
Vsevolod Ivanov

Concordia University

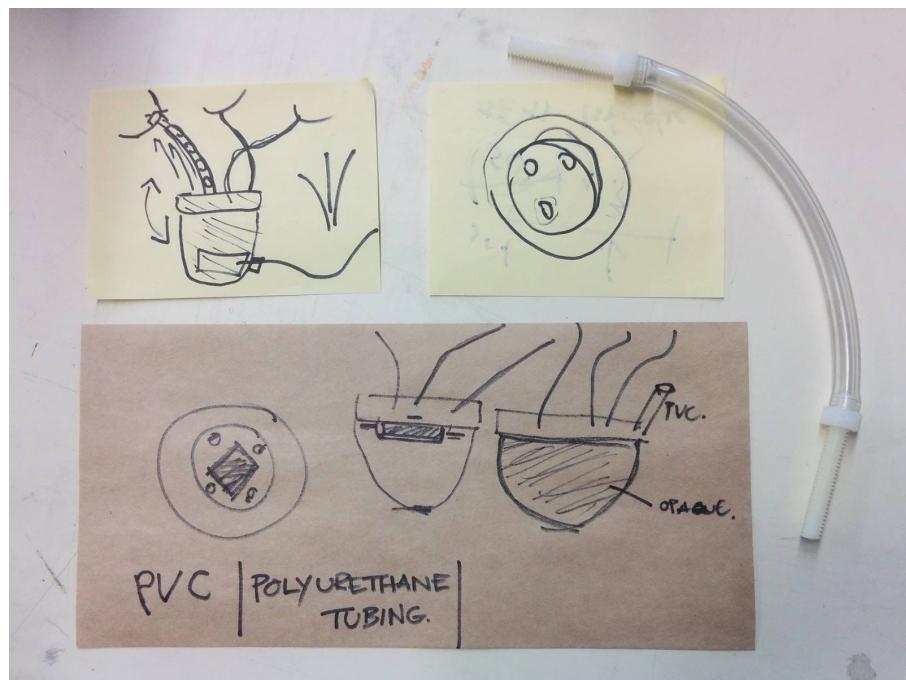
seva@tumahn.net

HackerPot

Fall 2016

Process

Concept



Translucid Pot

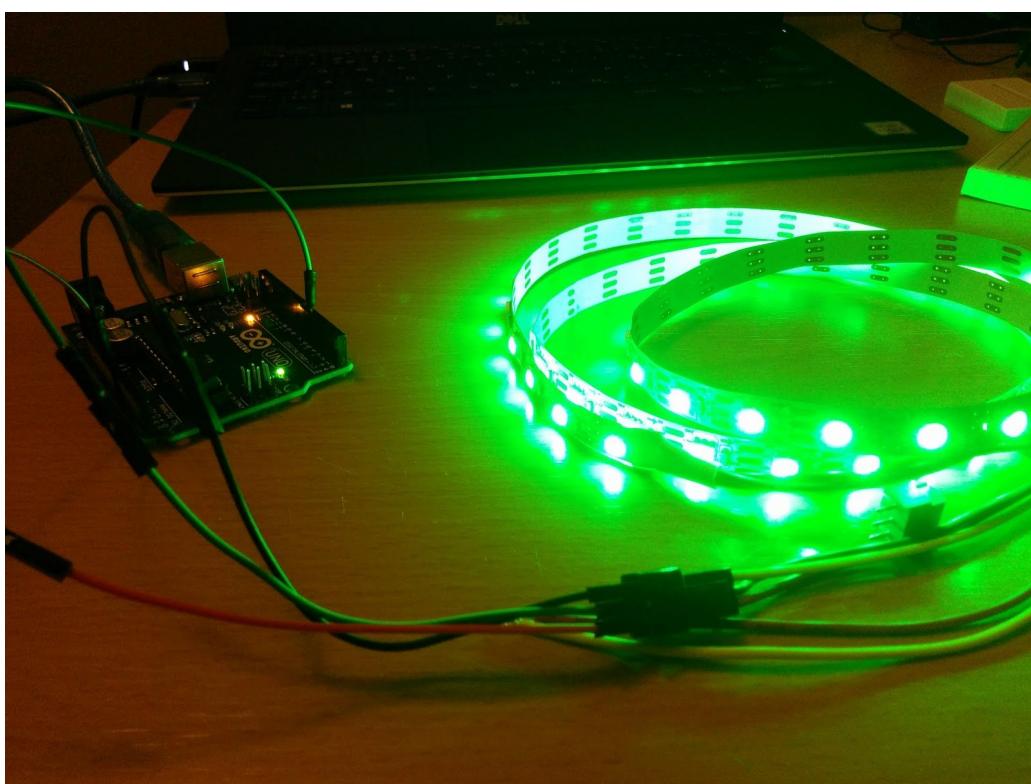
After long research of possible translucent spheres in multiple stores, I came to realize that it will have to be a lamp component :

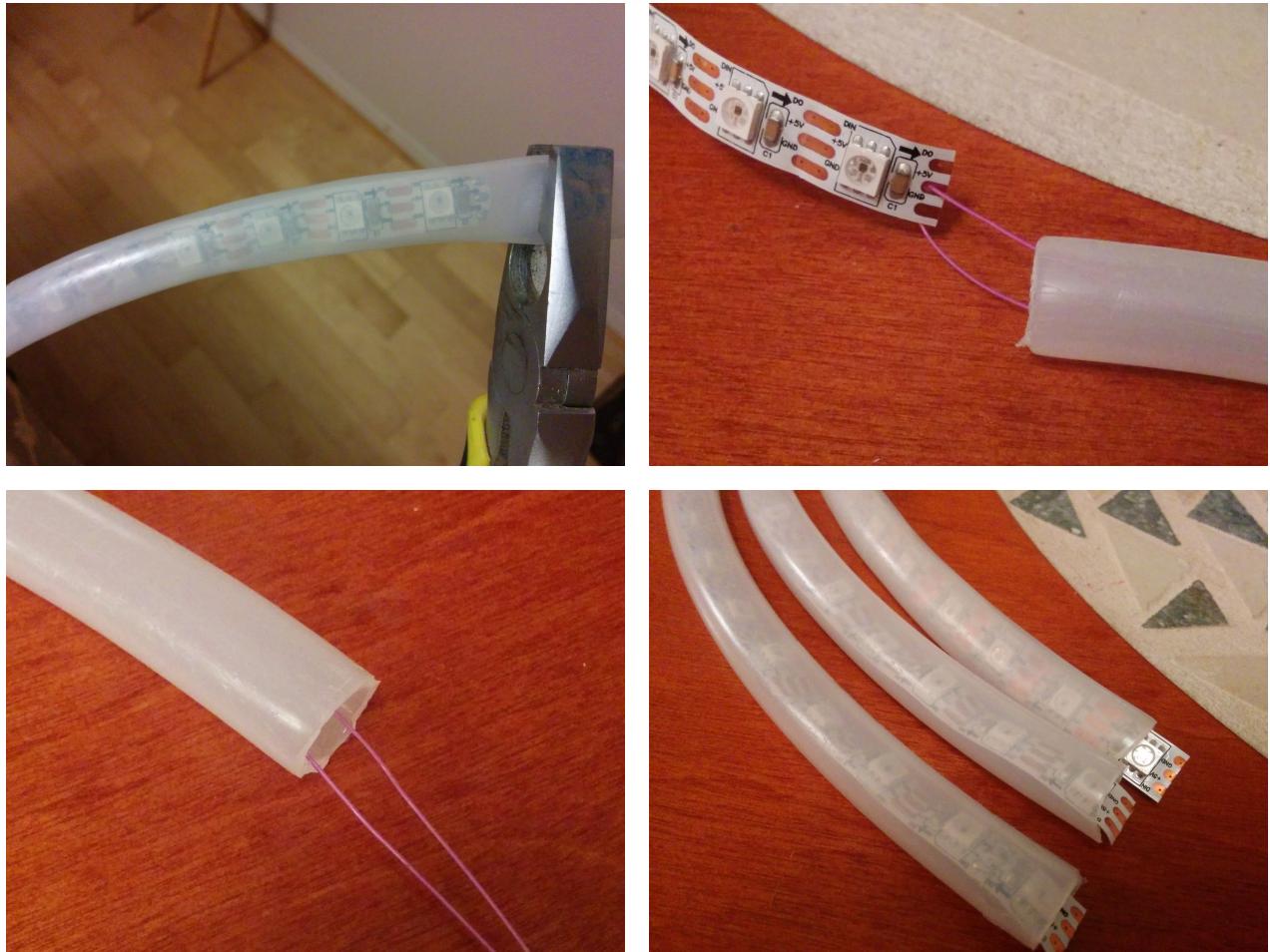


Finally, I found these which suited my needs :



Stems





That was a long and tedious task.

Pot + Stems

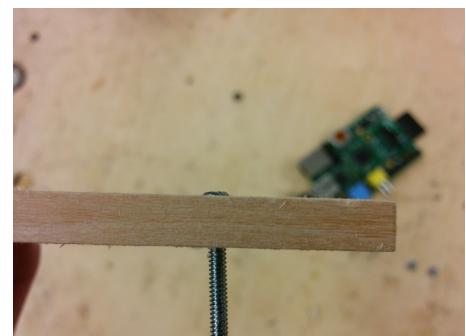
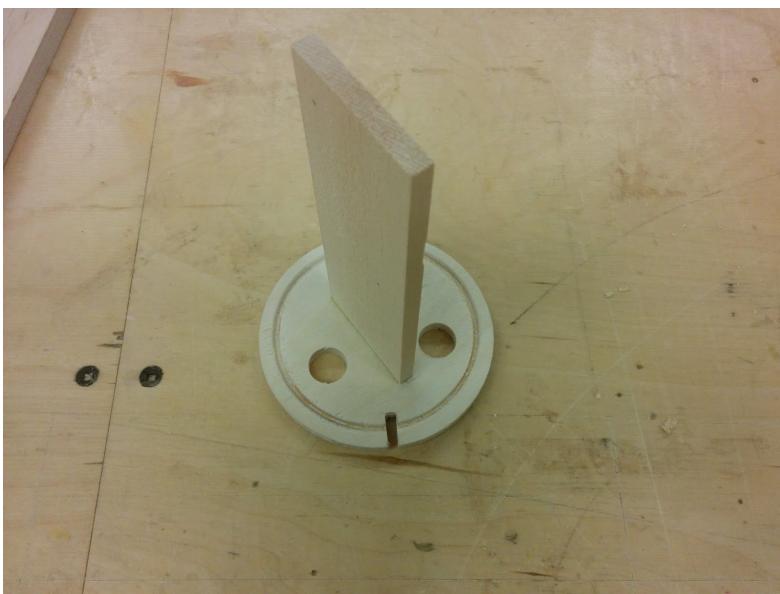
It was hard to tell but I prefered the translucid ones due to their uniformity :

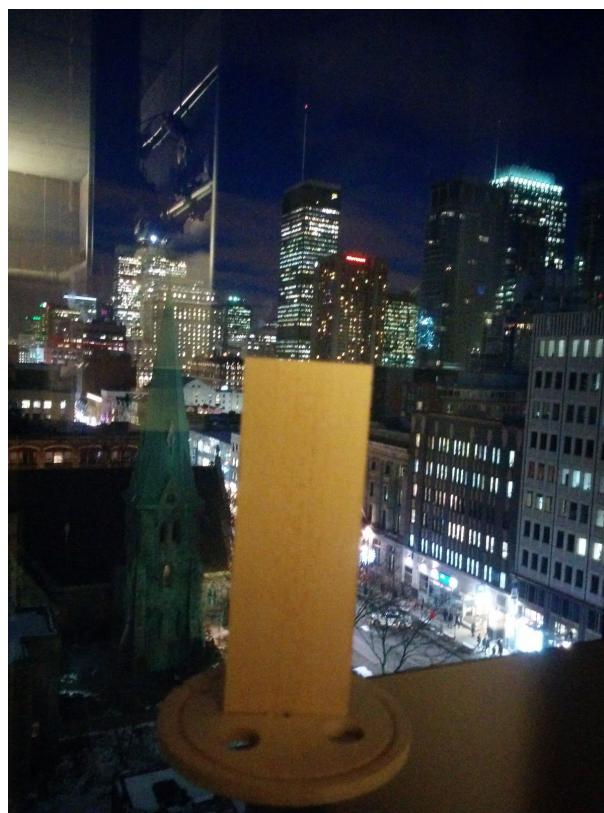




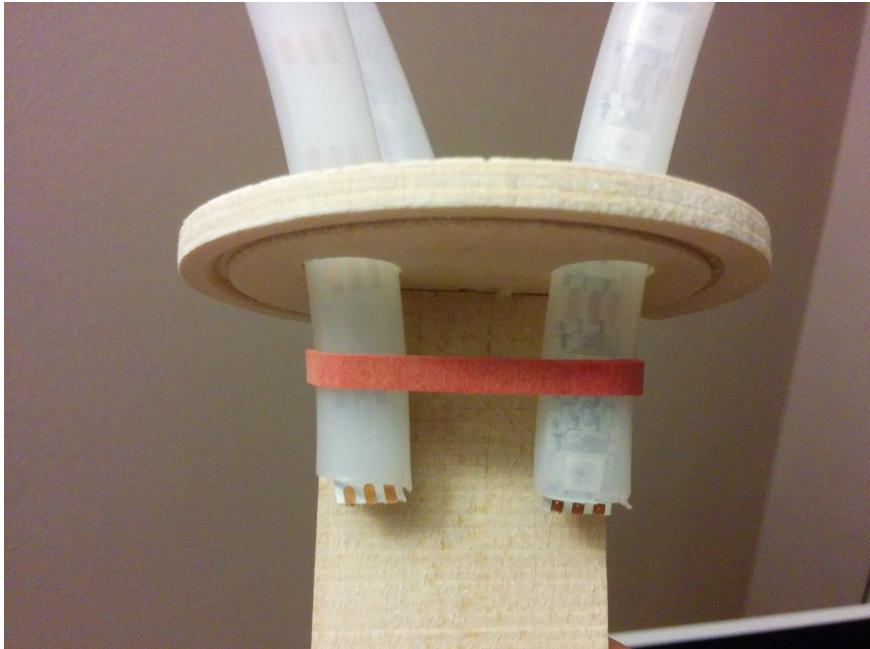
Wood structure

I settled for Concordia's Woodshop adventures to build a custom support for the hardware:





Stems + Wood Structure

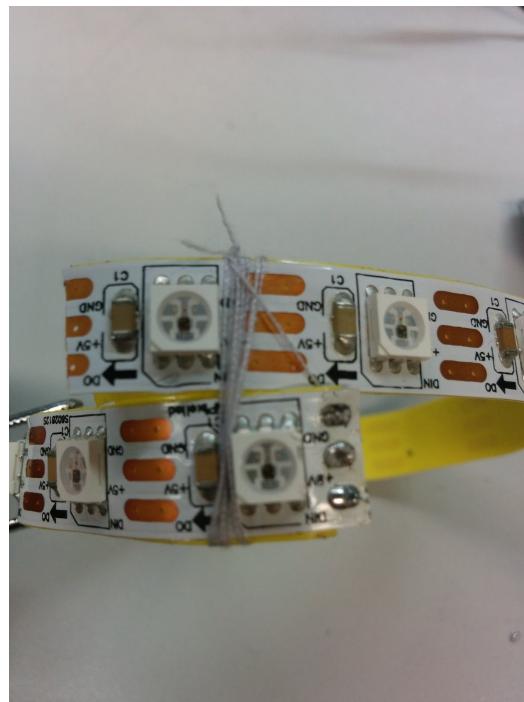
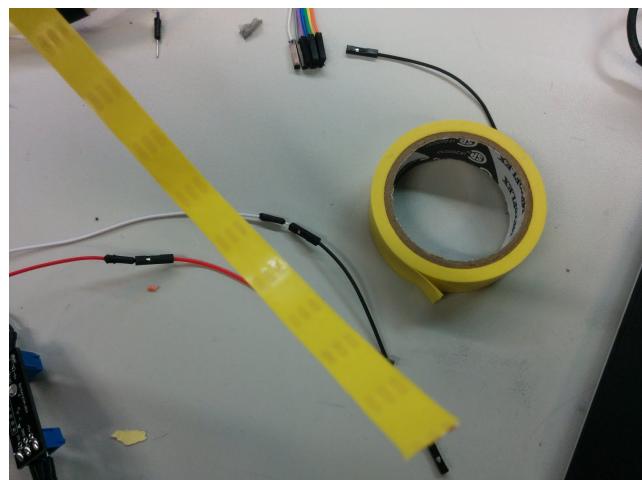
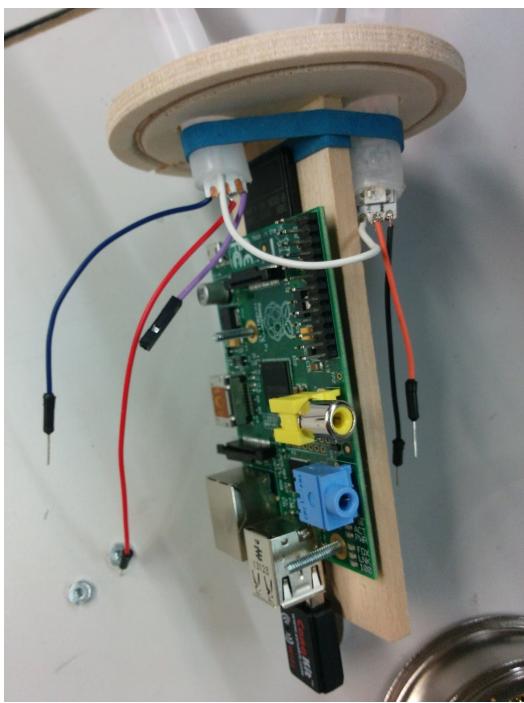


Hardware

The screenshot shows the Adafruit website with a search bar and navigation links for SHOP, BLOG, LEARN, FORUMS, and VIDEOS. A search bar and a 'Sign In' button are also present. The main content is a project titled 'NeoPixels on Raspberry Pi' by Tony DiCola. It features a thumbnail of a Raspberry Pi connected to a NeoPixel strip, a video thumbnail titled 'NeoPixels on Raspberry Pi', and two product cards for Raspberry Pi Model B+ and Model B with 512MB RAM, each with an 'Add To Cart' button.

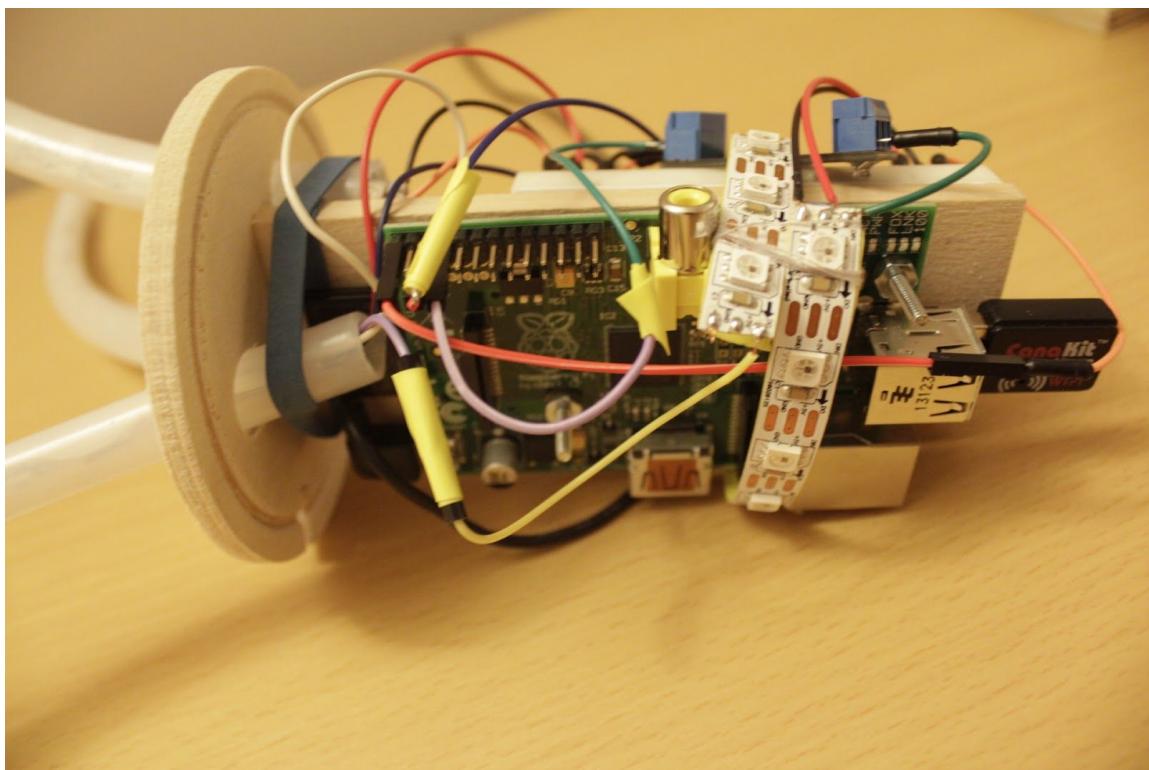
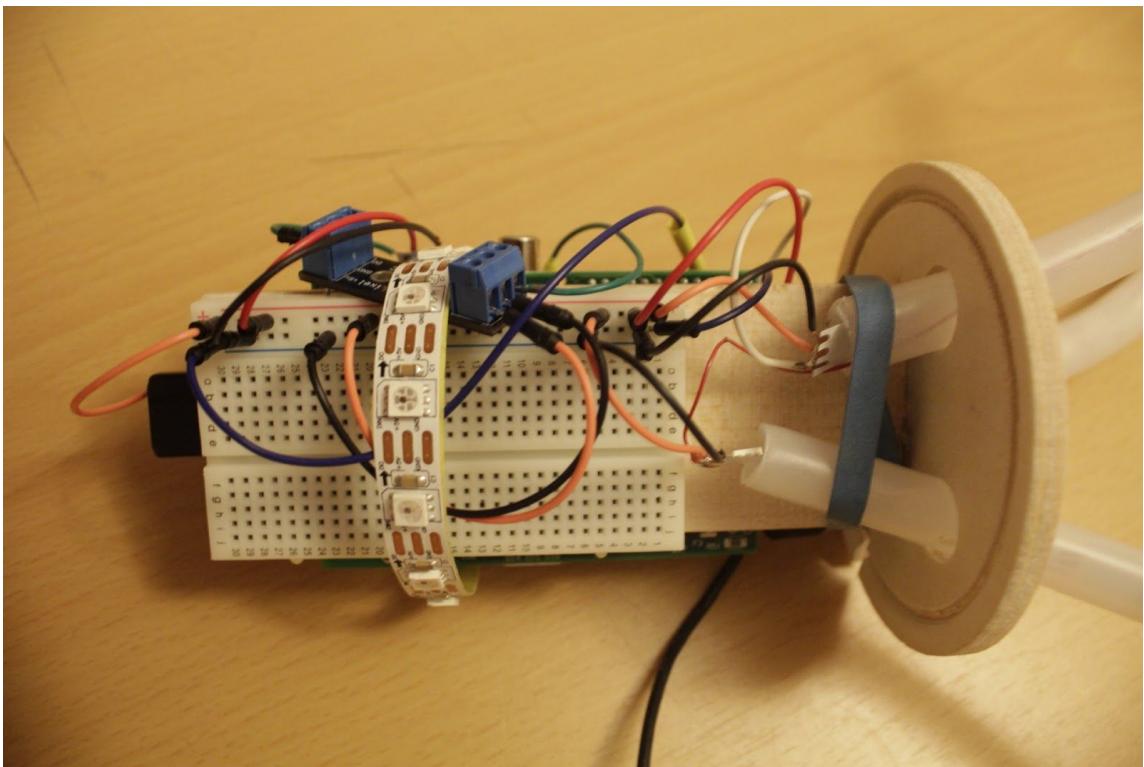
I used a Raspberry Pi due to intense network tasks. This Neowpixel library wasn't precise enough so I used SPLixel from Spekenzielabs to address all of the Neopixel strip in UART serial



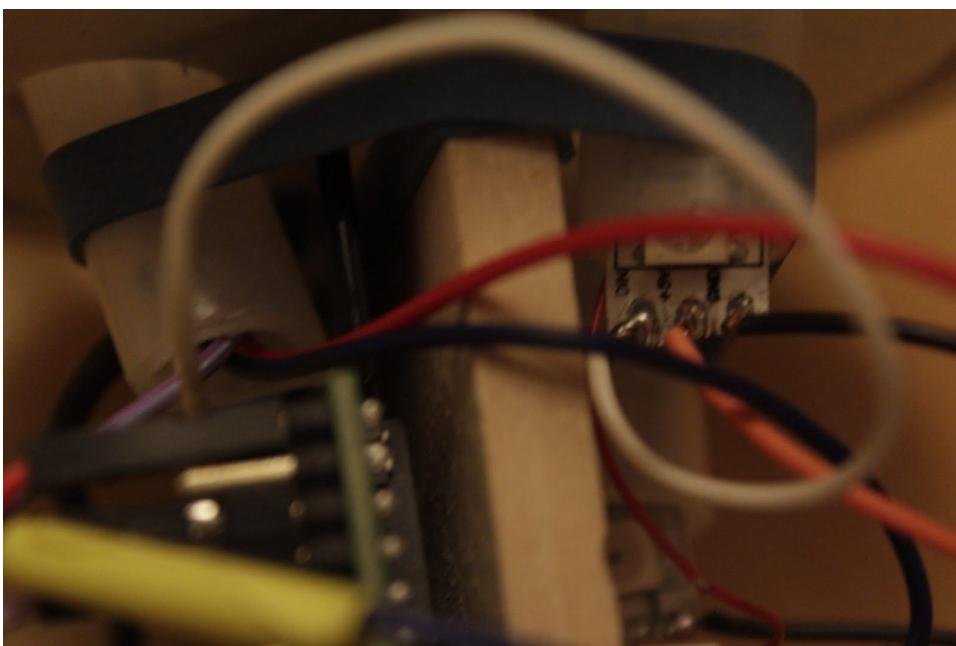
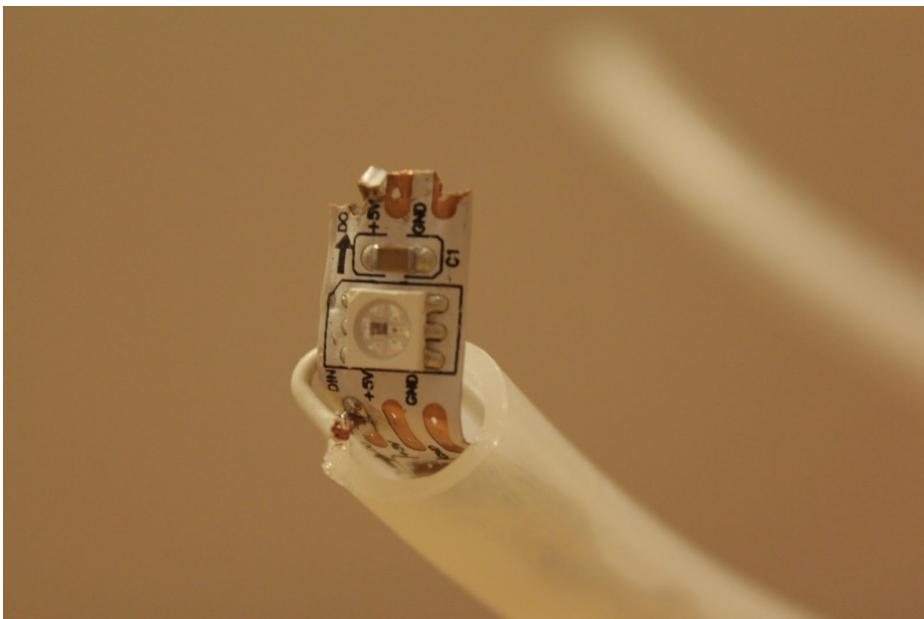


All of the Neopixel LED strips have DIN (data in), DOUT, 5V and GND lines. The goal is to power all of the LED strips from Raspberry Pi 5V and then interconnect their DIN to DOUT between the strips to address them individually using the serial commands. The SPLixel is a microcontroller allowing you to remove all Raspberry Pi interference due to internal tasks and to address each LED individually by sending 4 bytes according to its [datasheet](#).

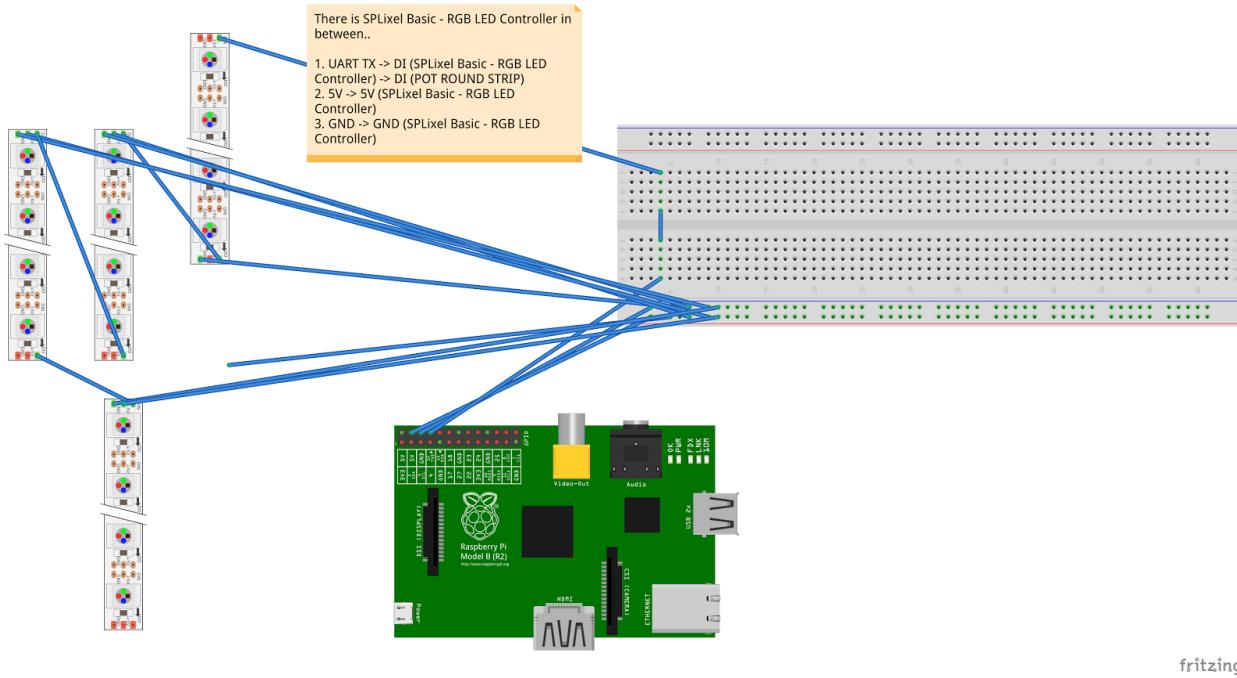
Here is the circuit layout of the HackerPot :



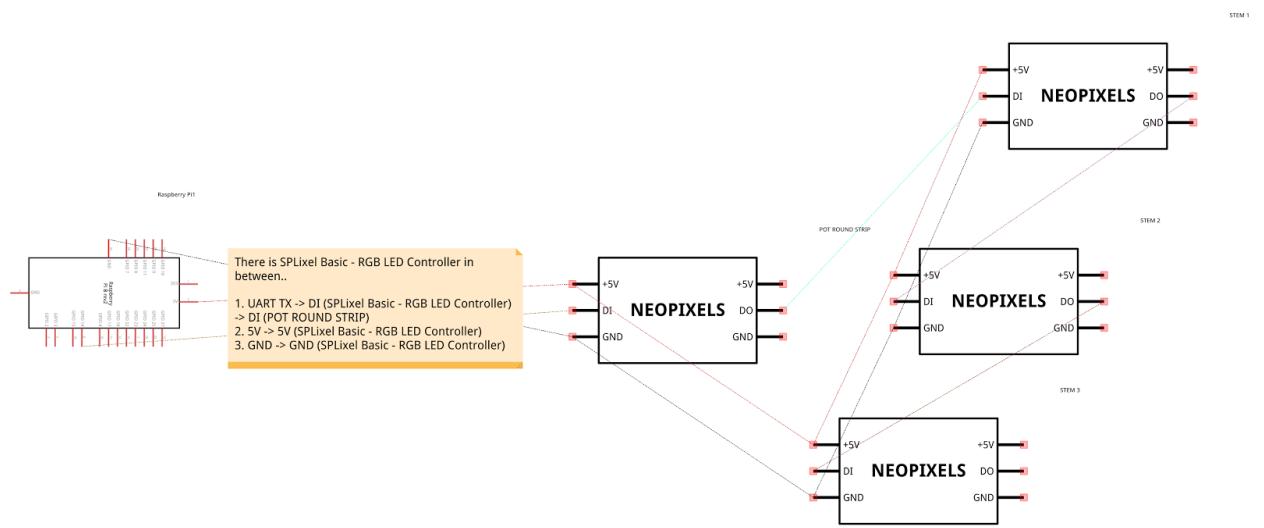
For DOUT (data out) I dropped a wired from the top of the step to the DIN at the bottom :



Circuit



fritzing



fritzing

Virtual

I had some troubles at finding my device in University. When I connected it to the network. I had no idea of its IP address and scanning the network was blocking me after a while. Plus, when I did a loop on all subnet to SSH on every IP, I did hit myself HoneyPots which were keeping the connection alive without any further response...

I found a way to find it by using one scan results of “nmap -sn <ips>” with the Raspberry Pi connected to the network and one another scan after disconnecting it. Then, I did an “sdiff” on both results and looked for a difference :

```
Nmap scan report for cslab-pluto.concordia.ca (10.115.140.156)      Nmap scan report for cslab-pluto.concordia.ca (10.115.140.156
Host is up (0.12s latency).          | Host is up (0.091s latency).
Nmap scan report for 10.115.140.171 | Host is up (0.028s latency).
Host is up (0.16s latency).          | Host is up (0.10s latency).
Nmap scan report for fa-ev9701-fib03.concordia.ca (10.115.140)        Nmap scan report for fa-ev9701-fib03.concordia.ca (10.115.140
Host is up (0.17s latency).          | Host is up (0.045s latency).
Nmap scan report for fa-ev9701-fib02.concordia.ca (10.115.140)        Nmap scan report for fa-ev9701-fib02.concordia.ca (10.115.140
Host is up (0.17s latency).          | Host is up (0.070s latency).
Nmap scan report for 10.115.140.204 | Host is up (0.070s latency).
Host is up (0.088s latency).          |
Nmap scan report for 10.115.140.215 | Host is up (0.070s latency).
Host is up (0.0082s latency).          <
Nmap scan report for cslab-neptune.concordia.ca (10.115.140.2)       Nmap scan report for cslab-neptune.concordia.ca (10.115.140.2
Host is up (0.11s latency).          | Host is up (0.076s latency).
Nmap scan report for fa-ev9417-pvise.concordia.ca (10.115.140)        Nmap scan report for fa-ev9417-pvise.concordia.ca (10.115.140
Host is up (0.019s latency).          | Host is up (0.12s latency).
Nmap scan report for prinstyluspro9900-ev9418.concordia.ca (1        Nmap scan report for prinstyluspro9900-ev9418.concordia.ca (1
Host is up (0.032s latency).          | Host is up (0.13s latency).
Nmap scan report for fa-rchail.concordia.ca (10.115.140.230)         Nmap scan report for fa-rchail.concordia.ca (10.115.140.230)
Host is up (0.12s latency).          | Host is up (0.12s latency).
Nmap scan report for cadx-ev8715.concordia.ca (10.115.140.231)       Nmap scan report for cadx-ev8715.concordia.ca (10.115.140.231
Host is up (0.12s latency).          | Host is up (0.12s latency).
Nmap scan report for 10.115.140.233 | Host is up (0.040s latency).
Host is up (0.075s latency).          | Host is up (0.040s latency).
Nmap scan report for fa-ev9418-prnt4.concordia.ca (10.115.140)        Nmap scan report for fa-ev9418-prnt4.concordia.ca (10.115.140
Host is up (0.049s latency).          | Host is up (0.13s latency).
```

At first, I thought of going with MHN (Modern Honeypot Network) to create this Honeypot for trapping the targets. However, turns out you need to virtualize them to allow a more high level interaction. I decided to install virtualbox as recommended :

```
pi@raspberrypi:~/Desktop $ sudo apt-get install virtualbox
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package virtualbox is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Package 'virtualbox' has no installation candidate
pi@raspberrypi:~/Desktop $ git clone https://github.com/threatstream/mhn.git
Cloning into 'mhn'...
remote: Counting objects: 6219, done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 6219 (delta 9), reused 0 (delta 0), pack-reused 6202
Receiving objects: 100% (6219/6219), 3.45 MiB | 721.00 KiB/s, done.
Resolving deltas: 100% (3180/3180), done.
Checking connectivity... done.
pi@raspberrypi:~/Desktop $ cd mhn/
pi@raspberrypi:~/Desktop/mhn $ ls
flags-LICENSE.txt install.sh LICENSE README.md scripts server Vagrantfile Vagrantfile.multiple-platforms
pi@raspberrypi:~/Desktop/mhn $ vagrant up
The provider 'VirtualBox' that was requested to back the machine
'server' is reporting that it isn't usable on this system. The
reason is shown below:

Vagrant could not detect VirtualBox! Make sure VirtualBox is properly installed.
Vagrant uses the 'VBoxManage' binary that ships with VirtualBox, and requires
it has to be available on the PATH. If VirtualBox is installed, please find the
'VBoxManage' binary and add it to the PATH environmental variable.
pi@raspberrypi:~/Desktop/mhn $ do
do domainname done dosfsck dosfslabel dotlockfile
pi@raspberrypi:~/Desktop/mhn $ sudo apt-get install docker
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

To discover that you can't due to Raspberry Pi limited capabilities (at least not on Raspbian).

Then, I started exploring docker but it needs a config file :

```
pi@raspberrypi:~/Desktop/mhn $ vagrant up --provider=docker
Bringing machine 'server' up with 'docker' provider...
Bringing machine 'honeypot' up with 'docker' provider...
==> honeypot: An error occurred. The error will be shown after all tasks complete.
==> server: An error occurred. The error will be shown after all tasks complete.
An error occurred while executing multiple actions in parallel.
Any errors that occurred are shown below.

An error occurred while executing the action on the 'server'
machine. Please handle this error then try again:

There are errors in the configuration of this machine. Please fix
the following errors and try again:

docker provider:
* One of "build_dir" or "image" must be set

An error occurred while executing the action on the 'honeypot'
machine. Please handle this error then try again:

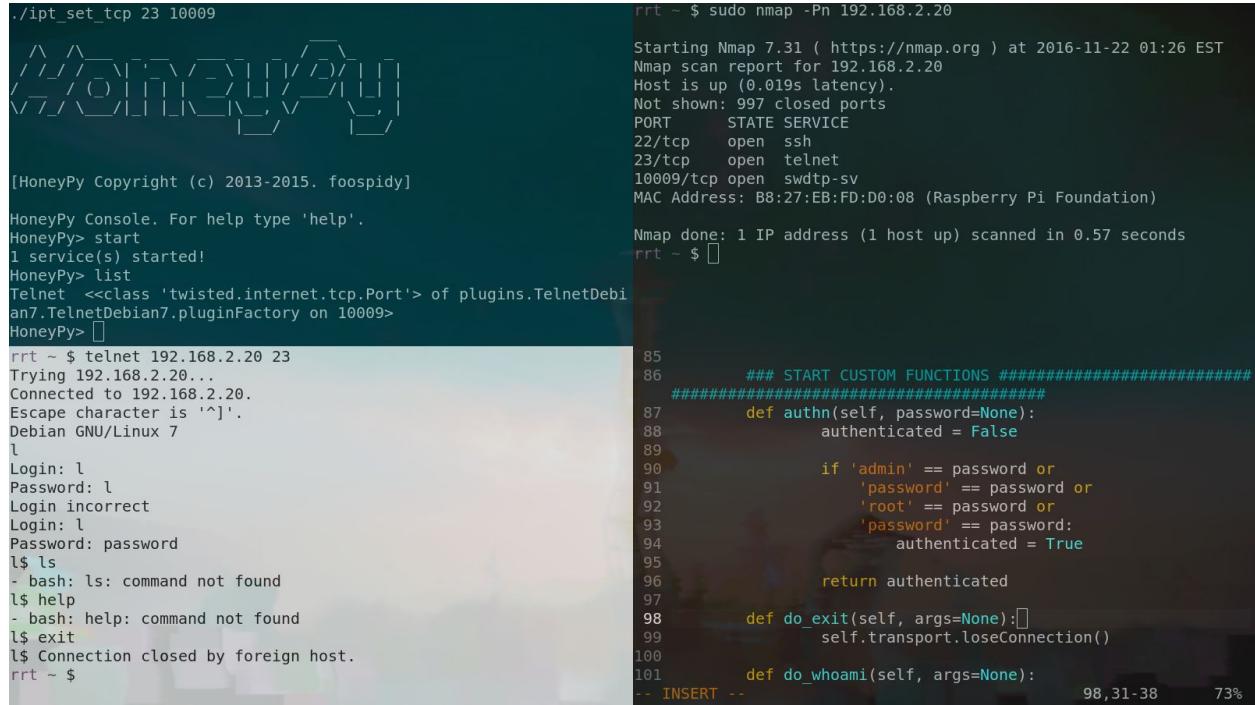
There are errors in the configuration of this machine. Please fix
the following errors and try again:

docker provider:
* One of "build_dir" or "image" must be set

pi@raspberrypi:~/Desktop/mhn $
```

I found one in their repositories but this all brought me to search for something more customizable since I needed a very precise triggering of the attacks...

I saw previously a library in Python called Twisted that allowed to directly extend TCP / UDP to create the desired protocols. This lead me to discover HoneyPy which is build on top of it. I used it with a combination of its Telnet plugin that I modified:



```

./ipt_set_tcp 23 10009
[ HoneyPy Copyright (c) 2013-2015. foospidy]
HoneyPy Console. For help type 'help'.
HoneyPy> start
1 service(s) started!
HoneyPy> list
Telnet  <<class 'twisted.internet.tcp.Port'> of plugins.TelnetDebian7.TelnetDebian7.pluginFactory on 10009>
HoneyPy> 

rrt ~ $ sudo nmap -Pn 192.168.2.20
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-22 01:26 EST
Nmap scan report for 192.168.2.20
Host is up (0.019s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
10009/tcp open  swntp-sv
MAC Address: B8:27:EB:FD:D0:08 (Raspberry Pi Foundation)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
rrt ~ $ 

85
86      ##### START CUSTOM FUNCTIONS #####
87      ##### #####
88      def authn(self, password=None):
89          authenticated = False
90
91          if 'admin' == password or
92              'password' == password or
93              'root' == password or
94              'password' == password:
95              authenticated = True
96
97          return authenticated
98
99      def do_exit(self, args=None):[]
100          self.transport.loseConnection()
101
102      def do_whoami(self, args=None):
-- INSERT --
98,31-38   73%

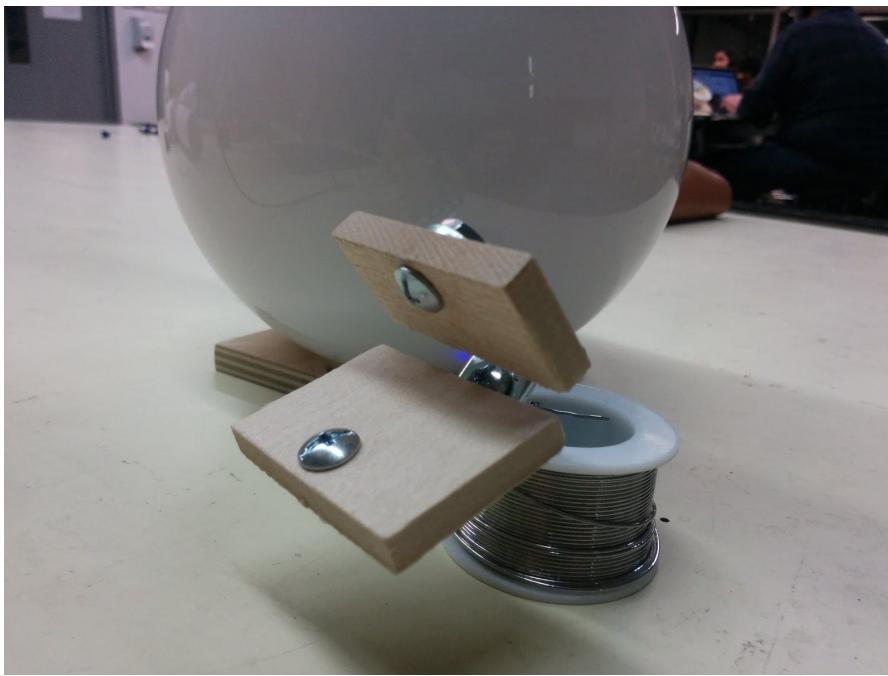
```

Flowers

I started by looking in the hardware store for Venus Flytrap alike shapes :



I tried to build some myself but I wasn't satisfied with the result :



Then, I found these which fitted the structure perfectly :



From there I put everything together as seen in prototype videos!