

Spy Cam *Installation* *Manual*

for the Raspberry Pi and Raspberry Pi Zero W

Topic: Installation



Table of Contents

Overview	3
Document Scope	3
Features	3
Terminology.....	4
Prerequisites	5
Required Hardware	5
Required Software	6
Required Security	8
Helpful Links to get you started.....	8
Pre-Installation.....	9
PROCEDURE 0: Load any Debian based operating system onto the Micro SD Card.	9
PROCEDURE 1: Update the Raspberry Pi Operating System	10
PROCEDURE 2: Option 1: Download the SpyCam solution from GitHub onto your laptop or host computer.	11
PROCEDURE 2: Option 2: Download the SpyCam solution from GitHub onto the RPi	12
PROCEDURE 3: (Optional but recommended) Update the configuration file to personalize your installation.	13
Installation.....	18
PROCEDURE 1: Run install.sh	18
PROCEDURE 2: Stubbed for now.....	20
PROCEDURE 3: Stubbed for now.....	21
Appendix A: Supplementary Instructions	22
PROCEDURE: Format the USB Storage using Linux and Fdisk.....	22

Overview

Document Scope

This document is written to instruct the user with basic Raspberry Pi knowledge on how to build a motion-activated security camera on the Raspberry Pi using the packaged tar file named, *spycam_scripts.tar*. The actual camera to be installed comes from <https://elinux.org/RPi-Cam-Web-Interface>. This was chosen over the well written and popular MOTIONEYES (https://github.com/ccrisan/motioneyes/wiki) as MOTIONEYES is bare metal RPi image and does not provide the needed functionality to automate the IOT features of this solution. If you are a NOOB or new to the Raspberry Pi or if all you are after is a working camera, then I suggest you try MOTIONEYES first and play around with it.

The installation guide applies to both the Raspberry Pi 3B and the Raspberry Pi Zero W. This solution assumes the RPi will use the SpyCam over a wireless connection, or wifi to connect to your router. Initial set up for the Raspberry Pi 3B can be over Ethernet. This solution is constructed to allow a headless installation, provided you follow the instructions on how to set up the configuration file before you boot up the RPi. See *PROCEDURE 3* under the *Pre-Installation* section.

General RPi setup is not explicitly covered in this document, but uses hyperlinks to refer you to vendor downloads and instructions on how to choose and load the operating system onto a Micro SD card. This solution was built on a PI Zero W using Raspbian Stretch as the base Operating System (see <https://www.raspberrypi.org/downloads/raspbian/>).

Features

Features Overview

- Easy installation. One script does all the work. One configuration file contains all the various settings found in the installed software configuration files. Personalize your setup in a single configuration file and have it update the other configuration files.
- Built in motion detection can send you emails and video attachment of intruder when the motion detection is triggered.
- Installs proven software from credible vendors. This solution installs the RPi Cam as taken from <https://elinux.org/RPi-Cam-Web-Interface>. It also updates V4L2 binaries and takes care of loading and installing any dependencies.
- Optional IOT baked in. SpyCam turns off when it detects your presence. Turns back on when you leave.
- Optional External USB storage is automatically formatted, mounted and used to hold your historical videos captured by SpyCam.
- Local Video Storage manages its own capacity and grooms off the oldest video when local space starts to fill up the SD card.

Features Details

1. One stop installation. Scripts pull down source(s)¹ and installs the needed binaries. The install script uses a configuration file, found in `./scripts/boot/swat.config` to instruct the `install.sh` what settings to use for your personal setup. After `install.sh` has run, the configuration file, `swat.config` is moved to the `/boot` directory of the RPi image, where you can load the SD into your laptop and change the `swat.config` using your laptop as the contents of `/boot` are readable and updatable.

¹ <http://git.linuxtv.org/v4l-utils.git>
https://github.com/silvanmelchior/RPi_Cam_Web_Interface.git

2. Built in motion detection can send you emails and video attachment of intruder when the motion detection is triggered. The motion detection continues to capture new video as long as there is motion detected. In order to keep from filling up your email and risk getting you banned as a bot², only the first video captured is sent to you, alerting you to intrusion. You will continue to receive new video emails once a minute until motion is no longer detected.
3. Optional IOT intelligence baked in. Camera turns off in your presence. Camera turns back on when you leave. You can choose to use your Cell Phone as a beacon, or use a Bluetooth iBeacon to talk to your RPi SpyCam announcing your presence. The configuration file has an entry for the cell phone IP and Bluetooth addresses. If you fill this in, the SPYCAM will turn off the camera when it detects the Cell Phone. The Cell Phone IP is scraped from the Wireless router; the Bluetooth search is simply looking for the Bluetooth address listed in the configuration file.
4. Formats and mounts a USB for secondary storage, providing you attach an empty USB to the RPi before running the install.sh script. The install solution wipes the USB and creates a VFAT mount to /media/cam, PROVIDING THIS IS THE ONLY USB PLUGGED INTO THE RPi when you run install.sh. In technical terms, the install process is looking for /dev/sda as the external storage to format and mount.
5. Self-maintaining storage. The videos are captured in /var/www/cam/media. If you start to fill up this directory, a cron job (a scheduled job running as root) will groom off the oldest video once an hour until appropriate available storage on /var is obtained. If you inserted a USB drive to the RPi before running the install.sh, then there should be a mounted drive where the videos are automatically copied from /var/www/cam/media/ to /media/cam/media.
6. Headless maintenance baked in. Once you have installed the spycam, there are two options for headless maintenance. You are always free to make changes as you see fit:
 - a. Reminder, you can change the /boot/swat.config file in your laptop, as it is readable from the SD card. To make your changes effective will require 2 reboots, 1 to update the changes and the other to make the changes take effect.
 - b. From the RPi itself, You can change the following by simply making the change to /boot/swat.config, run the command: `sudo systemctl start wat.service` and rebooting.
 - c. Here are the settings, which are explained in the terminology paragraph, you can change in wat.config:
 - i. `export MY_ROUTER_NAME="DEA_Surveillance"`
 - ii. `export MY_ROUTER_PW="NoDrugs4U"`
 - iii. `export MY_ROUTER_IP="192.168.1.1"`
 - iv. `export MY_SERVER_WIFI_IP="192.168.1.184"`
 - v. `export MY_SERVER_STATIC_IP="192.168.1.194"`
 - vi. `export MY_EMAIL_MAIL_HUB="mailhub=dea.gov:587"`
 - vii. `export MY_EMAIL_ADDRESS="bucbowie@dea.gov"`
 - viii. `export MY_EMAIL_PW="tscgvjtgmylcaca"`

Terminology

1. Raspberry Pi, Rpi, RPi refer to either the Raspberry Pi 3B or the Raspberry Pi Zero W. The installation itself is agnostic, but there are hardware differences between models Raspberry Pi 3B and the Raspberry Pi Zero W. These differences will be stated, when the content applies only to the Raspberry Pi Zero W.
2. Connection is used as a networking term, to refer to whether you are connected to the internet using ethernet (eth0) or wireless (wifi) (wlan0). The Raspberry Pi Zero W, does NOT have an Ethernet adapter built in, so we assume all connectivity on the Pi Zero W will be wifi.
3. eth0 is the generic term for the Ethernet connection. Your set up may have the Ethernet adapter using a different alias other than, eth0. From the command line, you can run, `ifconfig`, to list the networking information, including the Ethernet and Wireless aliases, such as eth0 and wlan0.

² bot - so many emails in such a short time that the email provider thinks you are remote computer sending spam

4. wlan0 applies to the generic term for the wireless connection. See terminology item 3 for addition info.
5. Configuration File Terms:
 - a. SWAT.CONFIG ROUTER INFO
 - i. MY_ROUTER_NAME is the SSID of your wireless router.
 - ii. MY_ROUTER_PW is the PSK or password to connect to your wireless router.
 - iii. MY_ROUTER_IP is the I.P. address of your wireless router. As most home wireless routes use the wireless router for a DSN server (assigns IP to connecting computers), the suffix of the IP address is generally 1 – as in 192.168.1.1.
 - b. SWAT.CONFIG Raspberry Pi INFO
 - i. MY_SERVER_WIFI_IP is the desired wireless IP of your RPi running the SpyCam. It generally refers to the /etc/dhcpd.conf entry: wlan0.
 - ii. MY_SERVER_STATIC_IP is the ethernet or wired (has a network cable plugged into the network jack) address you wish to use for the RPi running the SpyCam. The process to change the MY_SERVER_STATIC_IP will only work if you are physically using an ethernet connection at the time you are making changes to /boot/swat.config.
 - c. SWAT.CONFIG IOT INFO
 - i. CELL_STATIC_IP is the IP of your Cell Phone. Generally this found on the Cell phone under “About” or “Network”. We are looking for an IP Address in the format aaa.bbb.ccc.ddd, where there are 4 numbers separated by 3 periods.
 - ii. CELL_WIFI_MAC_ADDRESS is the MAC address is the MAC address of your Cell Phone wireless network card. Generally found in the same place as the Cell Phone IP. See CELL_STATIC_IP line item above this line.
 - iii. CELL_BLUETOOTH_ADDRESS is the Bluetooth address being broadcast by either your Cell Phone or a separate iBeacon.
 - d. Option SWAT.CONFIG Email INFO
 - i. MY_EMAIL_MAIL_HUB is the email provider you have an account with which allows one to send emails from a remote server, such as the RPi SpyCam, providing you also specify your email credentials. A GMAIL example is smtp.gmail.com:587.
 - ii. MY_EMAIL_ADDRESS is the email address you want your motion detection alerts to go to.
 - iii. MY_EMAIL_PW is the password for your email account you are using to send videos.

Prerequisites

Required Hardware

Hardware	Purpose	Description
Micro SD Card	Any Micro SD card with at least 8 GB of space. We prefer the class 10 over the class 1 or 4. The higher end (more expensive) Micro SD cards are faster and last longer. A fine example of the higher end SD card is, Sony 32GB High Speed Class 10 UHS-1 Micro SDHC up to 95MB/s Memory Card (SR32UXA/TQ) . In addition to looking for class “10”, review the transfer speed of the card. The faster the transfer speed, the better performance (up to a point of matching the USB 2 transfer rate.)	Will hold all the software for the Raspberry Pi. This holds the software to boot up, and will hold the scripts we are going to install on the RPi.
Raspberry Pi	The computer or server that we are installing the SpyCam software and scripts.	Can be either the Raspberry PI 3B or the Raspberry Pi Zero W.
Raspberry Pi Camera	Detect motion and collect video.	Comes in 2 flavors, the standard camera and the Pi NOIR, which can detect and

		capture InfraRed images. The standard camera has a clearer picture display for daylight or well lit areas, over the Pi NOIR. The Pi NOIR camera can capture InfraRed images if there is InfraRed light available. If not, the the PI NOIR offers no advantage over the standard camera for general use.
5 volt Micro USB Power adapter.	Plugs into wall and powers the Rpi.	We suggest a 5volt, 2.4 amp power source. The Raspberry Pi Zero W can run on 5volt, 1 amp power, but the camera and optional USB attached storage will put a higher load or demand on the Raspberry Pi Zero W.
Optional HDMI monitor	To display the computer's output.	
Optional USB based Keyboard and Mouse	Allow user to directly interact and make changes to the RPi.	Assuming the reader knows what a keyboard and mouse are, we point out the Raspberry Pi Zero W has only 1 micro USB adapter, so we suggest a Bluetooth Keyboard and mouse combo, which will require an Micro USB to USB Female adapter.
Optional HDMI cable.	Connects the RPi to the Monitor or "Screen". The Raspberry Pi Zero W requires the Optional Micro HDMI to Female HDMI adapter listed below.	The Raspberry Pi 3B uses the standard HDMI connection size. The Raspberry Pi Zero W has a Micro HDMI adapter and requires an additional adapter listed below to connect the Raspberry Pi Zero to the HDMI cable itself.
Optional USB Storage	<ol style="list-style-type: none"> 1. To offload the video captured and written locally on the Micro SD card. 2. Allow user to remove the USB storage and view the videos on a different computer. 	Any USB 2 or 3 storage device. The Raspberry Pi Zero W will require a Micro USB to USB Female adapter, as ALL the adapters on the Raspberry Pi Zero W are micro models.
Optional (Pi Zero W ONLY) Micro HDMI to Female HDMI adapter	Attaches to the Raspberry Pi Zero W in the Micro HDMI jack and provides a regular size HDMI jack.	

Required Software

Topic	Software	Purpose
Raspberry Pi	The base Operating System	Any Debian distribution for the Raspberry Pi . Our solution used Raspbian, version, Stretch. This can be found at the Raspberry Pi download page. See: https://www.raspberrypi.org/downloads/raspbian/
Internet	GitHub.com access to download scripts.tar	SpyCam installation package, which includes the installation PDF.
SD Formatter	Download link: https://www.sdcard.org/downloads/formatter_4/	Initialize or wipe clean the Micro SD card. Here is the online doc: https://www.sdcard.org/consumers/pdf/2017SDA_brochure_eng.pdf

Win32 Disk Imager	Download link: https://sourceforge.net/projects/win32diskimager/	Flashes or writes software onto the Micro SD card. Read more about it here: https://www.raspberrypi.org/documentation/installation/installing-images/windows.md
FileZilla or a File Transfer program using SCP or SFTP.	Download link: https://filezilla-project.org/download.php?show_all=1	Allows file transfer from Laptop or one computer to the Raspberry Pi. Used to copy the downloaded GitHub SpyCam download and loaded onto the Raspberry Pi.

Required Security

Hardware	Needed	Purpose
Wireless Router	Credentials: 1. The SSID or WiFi Router name. 2. The Wifi password or PSK.	The SpyCam must connect to the internet using a wireless connection, if the SpyCam is to email the user when motion is detected. The SpyCam runs without internet connectivity. The difference is simply the ability to notify the user of motion as it happens.
Mail server	Credentials to a mail server. Can be smtp.gmail.com or smtp.mail.yahoo.com. This requires a username and some sort of password or authentication token.	Send real time notification of motion, with video attached to the email.

This package will install a new user named, swat. It will be created as user=swat, password=swat. The swat user will be set up as a service account whose only function is to hold the automation scripts for the root user to run. There is no logging into your system as user swat; it is set up to be secure and only available/used by the system itself.

For the SpyCam itself, it is suggested you change the default password for the pi user. The two best known options for changing the pi user password are:

1. Change the default password for user pi from the command line.
2. Change the default password for user pi using the raspi-config tool.

Helpful Links to get you started

No point in reinventing the wheel, here is your Google link to search how to change the password for the pi user:

https://www.google.com/search?ei=HheVWpmAK6HZ5gL0jbewCg&q=raspberry+pi+change+password&og=raspberrypi+change+password&gs_l=psy-ab.3..0l2j0i22i30k1l5.17637.27543.0.27813.44.36.8.0.0.0.179.3099.25j10.35.0..3..0...1.1.64.psy-ab..1.43.3162...0i131k1j0i67k1j35i39k1j0i131i20i264k1j0i20i264k1j0i13k1j0i13i30k1j0i8i13i30k1j0i13i5i30k1j0i22i10i30k1.0.DE_KaDhezF8

For transferring files from your laptop or host computer to the Raspberry PI, you can GOOGLE that topic. Here is an example link:

<https://www.raspberrypi.org/documentation/remote-access/ssh/sftp.md>

For installing the Raspbian Operating System onto your Micro SD card, there are many helpful links Google will provide. Here is an example link:

Very Basic (NOOBS): <https://www.raspberrypi.org/documentation/installation/noobs.md>

Basic (using Raspbian): Format (wipe) the Micro SD card: <https://www.raspberrypi-spy.co.uk/2015/03/how-to-format-pi-sd-cards-using-sd-formatter/>

AND

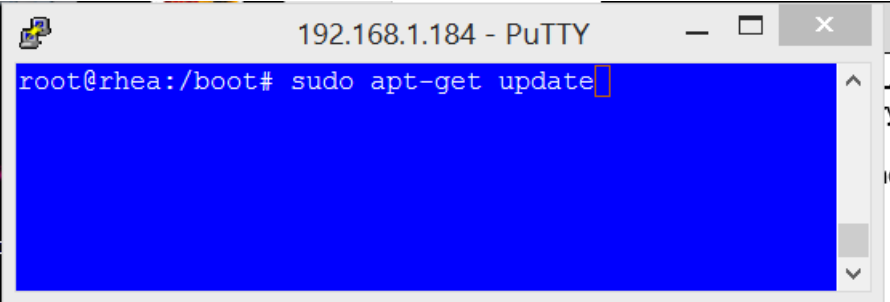
<https://www.raspberrypi.org/documentation/installation/installing-images/>

Pre-Installation

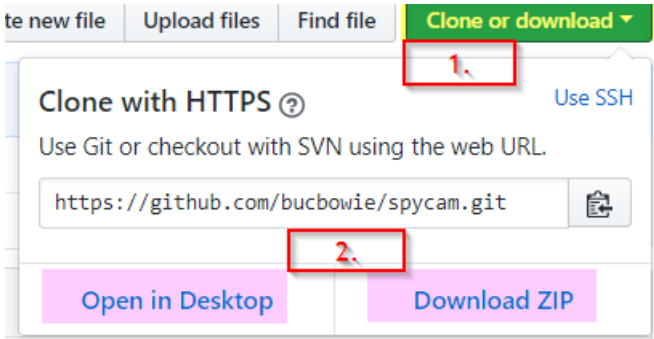
PROCEDURE 0: Load any Debian based operating system onto the Micro SD Card.

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: Load a Debian based operating system onto the Micro SD Card, intended for use by our Raspberry Pi.</p> <p>Plenty of fine information on this from the vendor and compliments of the Internet: https://www.raspberrypi.org/documentation/installation/installing-images/</p> <p>Expected Result: The Micro SD card should have the base operating system loaded onto it.</p>

PROCEDURE 1: Update the Raspberry Pi Operating System

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: Update the Raspberry Pi to have current binaries. The commands are run from the Raspberry Pi itself at the command line. There are 4 commands we suggest you run to update the Raspberry Pi to current patch level.</p> <p>Command: # sudo apt-get update</p> <p># sudo apt-get upgrade</p> <p># sudo apt-get dist-upgrade</p> <p># sudo rpi-update</p> <p>Expected Result: You should see something like this:</p> 
2.	<input type="checkbox"/>	End of section

PROCEDURE 2: Option 1: Download the SpyCam solution from GitHub onto your laptop or host computer.

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: Pull SpyCam solution from GitHub: https://github.com/bucbowie/spycam</p> <p>Command: Click on Clone or download and choose method to save file.</p> <p>Note, You can optionally open a Web Browser on the RPi and enter the address: https://github.com/bucbowie/spycam to pull the tar file onto the RPi itself, eliminating the need for Step 2.</p> <p>Here is the RPi command line command to pull the download:</p> <pre>wget https://github.com/bucbowie/spycam/archive/master.zip</pre> <p>Expected Result: You should see something like this: where 1. Is the button on the left hand side of the screen and 2. appears when you click the button. Use options listed in 2. to choose your download method.</p> 
2.	<input type="checkbox"/>	<p>Action: Copy the SpyCam download (spycam_scripts.tar) to the RPi.</p> <p>If you downloaded the spycam_scripts.tar on your laptop, then use the FileZilla or other file transfer tool to copy the tar file from YOUR computer to the RPi. We suggest you copy the spycam_scripts.tar file to the HOME (/home/username) of a user with SUDO privileges. You can use ROOT, but best practices advise against using ROOT user to install software.</p> <p>Referring the <i>Helpful Links</i> section of this document, here is an example of how to copy from your laptop or host computer to the Raspberry Pi: https://www.raspberrypi.org/documentation/remote-access/ssh/sftp.md.</p>

PROCEDURE 2: Option 2: Download the SpyCam solution from GitHub onto the RPi

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: Pull SpyCam solution from GitHub: https://github.com/bucbowie/spycam</p> <p>Command: <code>wget https://github.com/bucbowie/spycam/archive/master.zip</code></p> <p>Expected Result: You should see something like this:</p> <pre>pi@rhea:~ \$ ls -lart total 112 -rw-r--r-- 1 pi pi 675 Nov 28 20:22 .profile -rw-r--r-- 1 pi pi 220 Nov 28 20:22 .bash_logout -rw-r--r-- 1 pi pi 3523 Nov 28 20:22 .bashrc -rw-r--r-- 1 pi pi 12055 Mar 4 12:11 master.zip << This guy!</pre>
2.	<input type="checkbox"/>	<p>Action: Unzip master.zip.</p> <p>Command: <code># unzip master.zip</code></p> <p>Expected Result: You should see something like this:</p> <pre>pi@rhea:~ \$ unzip master.zip Archive: master.zip 71daa0a613b7b14d283ef89da7d25df6bdc2940a creating: spycam-master/ extracting: spycam-master/README.md inflating: spycam-master/spycam_scripts.tar</pre>
3.	<input type="checkbox"/>	<p>Action: Change into spycam-master directory and untar spycam_scripts.tar.</p> <p>Commands: <code># sudo cd spycam-master</code></p> <p><code># sudo tar -xvf ./spycam_scripts.tar</code></p> <p>Expected Result: You should see something like this:</p> <pre>pi@rhea:~/spycam-master \$ ls -lart total 104 drwxr-xr-x 2 jaskew sudo 4096 Feb 24 06:04 swat_install drwxr-xr-x 4 jaskew sudo 4096 Feb 25 11:27 scripts -rwxr-xr-x 1 jaskew sudo 8650 Feb 28 05:41 install.sh -rw-r--r-- 1 pi pi 71680 Feb 28 06:00 spycam_scripts.tar -rw-r--r-- 1 pi pi 9 Feb 28 06:00 README.md</pre>

PROCEDURE 3: (Optional but recommended) Update the configuration file to personalize your installation.

Dept. Research and Development	Raspberry Pi Projects	Author: J. Askew
Date: 2018-03-04	Subject: Spy Cam Installation	Draft-Version 1.1

Step	<input checked="" type="checkbox"/>	Action / Expected Result
------	-------------------------------------	--------------------------

1.	<input type="checkbox"/>	<p>Action: Review the spycam/scripts/boot/swat.conf file.</p> <p>Expected Result: You should see something like this:</p> <pre>##### # Server Hardware ##### export ETHERNET_DEVICE="eth0" # The Ethernet device type found in /etc/dhcpd.conf to override the Ethernet network of eth0. export WIFI_DEVICE="wlan0" # The wireless device type found in /etc/dhcpd.conf. to override the wireless network of wlan0. #-----# # The next 2 lines are for modifying the router # credentials. The settings are found in # /etc/wpa_supplicant/wpa_supplicant.conf. # If you do want to set these manually, simply # blank out the values in the next two lines, and # modify /etc/wpa_supplicant/wpa_supplicant.conf. # Example: # export MY_ROUTER_NAME="" # export MY_ROUTER_PW="" #-----# export MY_ROUTER_NAME="DEA_Surveillance" # The SSID of your router. export MY_ROUTER_PW="NoDrugs4U" # The PSK or password to your router. export MY_ROUTER_IP="172.16.1.1" # The IP of your router. #-----# # The next 2 lines are for STATIC IP. If you wish # to use DHCP and have the system set the server IP, # then blank them out. # These settings are found in /etc/dhcpd.conf. # You can modify the settings manually if you wish to # bypass this scripts modifying them. # Example: # export MY_SERVER_WIFI_IP="" # export MY_SERVER_STATIC_IP="" #-----# export MY_SERVER_WIFI_IP="172.16.1.184" # If you are using STATIC IP, this is the desired Wireless IP export MY_SERVER_STATIC_IP="172.16.1.194" # If you are using STATIC IP, this is the desired Ethernet IP export MY_CAMERA_NAME="Puppie_Cam_`echo \${MY_SERVER_WIFI_IP} cut -d"." -f4 sed 's/"/"/'`" #Unique Camera name ##### # Peripheral Hardware ##### # The next 3 settings are optional and used for the # optional IOT presence detection, where the # camera will turn off when your cell phone is # detected near by. Same goes for the BLUETOOTH # address, if you are using an iBeacon.</pre>
----	--------------------------	--

Step	✓	Action / Expected Result
	<input checked="" type="checkbox"/>	<pre> # If you do not wish to use the IOT automatic # # presence detection to turn off the camera, simply # # blank out the values for the next 3 lines. # # Example: # # export CELL_STATIC_IP="" # # export CELL_WIFI_MAC_ADDRESS="" # # export CELL_BLUETOOTH_ADDRESS="" # #-----# export CELL_STATIC_IP="172.16.1.182" # IP of your Cell Phone. Optional setting, but used for IOT. export CELL_WIFI_MAC_ADDRESS="80:01:86:74:18:d6" # MAC Address of your Cell Phone Wireless Network Card. export CELL_BLUETOOTH_ADDRESS="04:C2:3D:AE:42:7E" # Bluetooth address of your phone or any iBeacon you wish to use. ##### # Script control # ##### export MY_EMAIL_MAIL_HUB="smtp.dea.gov:587" # The MAIL service to send email. Known as the Mail HUB. export MY_EMAIL_ADDRESS="bucbowie@dea.gov" # Your email ID for the mail service. export MY_EMAIL_PW="tscggvjlgmzlcaca" # Your email password or authentication token. export CAMERA_CNT_WIFI_ABSENT_MINUTES=4 # Minutes to delay turning on the Camera once you have left. export CAMERA_FOLDER_ROOT="/var/www/cam" # The root directory where the Camera's config and output go. </pre>
2.	<input type="checkbox"/>	<p>Action: Review swat.config by paragraph. Start with the router information.</p> <p>If you do not want the scripts managing your Router information, simply blank out the values in swat.config and set them in /etc/wpa_supplicant/wpa_supplicant.conf.</p> <p>Expected Result: You should see something like this:</p> <pre> export MY_ROUTER_NAME="" export MY_ROUTER_PW="" #-----# # The next 2 lines are for modifying the router # # credentials. The settings are found in # # /etc/wpa_supplicant/wpa_supplicant.conf. # # If you do want to set these manually, simply # # blank out the values in the next two lines, and # # modify /etc/wpa_supplicant/wpa_supplicant.conf. # # Example: # # export MY_ROUTER_NAME="" # # export MY_ROUTER_PW="" # #-----# export MY_ROUTER_NAME="DEA Surveillance" # The SSID of your router export MY_ROUTER_PW="NoDrugs4U" export MY_ROUTER_IP="172.16.1.1" #-----# </pre> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>Configurable settings found in /etc/wpa_supplicant/wpa_supplicant.conf. You can blank out the values if you wish to manually set these.</p> </div>

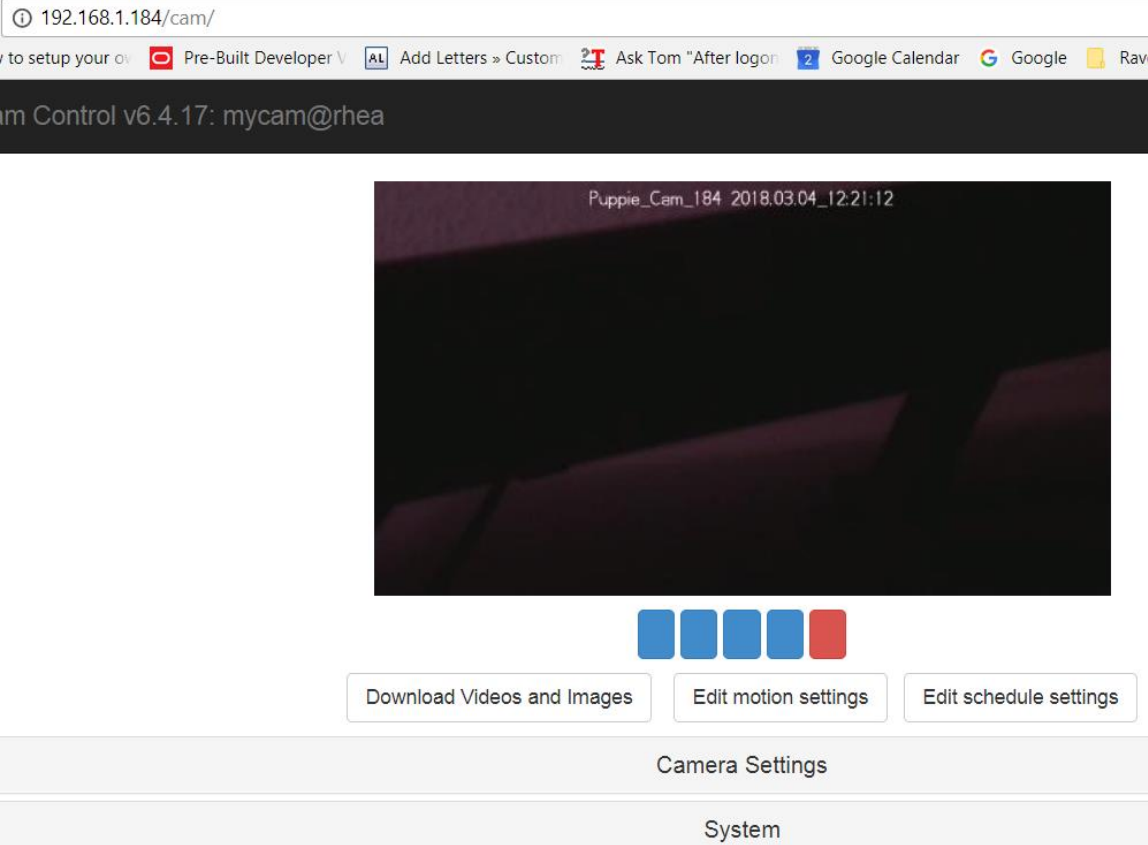
Step	<input checked="" type="checkbox"/>	Action / Expected Result
3.	<input type="checkbox"/>	<p>Action: Review swat.config STATIC IP paragraph.</p> <p>If you are not using static IP, but relying on DHCP for the system to assign your RPi an IP address, then set the following to have blanks for the values.</p> <p>Expected Result: You should see something like this:</p> <pre>export MY_SERVER_WIFI_IP="" export MY_SERVER_STATIC_IP="" export MY_ROUTER_IP="172.16.1.1" # The IP of your router. #-----# # The next 2 lines are for STATIC IP. If you wish # to use DHCP and have the system set the server IP, # # then blank them out. # # These settings are found in /etc/dhcpd.conf. # # You can modify the settings manually if you wish to # # bypass this scripts modifying them. # # Example: # # export MY_SERVER_WIFI_IP="" # # export MY_SERVER_STATIC_IP="" # #-----# export MY_SERVER_WIFI_IP="172.16.1.184" # If you are using STATIC IP, this is the desired Wireless IP export MY_SERVER_STATIC_IP="172.16.1.194" # If you are using STATIC IP, this is the desired Ethernet IP ### # Server Hardware continued ### export MY_CAMERA_NAME="Puppie_Cam `echo \${M ##### # Peripheral Hardware #####</pre> <p>These are configurable and found in /etc/dhcpd.conf. Only used for STATIC IP Addresses</p>
4.	<input type="checkbox"/>	<p>Action: Review swat.config (optional) IOT Presence detection paragraph.</p> <p>These settings are for the optional IOT detection of your cell phone's IP address or Bluetooth address or the Bluetooth address of any iBeacon you wish to use. If you do not want this option enabled, simply blank out the values.</p> <p>Expected Result: You should see something like this:</p> <pre>export CELL_STATIC_IP="" export CELL_WIFI_MAC_ADDRESS="" export CELL_BLUETOOTH_ADDRESS="" # presence detection to turn off the camera, simply # # blank out the values for the next 3 lines. # # Example: # # export CELL_STATIC_IP="" # # export CELL_WIFI_MAC_ADDRESS="" # # export CELL_BLUETOOTH_ADDRESS="" # #-----# export CELL_STATIC_IP="172.16.1.182" # IP of your Cell Phone Optional setting, but used for IOT export CELL_WIFI_MAC_ADDRESS="80:01:86:74:18:d6" export CELL_BLUETOOTH_ADDRESS="04:C2:3D:AE:42:7E" ##### # Script control #####</pre> <p>Optional settings for IOT Presence detection. The Cell Phone's IP address, the MAC address and any Bluetooth iBeacon address. If you do not want to use the IOT presence, simply blank out the values.</p>

Step	<input checked="" type="checkbox"/>	Action / Expected Result
5.	<input type="checkbox"/>	<p>Action: Review swat.config email settings.</p> <p>These settings are optional and allow you to be sent an email with a video attachment when the motion detection is triggered. To disable, simply blank out the values.</p> <p>Expected Result: You should see something like this:</p> <p>Export MY_EMAIL_MAIL_HUB=""</p> <p>Export MY_EMAIL_ADDRESS=""</p> <p>Export MY_EMAIL_PW=""</p> <pre>##### # Script control ##### export MY_EMAIL_MAIL_HUB="smtp.dea.gov:587" export MY_EMAIL_ADDRESS="bucbowie@dea.gov" export MY_EMAIL_PW="tscggvjlgmzlcaca" export CAMERA_CNT_WIFI_ABSENT_MINUTES=4 export CAMERA_FOLDER_ROOT="/var/www/cam" #-----# # Meta Data #-----#</pre> <p><i># The MAIL service to send email. Known as the Mail HUB. # Have email ID for the mail service.</i></p> <p>The email service and credentials for notification when an intruder has triggered the motion detection. If you do not want an email, set the values to blanks.</p>
6.	<input type="checkbox"/>	<p>Action: Save your results in swat.config. We are done and ready to install.</p>

Installation

PROCEDURE 1: Run install.sh

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: From command line, run install.sh</p> <p>Command: # sudo ./install.sh</p> <p>Expected Result: You should see something like this:</p>

Step	<input checked="" type="checkbox"/>	Action / Expected Result
2.	<input type="checkbox"/>	<p>Action: After RPi reboots, open web browser and verify camera is streaming.</p> <p>Command: # <code>http://Your-RPi-IP/cam</code></p> <p>Expected Result: You should see something like this:</p> 

PROCEDURE 2: Stubbed for now

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	Action:. Command: <code>Grant</code> Expected Result: You should see something like this:
2.	<input type="checkbox"/>	End of section

PROCEDURE 3: Stubbed for now.

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action:.</p> <p>Command: <code>Grant</code></p> <p>Expected Result: You should see something like this:</p>
2.	<input type="checkbox"/>	<p>Action:.</p> <p>Command: <code>Grant</code></p> <p>Expected Result: You should see something like this:</p>
3.	<input type="checkbox"/>	<p>Action:.</p> <p>Command: <code>Grant</code></p> <p>Expected Result: You should see something like this:</p>
4.	<input type="checkbox"/>	
5.	<input type="checkbox"/>	
6.	<input type="checkbox"/>	
7.	<input type="checkbox"/>	
8.	<input type="checkbox"/>	
9.	<input type="checkbox"/>	
10.	<input type="checkbox"/>	

Appendix A: Supplementary Instructions

PROCEDURE: Format the USB Storage using Linux and Fdisk.

Step	<input checked="" type="checkbox"/>	Action / Expected Result
1.	<input type="checkbox"/>	<p>Action: After plugging in the usb drive, run blkid to verify the partition. Look for the /dev/sd line item.</p> <p>Command: blkid</p> <p>Expected Result: You should see something like this:</p> <pre>root@rhea:~# blkid /dev/mmcblk0p1: LABEL="boot" UUID="0298-4814" TYPE="vfat" /dev/mmcblk0p2: LABEL="rootfs" UUID="d4f0fd64-ad9d-4cfd-aa /dev/mmcblk0: PTUUID="b0e18a51" PTTYPER="dos" /dev/sda: PTUUID="86298c1d" PTTYPER="dos"</pre>
2.	<input type="checkbox"/>	<p>Action: From command line, run fdisk against the USB drive identified in step 1.</p> <p>Command: fdisk /dev/sda</p> <p>Expected Result: You should see something like this:</p> <pre>root@rhea:~# fdisk /dev/sda Welcome to fdisk (util-linux 2.29.2). Changes will remain in memory only, until you decide to write them. Be careful before using the write command.</pre>

Step	<input checked="" type="checkbox"/>	Action / Expected Result
3.	<input type="checkbox"/>	<p>Action: Initialize the USB partition and create a new partition</p> <p>Commands:</p> <ul style="list-style-type: none"> o # create a new empty DOS partition table n # add a new partition <p>Expected Result: You should see something like this:</p> <pre>Command (m for help): n Partition type p primary (0 primary, 0 extended, 4 free) e extended (container for logical partitions) Select (default p):</pre> <p>Choose p, the default, or you can simply press <ENTER>.</p> <p>Take the defaults for the next 3 choices:</p> <pre>Partition number (1-4, default 1): First sector (2048-30302207, default 2048): Last sector, +sectors or +size{K,M,G,T,P} (2048-30302207, default 30302207):</pre> <p>Commands:</p> <ul style="list-style-type: none"> t - #change a partition type The type we want is: HPFS/NTFS/exFAT w - write table to disk and exit partprobe - # refresh the system partition table mkfs.vfat /dev/sda1 - # Create a Linux/Windows readable partition.

Step	<input checked="" type="checkbox"/>	Action / Expected Result
4.	<input type="checkbox"/>	<p>Action: Issue mount to test the newly formatted USB drive.</p> <p>Command: <code>mount -t vfat -o rw,nofail /dev/sda1 /media/cam</code></p> <p>Expected Result: You should see something like this: (Command: <code>df -k</code>)</p> <pre> root@rhea:~# df -k Filesystem 1K-blocks Used Available Use% Mounted on /dev/root 14791776 4803648 9324204 35% / devtmpfs 443792 0 443792 0% /dev tmpfs 448400 0 448400 0% /dev/shm tmpfs 448400 11652 436748 3% /run tmpfs 5120 4 5116 1% /run/lock tmpfs 448400 0 448400 0% /sys/fs/cgr /dev/mmcblk0p1 41853 21329 20524 51% /boot tmpfs 89680 0 89680 0% /run/user/1 tmpfs 89680 0 89680 0% /run/user/1 tmpfs 89680 0 89680 0% /run/user/1 /dev/sda1 15135280 8 15135272 1% /media/cam </pre>
5.	<input type="checkbox"/>	<p>Action: Update /etc/fstab to persist the mount.</p> <p>Add the following line to the /etc/fstab:</p> <p>Commands: <code>/dev/sda1 /media/cam vfat defaults,noatime,nofail,rw 0 0</code></p>

END OF DOCUMENT