Lab 2: Droning On

Lab overview:

This lab will provide details of drone systems and different ways of reverse engineering drones from the available firmware. This lab will also provide good understanding and hands on experience of drone functions and ways to run simulator based on the available firmware. The overall goal of this lab is to explore the firmware of a drone. This skill can be used for digital forensics and security analysis. The drone under examination is the Autel Evo II.

Requirements:

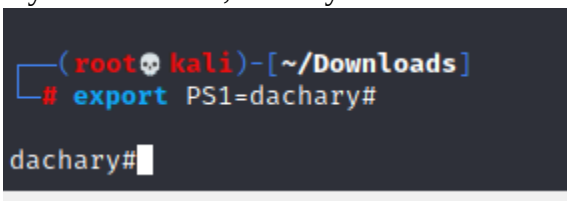
There are various requirements for this lab including good knowledge of drones and Linux system.

OS: Linux OS (I used Kali Linux for this lab)

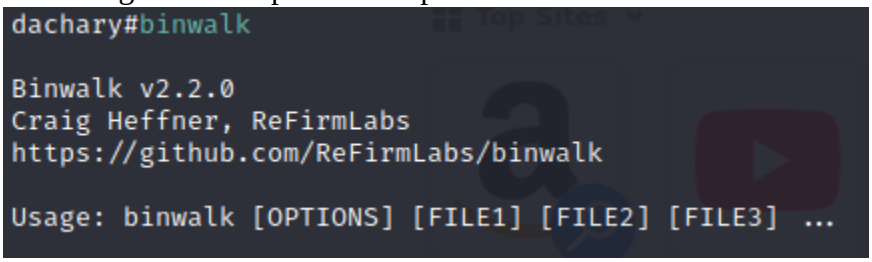
Firmware: We will use the available firmware (version 2.5.18 beta) from the given link. (https://dl.dropboxusercontent.com/s/75v58yhjou0zbuj/Model-C_FW_V2.5.18.bin?dl=0)

Dependencies: Various dependencies required are binwalk and qemu VM.

1. **STEP 1:**
   Set up terminal: I set the terminal name to my GMU email name by using export command and set that to PS1 environment. Here is the screenshot of changing my terminal name to my GMU ID. i.e., dachary as follows.



2. **STEP 2:**
   Setup binwalk: In the installed distribution of Kali I have, binwalk is already installed. Following sreenshot provies the proof and the version of binwalk installed in my system.



   From the screenshot, version 2.2.0 of binwalk is running on my system. There are various options available in the manual page of binwalk which will be used in further steps.

3. **STEP 3**:
   Autel EVO II: (capabilities, type of controls/ground stations, intended purpose, and target demographic (user base) of the drone)

The Autel EVO II is capable of capturing footages in 8K with resolutions up to 7680×4320. It is also capable of phase detection by precision auto focus that enables tracking of fast-moving subjects accurately. This drone is equipped with 19 groups of sensors including 12 visual sensors, the main camera, ultrasound, IMUs and other sensors which enables building 3-D maps and path planning in real time. Using all these sensors it is able to model location and speed of targets simultaneously, predict their trajectory accurately, and track them continuously while identifying various objects at the same time. It has 40 minutes of flight time with the battery of 7100 mAh, with 5.5 miles range of video transmission from the pilot's location with bitrate of 120Mbps. It can resist up to 39 mph winds and can fly up to 45 mph with max of 18 mph ascent and 9 mph of descent speed. The max takeoff weight is 4.4 lbs. It is suitable to use in temperatures of range 14 F to 104 F. This drone works in frequency of 2.4 ~ 2.4853 GHz. The omnidirectional binocular sensing system can measure accurately in range of 11 – 20 meters in forward, backwards, upwards, downwards, and side wise. The remote controller can transmit 9 KM FCC at the same frequency as the drone frequency with 720p/180 p @ 30 fps video transmission.

4. **STEP 4**:

The 11 components of the firmware version with their function are as follows:

Component	**Version**	**Function**
Flight Control	V0.0.4.7	Determine orientation, motion, and speed and help control drone accordingly.
Camera	V0.2.30.30	Visualize, real time stream, and 3-D modeling, object recognition.
Remote Controller	V2.0.4.5	Controlling drone remotely.
RC Panel	V3.0.11.0	Sends/ receives radio control signals.
Image Transmission	V1.1.1.41	Transmits image captured by drone.
RC Image Transmission	V1.1.1.41	Transmits image through RC signals.
Gimbal	V0.1.41.0	Provides stabilization for cameras and other sensors.
Battery	V0.0.14.0	Provides power for remote control and drone.
Visual Module	V0.2.30.30	Used for visual based tracking and navigation
Sonar	V1.2.1.25	Sends sound waves that gets reflected on object for object detection.
ESC1-4	V1.0.3.6	ESC/ Electronic Speed controllers allow flight controllers to control and adjust speed of drones electric motors.

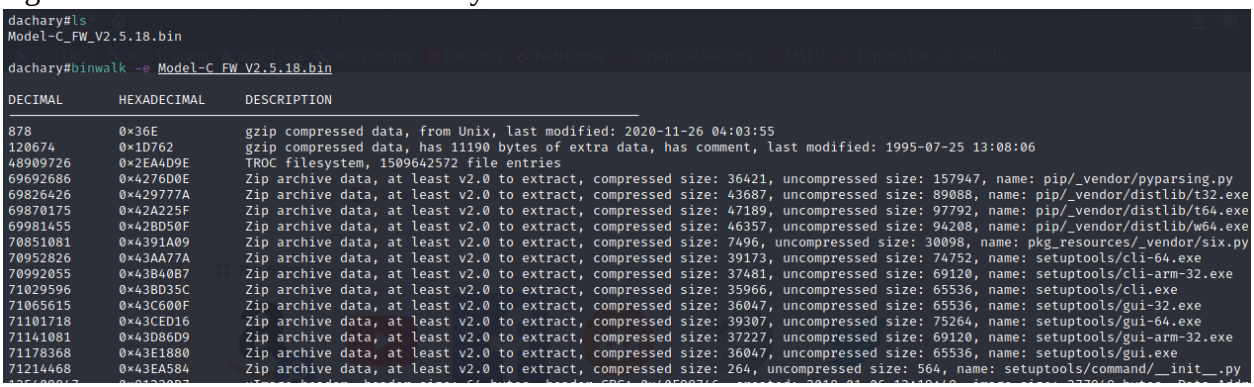
IMU or Inertial Measurement Unit is a sensor that detects motion along a horizontal plane as well as increase and decrease in altitude. It uses accelerometers and gyroscopes to measure acceleration and rotation which can be used to provide position data of the drone. Thus, the common application of IMU include control and stabilization, guidance, and correction, measurement and testing, and mobile mapping.

5. **STEP 5**:

Downloaded image: Here is the screen shot that shows the original bin file.

```
dachary#ls
Model-C_FW_V2.5.18.bin

dachary#
```

Unpack .bin using Binwalk: I used "binwalk -e <filename>" command to extract the files in the bin folder. We have a directory of extracted files, the new directory is "_Model-C_FW_V2.5.18.bin.extracted". The binwalk unpacked all the embedded files and executable codes in the given binary file. Thus, binwalk is used to identify files and code embedded inside of firmware images. It uses libmagic library and is compatible with magic signatures created for Unix file utility. The screenshot of the extraction is shown below:



```
dachary#ls
Model-C_FW_V2.5.18.bin

dachary#binwalk -e Model-C_FW_V2.5.18.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
878           0x36E           gzip compressed data, from Unix, last modified: 2020-11-26 04:03:55
120674        0x1D762         gzip compressed data, has 11190 bytes of extra data, has comment, last modified: 1995-07-25 13:08:06
48909726      0x2EA4D9E       TROC filesystem, 1509642572 file entries
69692686      0x4276D0E       Zip archive data, at least v2.0 to extract, compressed size: 36421, uncompressed size: 157947, name: pip/_vendor/pyparsing.py
69826426      0x429777A       Zip archive data, at least v2.0 to extract, compressed size: 43687, uncompressed size: 89088, name: pip/_vendor/distlib/t32.exe
69870175      0x42A225F       Zip archive data, at least v2.0 to extract, compressed size: 47189, uncompressed size: 97792, name: pip/_vendor/distlib/t64.exe
69981455      0x42BD50F       Zip archive data, at least v2.0 to extract, compressed size: 46357, uncompressed size: 94208, name: pip/_vendor/distlib/w64.exe
70851081      0x4391A09       Zip archive data, at least v2.0 to extract, compressed size: 7496, uncompressed size: 30098, name: pkg_resources/_vendor/six.py
70952826      0x43AA77A       Zip archive data, at least v2.0 to extract, compressed size: 39173, uncompressed size: 74752, name: setuptools/cli-64.exe
70992055      0x43B40B7       Zip archive data, at least v2.0 to extract, compressed size: 37481, uncompressed size: 69120, name: setuptools/cli-arm-32.exe
71029596      0x43BD35C       Zip archive data, at least v2.0 to extract, compressed size: 35966, uncompressed size: 65536, name: setuptools/cli.exe
71065615      0x43C600F       Zip archive data, at least v2.0 to extract, compressed size: 36047, uncompressed size: 65536, name: setuptools/gui-32.exe
71101718      0x43CED16       Zip archive data, at least v2.0 to extract, compressed size: 39307, uncompressed size: 75264, name: setuptools/gui-64.exe
71141081      0x43D86D9       Zip archive data, at least v2.0 to extract, compressed size: 37227, uncompressed size: 69120, name: setuptools/gui-arm-32.exe
71178368      0x43E1880       Zip archive data, at least v2.0 to extract, compressed size: 36047, uncompressed size: 65536, name: setuptools/gui.exe
71214468      0x43EA584       Zip archive data, at least v2.0 to extract, compressed size: 264, uncompressed size: 564, name: setuptools/command/__init__.py
```

6. **STEP 6**:

The result of the binwalk file is shown in the screenshot below:

```
dachary#ls
Model-C_FW_V2.5.18.bin  _Model-C_FW_V2.5.18.bin.extracted

dachary#cd _Model-C_FW_V2.5.18.bin.extracted
```

```
dachary#ls
1D762.gz  _36E.extracted  81B244F      906460E        9CA3D1F  B01C102.yaffs  _fwimage.upg.extracted  ubifs-root  yaffs-root-0
36E       4276D0E.zip     84442EF.ubi  94F26A2.yaffs  AB8E06E  fwimage.upg    pip                     yaffs-root
```

The "file" command is used to see the file type in Linux. From the screenshot above we can see that the file "36E" is tar archive file.

```
dachary#cd _36E.extracted

dachary#ls
0.tar  boot  boot_md5  config.ini  kernel  kernel_md5  len_upgrade  len_upgrade_md5  rootfs.ext4  rootfs.ext4_md5  version.txt

dachary#
```

```
dachary#binwalk -e 36E

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             POSIX tar archive (GNU)


dachary#
```

On unzipping 36E file we got 10 files as seen in the screenshot above.

The content in the config.ini is shown below:

```
dachary#cd _36E.extracted

dachary#ls
0.tar  boot  boot_md5  config.ini  kernel  kernel_md5  len_upgrade  len_upgrade_md5  rootfs.ext4  rootfs.ext4_md5  version.txt

dachary#
```

This suggest that the bootloader is U-Boot bootloader because of the arguments used in the config.ini files. The arg root/dev/mmcblk0p3 and mmc read determines that the bootloader is U-boot.
The filesystem used is TROC.
The TTY is set to the Baud rate of 115200 bits per sec.
The rootfs.ext4 is android sparse image as shown in the screenshot below.

```
dachary#file rootfs.ext4
rootfs.ext4: Android sparse image, version: 1.0, Total of 102400 4096-byte output blocks in 5944 input chunks.
```

7. STEP 7: Root file is found in the extracted .bin obtained from the binwalk process followed by **ubifs-root/329989061/rootfs**. The content of root is shown below: There are all the main directories that contains all settings and configurations.

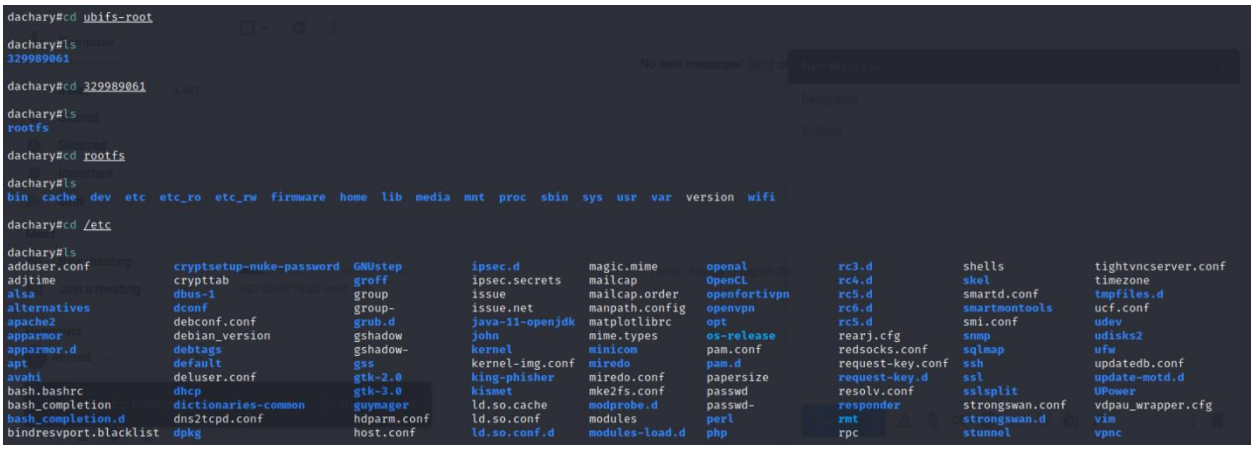
```
dachary#cd ubifs-root

dachary#ls
329989061

dachary#cd 329989061

dachary#ls
rootfs

dachary#cd rootfs

dachary#ls
bin  cache  dev  etc  etc_ro  etc_rw  firmware  home  lib  media  mnt  proc  sbin  sys  usr  var  version  wifi
```

The CPU architecture is mainly found in the root/proc/cpuinfo in the regular linux file system but there was nothing inside proc directory. From the observation and the
String command recursively for rootfs file we found out that the the CPU architecture is 64 bits.

```
desc-size
desc_size
%s requires '-O 64bit'

'%s' must be before 'resize=%u'

Invalid desc_size: '%s'
```

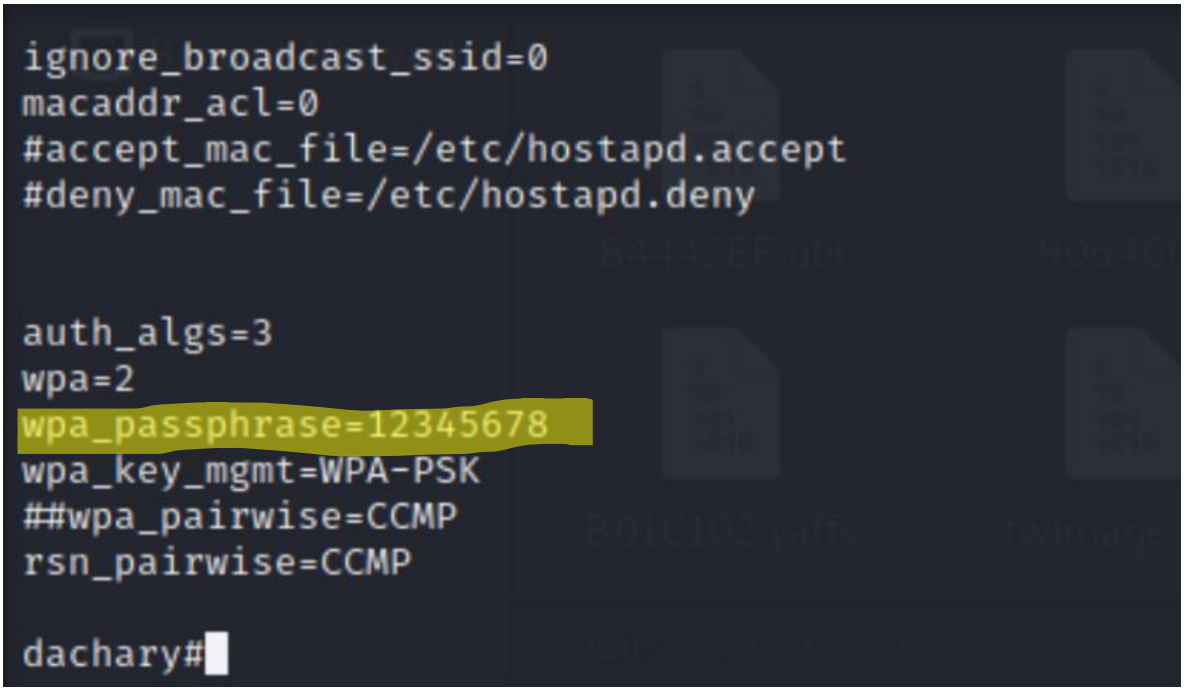
8. STEP 8: Configuration files

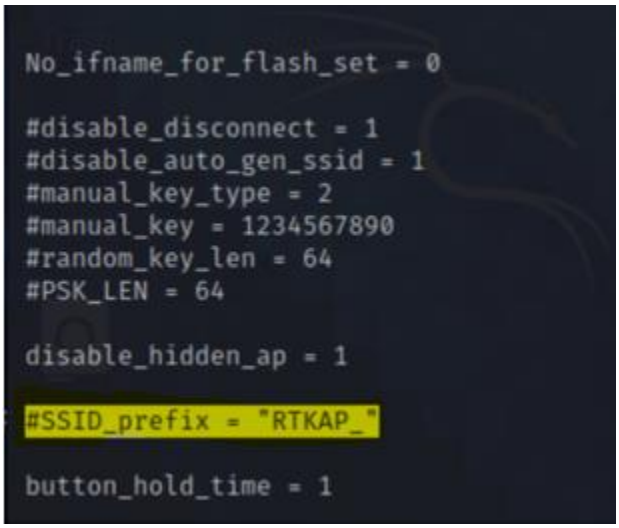
The configurations are stored in /etc in the Linux file system. The wifi access point is contained in /etc/hostapd-wpa.conf file. More configuration setting is inside /rootfs/wifi/Realtek.



```
dachary#cd ubifs-root

dachary#ls
329989061

dachary#cd 329989061

dachary#ls
rootfs

dachary#cd rootfs

dachary#ls
bin  cache  dev  etc  etc_ro  etc_rw  firmware  home  lib  media  mnt  proc  sbin  sys  usr  var  version  wifi

dachary#cd /etc

dachary#ls
adduser.conf            cryptsetup-nuke-password  GNUstep          ipsec.d          magic.mime       openal           rc3.d          shells              tightvncserver.conf
adjtime                 crypttab                  groff            ipsec.secrets    mailcap          OpenCL           rc4.d          skel                timezone
alsa                    dbus-1                    group            issue            mailcap.order    openfortivpn     rc5.d          smartd.conf         tmpfiles.d
alternatives            dconf                     group-           issue.net        manpath.config   openvpn          rc6.d          smartmontools       ucf.conf
apache2                 debconf.conf              grub.d           java-11-openjdk  matplotlibrc     opt              rc5.d          smi.conf            udev
apparmor                debian_version            gshadow          john             mime.types       os-release       rearj.cfg      snmp                udisks2
apparmor.d              debtags                   gshadow-         kernel           minicom          pam.conf         redsocks.conf  sqlmap              ufw
apt                     default                   gss              kernel-img.conf  miredo           pam.d            request-key.conf  ssh              updatedb.conf
avahi                   deluser.conf              gtk-2.0          king-phisher     miredo.conf      papersize        request-key.d  ssl                 update-motd.d
bash.bashrc             dhcp                      gtk-3.0          kismet           mke2fs.conf      passwd           resolv.conf    sslsplit            UPower
bash_completion         dictionaries-common       guymager         ld.so.cache      modprobe.d       passwd-          responder      strongswan.conf     vdpau_wrapper.cfg
bash_completion.d       dns2tcpd.conf             hdparm.conf      ld.so.conf       modules          perl             rmt            strongswan.d        vim
bindresvport.blacklist  dpkg                      host.conf        ld.so.conf.d     modules-load.d   php              rpc            stunnel             vpnc
```

```
dachary#cat wscd.conf
#detail please reference config_file_README.txt
wlan_fifo0 ="/wifi/realtek/wscd-wlan0.fifo"
wlan_fifo1 ="/wifi/realtek/wscd-wlan1.fifo"

SSID_prefix = "Reaktek_AP_"

use_ie = 1

# AUTH_OPEN=1, AUTH_WPAPSK=2, AUTH_SHARED=4, AUTH_WPA=8, AUTH_WPA2=0×10, AUTH_WPA2PSK=0×20
auth_type_flags = 39

# ENCRYPT_NONE=1, ENCRYPT_WEP=2, ENCRYPT_TKIP=4, ENCRYPT_AES=8
encrypt_type_flags = 15

uuid = 630412531019200612 28aabbccddeeff
device_name = "RTK_AP"
manufacturer = "Realtek"
manufacturerURL = "http://www.realtek.com/"
modelURL = "http://www.realtek.com/"
model_name = "RTL8xxx"
model_num = "EV-2010-09-20"
serial_num = "123456789012347"
modelDescription = "WLAN Access Point"
device_attrib_id = 1
device_oui = 0050f204
device_category_id = 6
device_sub_category_id = 1

# PASS_ID_DEFAULT=0, PASS_ID_USER=1, PASS_ID_MACHINE=2, PASS_ID_REKEY=3,
# PASS_ID_PB=4, PASS_ID_REG=5, PASS_ID_RESERVED=6
device_password_id = 0
```

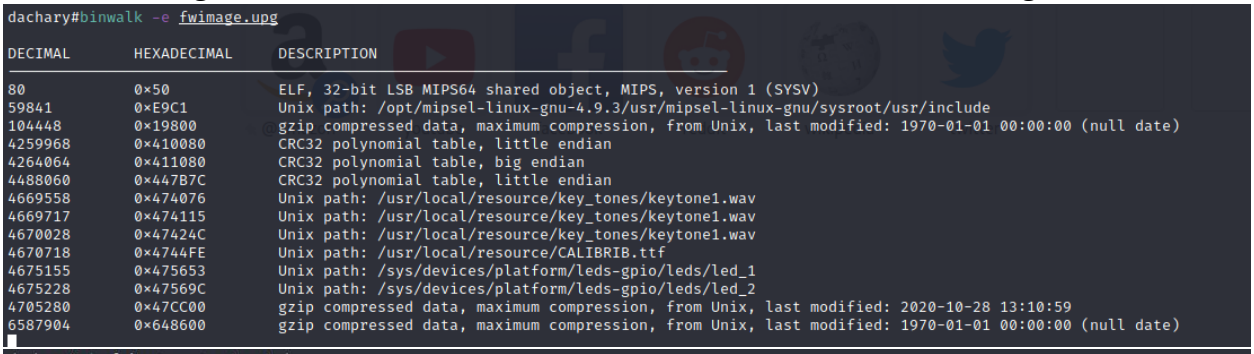


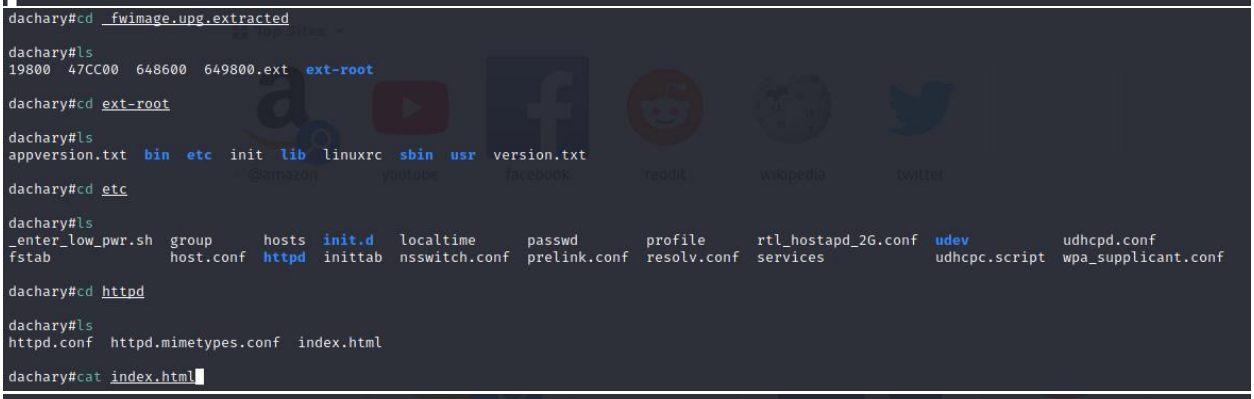


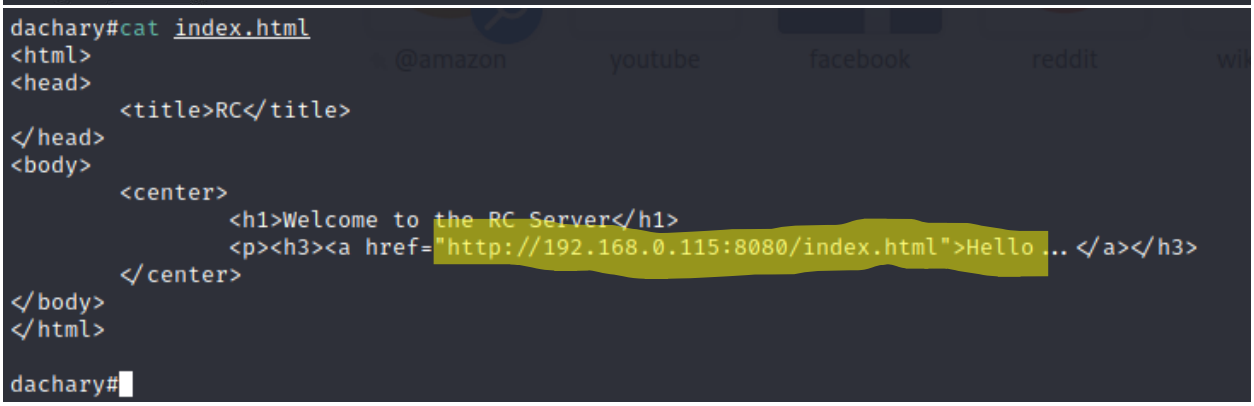
From the above observation and screenshot the wpa password is 12345678 and the SSID prefix is “RTKAP_” as seen above.

9. STEP 9: HTTPS

In the following screenshots we will see where the RC server and HTTP is being used.







From the above screenshot the address of RC server is 192.168.0.115 and the port it is listening is port 8080. Http is running on an apache server because it uses httpd. It is designed to be run as a standalone daemon process. When used like this it will create a pool of child processes or threads to handle requests. It is started with hello message as shown in the screenshot above.

10. STEP 10: Qemu

I installed Qemu as follows.

```
root@kali:~# apt-get install qemu
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libomp5-9 libpython-all-dev python-all python-all-dev
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  qemu
0 upgraded, 1 newly installed, 0 to remove and 1641 not upgraded.
Need to get 68.4 kB of archives.
After this operation, 96.3 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 qemu amd64 1:5.2+dfsg-3 [68.4 kB]
Fetched 68.4 kB in 1s (97.0 kB/s)
Selecting previously unselected package qemu.
(Reading database ... 303903 files and directories currently installed.)
Preparing to unpack .../qemu_1%3a5.2+dfsg-3_amd64.deb ...
Unpacking qemu (1:5.2+dfsg-3) ...
Setting up qemu (1:5.2+dfsg-3) ...
```

I tried mounting the firmware image in the qemu but the attempt failed. I also researched into angr emulator and installed angr as follows.

```
dachary#sudo apt-get install python3-dev libffi-dev build-essential virtualenvwrapper
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
build-essential is already the newest version (12.9).
build-essential set to manually installed.
The following additional packages will be installed:
  libffi7 libpython3-dev libpython3-stdlib libpython3.9 libpython3.9-dev libpython3.9-minimal libpython3.9-stdlib python-pip-whl python3 python3-distlib
  python3-distutils python3-filelock python3-lib2to3 python3-minimal python3-pbr python3-pip python3-stevedore python3-virtualenv python3-virtualenv-clone
  python3-virtualenvwrapper python3-wheel python3.9 python3.9-dev python3.9-minimal virtualenv
Suggested packages:
  python3-doc python3-tk python3-venv python3.9-venv python3.9-doc virtualenvwrapper-doc
The following NEW packages will be installed:
  python-pip-whl python3-distlib python3-filelock python3-pbr python3-pip python3-stevedore python3-virtualenv python3-virtualenv-clone python3-virtualenvwrapper
  python3-wheel virtualenv virtualenvwrapper
The following packages will be upgraded:
  libffi-dev libffi7 libpython3-dev libpython3-stdlib libpython3.9 libpython3.9-dev libpython3.9-minimal libpython3.9-stdlib python3 python3-dev python3-distutils
  python3-lib2to3 python3-minimal python3.9 python3.9-dev python3.9-minimal
16 upgraded, 12 newly installed, 0 to remove and 456 not upgraded.
Need to get 14.3 MB of archives.
After this operation, 5,462 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 python3.9-dev amd64 3.9.2-1 [515 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libpython3.9-dev amd64 3.9.2-1 [4,028 kB]
```