packages

$ sudo cp ./pyparsing.py /usr/lib/python2.7/dist-packages

$ sudo cp ./pyparsing.pyc /usr/lib/python2.7/dist-packages

$ sudo rm -r pyparsing-2.0.3
```

If you're writing the commands by hand, make sure to note the spaces between the paths.

If you successfully installed pyparsing version 1.5.7, run:

```
$ pip freeze
```

And look for pyparsing on the printed result.

Troubleshooting

If you still have version 2.0.3 installed (or you found the error ***Not uninstalling pyparsing at (path), outside environment (path)***), you have some options:

Option 1: Look into python virtual environments. This will allow you to install certain modules with older versions to work on certain projects, without using the updated versions in your computer.

Option 2: This is a hack to install pyparsing 1.5.7. Note that this method will substitute your current version of pyparsing. Go to your local python files (for me it is /home/flavio/.local/lib/python2.7/site-packages). Run:

```
$ pip install pyparsing==1.5.7
```

```
$ sudo cp ./pyparsing-1.5.7.dist-info
/usr/lib/python2.7/dist-packages

$ sudo cp ./pyparsing.py /usr/lib/python2.7/dist-packages

$ sudo cp ./pyparsing.pyc /usr/lib/python2.7/dist-packages
```

1.3) Pacumen

Download Pacumen here.

Unzip ($ unzip pacumen_master.zip), enter the unzipped directory and run:

```
$ python setup.py build

$ pip install numpy

$ sudo python setup.py install
```

The installed folder will be somewhere in your PATH variable. In my case, it was on /usr/local/bin. You can find out your PATH variable by running:

```
$ echo $PATH
```

Look into the printed PATH directories to find the following scripts: `pacumen_classify.py, pacumen_timeseries.py, pacumen_train.py, pacumen_visualize.py, train_all.py, xval.py`.

These Pacumen scripts will be present somewhere in your printed PATH directories if the installation was successful.

1.4) Regex

Run:

```
$ pip install regex
```

1.5) Particle

First, we need libjpeg installed. For that, check your command for your Linux version here. For my computer (Ubuntu 16.04) I used the command:

```
$ sudo apt-get install libtiff5-dev libjpeg8-dev zlib1g-dev
libxml2 libxml2-dev libfreetype6-dev liblcms2-dev libwebp-
```

```
dev tcl8.6-dev tk8.6-dev python-tk libxslt-dev libxslt1-dev
python-dev
```

Now run the command (**Note: If your python version is 3.x**, you should substitute *python-lxml* for *python3-lxml* in the command line):

```
$ sudo apt-get install python-lxml
```

Download libxml2 here. Extract the libxml2 contents and open a terminal window inside the folder *libxml2-2.9.3*. Execute the commands:

```
$ ./configure --prefix=/usr --disable-static --with-history && make
```

```
$ sudo make install
```

If you get an error during the make install phase, you might not need to reinstall. Attempt to download and install libxslt (next section).

Download libxslt here. Extract the libxslt contents. Inside the libxslt-1.1.28 folder, open a terminal window. Run the commands:

```
$ ./configure --prefix=/usr –disable-static && make
```

```
$ sudo make install
```

If you get an error during the *make install* phase, you might not need to reinstall. Attempt to download and install lxml (next section).

Now install lxml. This step can take a few minutes, so let the command run until it either returns an error or success.

If there were previous errors, they might or might not affect this step. Run the command:

```
$ pip install lxml
```

If you get an error during this phase, you might have to reinstall libxml or libxslt.

Now run:

```
$ pip install pillow
```

```
$ pip install particle
```

1.6) Automatamm

Automatamm is used for the script *pacumen_timeseries.py*. I was unable to find automatamm online for download. Pacumen's author was contacted regarding this, but no response was received.

If not installed, all scripts work except for *pacumen_timeseries.py*.

2) Using Pacumen

In order to use Pacumen, it is necessary to open a terminal in the folder pacumen was installed from (pacumen_master).

Datasets:

A few datasets were generated in the lab using Wireshark. The datasets will be described through these names:

Chrome Random – Dataset generated in the lab using **Google Chrome**, browsing random websites and actively avoiding **Gmail, Facebook, Twitter and Linkedin**.

Firefox Random – Dataset generated in the lab using **Mozilla Firefox**, browsing random websites and actively avoiding **Gmail, Facebook, Twitter and Linkedin**.

Chrome [Facebook / Gmail / Linkedin] – Dataset generated in the lab using **Google Chrome**, browsing only the indicated website. E.g.: **Chrome Facebook** was generated by browsing only **Facebook** on **Google Chrome**.

Firefox [Facebook / Gmail / Linkedin / Outlook / Twitter / Youtube] – Same as the previous dataset, however generated by browsing on **Mozilla Firefox**.

Skype – Dataset generated in the lab using **Skype.**

Macc50k – 50,000 packets from the publicly available dataset **macc2012_00003.pcap** under the MACCDC section in the Cyber Defense Exercises section on Netresec's public available [3] pcap files.

It's important to note that **Skype was not installed before it was needed for its dataset**, therefore there is no traffic from it on the other datasets.

2.1) Pacumen_classify_pcap.py

According to the help section, this script prints the probability that a pcap file contains the protocol the classifier was trained for.

```
def print_help():
  print '''
  run a classifier against a pcap and print the probability that it contains the classified protocol

  usage: %s -C classifier <pcap files>

  ''' % (sys.argv[0])
```

Therefore, this script was tested for its classifications against different datasets, some which were generated according to the classifier and some which weren't. This section presents the results.

2.1.1) ssh.chrome.facebook

When using this classifier, the results were as follows:

Dataset **Chrome Facebook – 0.967423**.

Dataset **Chrome Random – 0.997666**.

Dataset **Firefox Random – 0.99999**.

Chrome Facebook:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.facebook ./CustomDB/ChromeFacebook.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.967423   ./CustomDB/ChromeFacebook.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.facebook ./CustomDB/ChromeRandomBrowsing.p
cap
WARNING: No route found for IPv6 destination :: (no default route?)
0.997666  ./CustomDB/ChromeRandomBrowsing.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.facebook ./CustomDB/FirefoxRandomBrowsing.
pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990  ./CustomDB/FirefoxRandomBrowsing.pcap
```

2.1.2) ssh.chrome.gmail

When using this classifier, the results were as follows:

Dataset **Chrome Gmail – 0.730966**.

Dataset **Chrome Random – 0.871624**.

Dataset **Firefox Random – 0.996578**.

Chrome Gmail:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.gmail ./CustomDB/ChromeGmail.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.730966  ./CustomDB/ChromeGmail.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.gmail ./CustomDB/ChromeRandomBrowsing.pcap

WARNING: No route found for IPv6 destination :: (no default route?)
0.871624  ./CustomDB/ChromeRandomBrowsing.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.gmail ./CustomDB/FirefoxRandomBrowsing.pca
p
WARNING: No route found for IPv6 destination :: (no default route?)
0.996578  ./CustomDB/FirefoxRandomBrowsing.pcap
```

2.1.3) ssh.chrome.linkedin

When using this classifier, the results were as follows:

Dataset **Chrome Linkedin – 0.998342**.

Dataset **Chrome Random – 0.99999**.

Dataset **Firefox Random – 0.99983**.

Chrome Linkedin:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.linkedin ./CustomDB/ChromeLinkedin.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.998342  ./CustomDB/ChromeLinkedin.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.linkedin ./CustomDB/ChromeRandomBrowsing.p
cap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990  ./CustomDB/ChromeRandomBrowsing.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.chrome.linkedin ./CustomDB/FirefoxRandomBrowsing.
pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999830  ./CustomDB/FirefoxRandomBrowsing.pcap
```

2.1.4) ssh.firefox.facebook

When using this classifier, the results were as follows:

Dataset **Firefox Facebook – 0.997351**.

Dataset **Firefox Random – 0.980129**.

Dataset **Chrome Random – 0.995892**.

Firefox Facebook:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.facebook ./CustomDB/FirefoxFacebook.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.997351  ./CustomDB/FirefoxFacebook.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.facebook ./CustomDB/FirefoxRandomBrowsing
.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.980129  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.facebook ./CustomDB/ChromeRandomBrowsing.
pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.995892  ./CustomDB/ChromeRandomBrowsing.pcap
```

2.1.5) ssh.firefox.gmail

When using this classifier, the results were as follows:

Dataset **Firefox Gmail – 0.236685**.

Dataset **Firefox Random – 0.999931**.

Dataset **Chrome Random – 0.973753**.

Firefox Gmail:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.gmail ./CustomDB/FirefoxGmail.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.236685  ./CustomDB/FirefoxGmail.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.gmail ./CustomDB/FirefoxRandomBrowsing.pc
ap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999931  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.gmail ./CustomDB/ChromeRandomBrowsing.pca
p
WARNING: No route found for IPv6 destination :: (no default route?)
0.973753  ./CustomDB/ChromeRandomBrowsing.pcap
```

2.1.6) ssh.firefox.linkedin

When using this classifier, the results were as follows:

Dataset **Firefox Linkedin – 0.999989**.

Dataset **Firefox Random – 0.99999**.

Dataset **Chrome Random – 0.999987**.

Firefox Linkedin:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.linkedin ./CustomDB/FirefoxLinkedin.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999989  ./CustomDB/FirefoxLinkedin.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.linkedin ./CustomDB/FirefoxRandomBrowsing
.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.linkedin ./CustomDB/ChromeRandomBrowsing.
pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999987  ./CustomDB/ChromeRandomBrowsing.pcap
```

2.1.7) ssh.firefox.twitter

When using this classifier, the results were as follows:

Dataset **Firefox Twitter – 0.275021**.

Dataset **Firefox Random – 0.377583**.

Dataset **Chrome Random – 0.999079**.

Firefox Twitter:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.twitter ./CustomDB/FirefoxTwitter.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.275021  ./CustomDB/FirefoxTwitter.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.twitter ./CustomDB/FirefoxRandomBrowsing.
pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.377583  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.firefox.twitter ./CustomDB/ChromeRandomBrowsing.p
cap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999079  ./CustomDB/ChromeRandomBrowsing.pcap
```

2.1.8) ssh.skype

When using this classifier, the results were as follows:

Dataset **Skype – 0.99999**.

Dataset **Firefox Random – 0.99999**.

Dataset **Chrome Random – 0.99999**.

Skype:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.skype ./CustomDB/Skype.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990  ./CustomDB/Skype.pcap
```

Firefox Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.skype ./CustomDB/FirefoxRandomBrowsing.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Chrome Random browsing:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/ssh.skype ./CustomDB/ChromeRandomBrowsing.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.999990   ./CustomDB/ChromeRandomBrowsing.pcap
```

2.2) pacumen_train.py

According to the help section of this script, the output is a classifier generated by providing an input pcap file with the target protocol and another input pcap file with the non-target protocol.

```
def print_help():
  print '''
  train a classifier for a protocol over an encryptd tunnel given pcaps
  you can specify multiple pcaps that belong to the target protocol and
  multiple pcaps that belong do not belong to the target protocol
  at least one of each must be supplied

  an output filename must also be supplied
  '''

  print 'usage: %s [-T target] [-N nontarget] [-B bias] <outputfilename>' % (sys.argv[0])

  print '''
  -T target: specify a pcap with the target protocol, may be used multiple times
  -N nontarget: specifiy a pcap without the target protocol, may be used multiple times
  -B float: bias towards >= indicates positive class (default: auto), -bias may be used for the opposite
  (optional) -D max depth: maximum depth of decision tree (default: 9)
  (optional) -M minimum bias: minimum bias to use with -B auto
  '''
```

A few classifiers were generated with this script. When no bias is given, the script looks for a bias automatically, therefore the scripted was allowed to look for the best bias for each case. Results from some of the tests are presented in this section.

2.2.1) Youtube

Classifier generation

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_train.p
y -T ./CustomDB/FirefoxYoutube.pcap -N ./CustomDB/FirefoxRandomBrowsing.pcap ./c
lassifiers/youtube_classifier
WARNING: No route found for IPv6 destination :: (no default route?)
reading pcaps
have 9 rows of target data and 23 rows of non-target data
bias 4.000000, p(positive|zerovector) = 0.500000
bias 6.000000, p(positive|zerovector) = 0.500000
bias 7.000000, p(positive|zerovector) = 0.500000
bias 7.500000, p(positive|zerovector) = 0.500000
bias 7.750000, p(positive|zerovector) = 0.500000
bias 7.875000, p(positive|zerovector) = 0.500000
bias 7.937500, p(positive|zerovector) = 0.500000
bias 7.968750, p(positive|zerovector) = 0.500000
bias 7.984375, p(positive|zerovector) = 0.500000
bias 7.992188, p(positive|zerovector) = 0.500000
bias 7.996094, p(positive|zerovector) = 0.500000
bias 7.998047, p(positive|zerovector) = 0.500000
bias 7.999023, p(positive|zerovector) = 0.500000
bias 7.999512, p(positive|zerovector) = 0.500000
bias 7.999756, p(positive|zerovector) = 0.500000
bias 7.999878, p(positive|zerovector) = 0.500000
bias 7.999939, p(positive|zerovector) = 0.500000
bias 7.999969, p(positive|zerovector) = 0.500000
bias 7.999985, p(positive|zerovector) = 0.500000
bias 7.999992, p(positive|zerovector) = 0.500000
bias 7.999996, p(positive|zerovector) = 0.500000
bias 7.999998, p(positive|zerovector) = 0.500000
writing classifier to file
Used packet sizes: set([])
```

Classifier test

Dataset **Firefox Youtube: 0.5**.

Dataset **Firefox Random: 0.5**.

Dataset **Macc50k: 0.5**.

Firefox Youtube:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/youtube_classifier ./CustomDB/FirefoxYoutube.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/FirefoxYoutube.pcap
```

Firefox Random:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/youtube_classifier ./CustomDB/FirefoxRandomBrowsing.p
cap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Macc50k:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/youtube_classifier ./CustomDB/macc_50kto100k.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/macc_50kto100k.pcap
```

2.2.2) Outlook

Classifier generation

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_train.p
y -T ./CustomDB/FirefoxOutlook.pcap -N ./CustomDB/FirefoxRandomBrowsing.pcap ./c
lassifiers/outlook_classifier
WARNING: No route found for IPv6 destination :: (no default route?)
reading pcaps
have 9 rows of target data and 23 rows of non-target data
bias 4.000000, p(positive|zerovector) = 0.500000
bias 6.000000, p(positive|zerovector) = 0.500000
bias 7.000000, p(positive|zerovector) = 0.500000
bias 7.500000, p(positive|zerovector) = 0.500000
bias 7.750000, p(positive|zerovector) = 0.500000
bias 7.875000, p(positive|zerovector) = 0.500000
bias 7.937500, p(positive|zerovector) = 0.500000
bias 7.968750, p(positive|zerovector) = 0.500000
bias 7.984375, p(positive|zerovector) = 0.500000
bias 7.992188, p(positive|zerovector) = 0.500000
bias 7.996094, p(positive|zerovector) = 0.500000
bias 7.998047, p(positive|zerovector) = 0.500000
bias 7.999023, p(positive|zerovector) = 0.500000
bias 7.999512, p(positive|zerovector) = 0.500000
bias 7.999756, p(positive|zerovector) = 0.500000
bias 7.999878, p(positive|zerovector) = 0.500000
bias 7.999939, p(positive|zerovector) = 0.500000
bias 7.999969, p(positive|zerovector) = 0.500000
bias 7.999985, p(positive|zerovector) = 0.500000
bias 7.999992, p(positive|zerovector) = 0.500000
bias 7.999996, p(positive|zerovector) = 0.500000
bias 7.999998, p(positive|zerovector) = 0.500000
writing classifier to file
Used packet sizes: set([])
```

Classifier test

Dataset **Firefox Outlook: 0.5**.

Dataset **Firefox Random: 0.5**.

Dataset **Macc50k: 0.5**.

Firefox Outlook:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/outlook_classifier ./CustomDB/FirefoxOutlook.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/FirefoxOutlook.pcap
```

Firefox Random:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/outlook_classifier ./CustomDB/FirefoxRandomBrowsing.p
cap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/FirefoxRandomBrowsing.pcap
```

Macc50k:

```
flavio@flavio-desktop:~/Desktop/Downloads/pacumen-master$ python pacumen_classif
y_pcap.py -C ./classifiers/outlook_classifier ./CustomDB/macc_50kto100k.pcap
WARNING: No route found for IPv6 destination :: (no default route?)
0.500000  ./CustomDB/macc_50kto100k.pcap
```

2.2.3) Other tests

Other classifiers were generated using datasets separating other features such as: TCP packets as target vs other protocol packets as non-targets; TCP port 80 packets as target vs anything else as non-targets. However, upon use of these classifiers on other datasets, the result was always 0.5.

3) Discussion

The experiments with the classifiers installed with Pacumen didn't provide the expected results, regardless of which browser was used or which websites were used for generating the datasets. The classifiers generated by Pacumen's script on different datasets always yielded the same results when tested, regardless of the contents of the training and test datasets.

Given there was a library missing (automatamm), I speculate this might have some impact on the used features of the software, resulting on the output obtained from the tests.

4) References

(1) Niemczyk, B; Rao, P.; Chhabra, V. **Pacumen** [Computer software]. Retrieved from: https://github.com/bniemczyk/pacumen. Accessed in: July 13th, 2016.

(2) Niemczyk, B; Rao, P. **Identification over encrypted Channels**. Retrieved from: https://www.blackhat.com/docs/us-14/materials/us-14-Niemczyk-Probabilist-Spying-On-Encrypted-Tunnels.pdf. Accessed in: July 13th, 2016.

(3) Netresec. **Publicly available PCAP files**. Retrieved from: http://www.netresec.com/?page=PcapFiles. Accessed in: July 13th, 2016.