

IOT

Firmware Analysis

Name: Isha Gupta

What is firmware?

Firmware is a piece of code residing on the non volatile section of the device allowing and enabling the device to perform different tasks required for the functioning of the device. It also helps in functioning of various devices, kernel, boot loader, file system and additional resources.

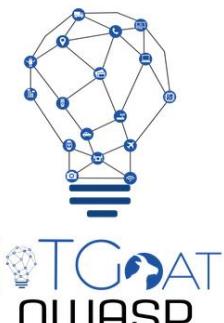
In this we will extract the firmware and analyse it.

Environment used:

Attify OS

Firmware to be analysed:

OWASP IoTGoat



Steps involved :

1) Download the firmware that you want to analyse.

Download link: <https://github.com/OWASP/IoTGoat/releases>

2) Analyse the firmware by using **binwalk** tool.

binwalk IoTGoat-raspberry-pi2.img

From here we come to know about

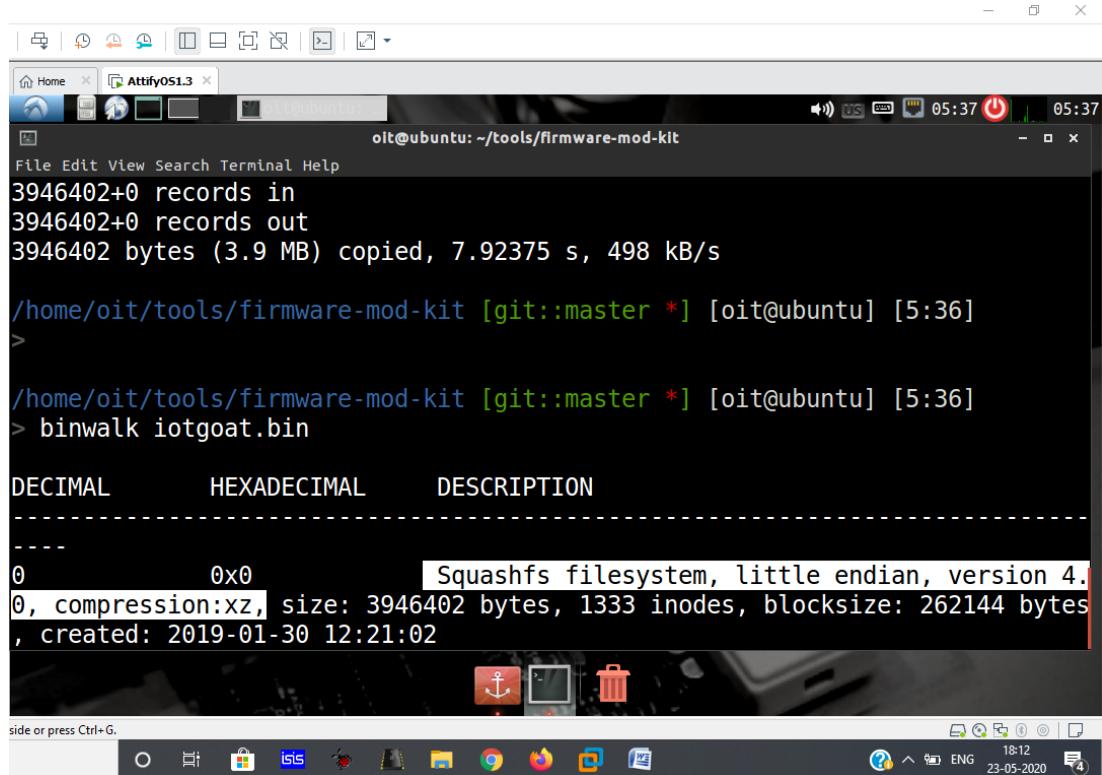
- filesystem - Squashfs
- compression – xz
- address – 29360128

3) We have seen in last step after how many offset it should start extracting i.e. 29360128

```
dd if=IoTGoat-raspberry-pi2.img bs=1 skip=29360128 of=iotgoat.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
-	-	Squashfs filesystem, little endian, version 4.
0	0x0	

Now, check the output file



```
3946402+0 records in
3946402+0 records out
3946402 bytes (3.9 MB) copied, 7.92375 s, 498 kB/s

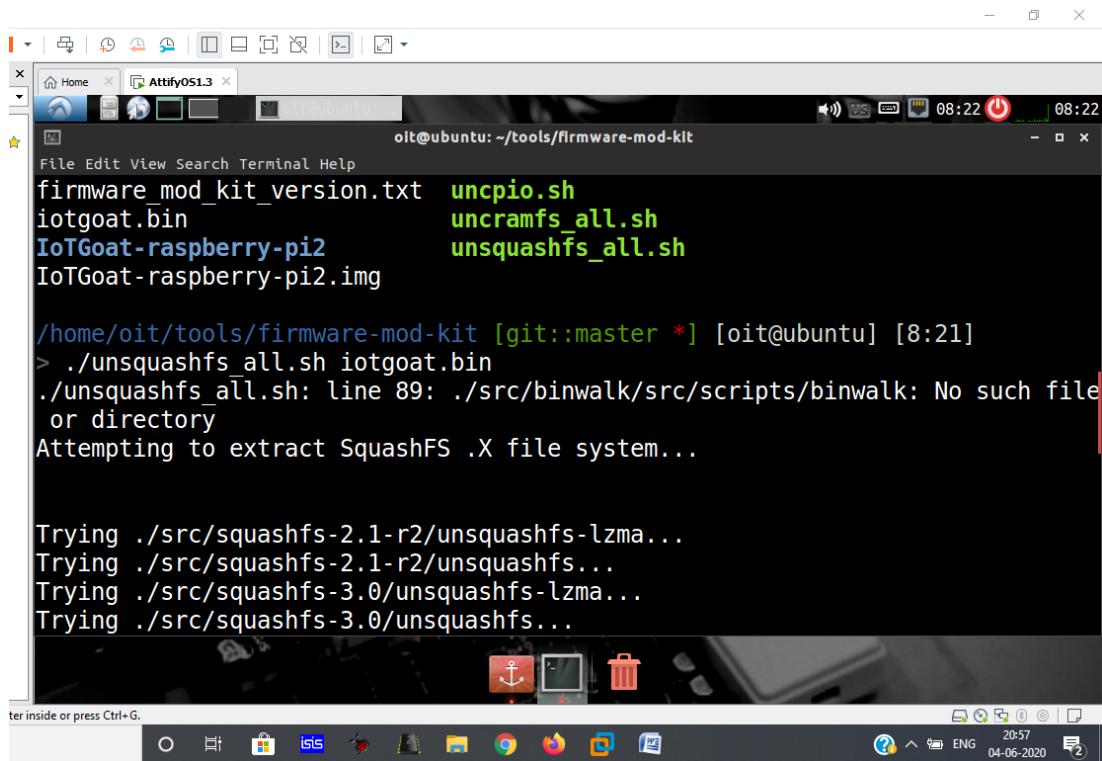
/home/oit/tools/firmware-mod-kit [git::master *] [oit@ubuntu] [5:36]
>

/home/oit/tools/firmware-mod-kit [git::master *] [oit@ubuntu] [5:36]
> binwalk iotgoat.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
----          -----          -----
0            0x0              Squashfs filesystem, little endian, version 4.1
0, compression:xz, size: 3946402 bytes, 1333 inodes, blocksize: 262144 bytes
, created: 2019-01-30 12:21:02
```

4) Now extract it using

```
unsquashfs_all.sh iotgoat.bin
```



```
firmware_mod_kit_version.txt  uncpio.sh
iotgoat.bin                  uncramfs_all.sh
IoTGoat-raspberry-pi2        unsquashfs_all.sh
IoTGoat-raspberry-pi2.img

/home/oit/tools/firmware-mod-kit [git::master *] [oit@ubuntu] [8:21]
> ./unsquashfs_all.sh iotgoat.bin
./unsquashfs_all.sh: line 89: ./src/binwalk/src/scripts/binwalk: No such file
or directory
Attempting to extract SquashFS .X file system...

Trying ./src/squashfs-2.1-r2/unsquashfs-lzma...
Trying ./src/squashfs-2.1-r2/unsquashfs...
Trying ./src/squashfs-3.0/unsquashfs-lzma...
Trying ./src/squashfs-3.0/unsquashfs...
```

We see squashfs-root with all the root directory

```

AttifyOS1.3
File Edit View Search Terminal Help
iotgoat.bin      uncpio.sh
IoTGoat-raspberry-pi2  uncramfs_all.sh
IoTGoat-raspberry-pi2.img  unsquashfs_all.sh

/home/oit/tools/firmware-mod-kit [git::master *] [oit@ubuntu] [8:30]
> cd squashfs-root

/home/oit/tools/firmware-mod-kit/squashfs-root [git::master *] [oit@ubuntu] [8:30]
> ls
bin  dnsmasq_setup.sh  lib  overlay  rom  sbin  tmp  var
dev  etc                mnt  proc    root  sys  usr  www

/home/oit/tools/firmware-mod-kit/squashfs-root [git::master *] [oit@ubuntu] [8:30]
>

```

5) Another way to extract this firmware is by using binwalk

`binwalk -e IoTGoat-raspberry-pi2.img`

DECIMAL	HEXADECIMAL	DESCRIPTION
4253711	0x40E80F	Copyright string: "copyright does *not* cover user programs that use kernel"
4253946	0x40E8FA	Copyright string: "copyrighted by the Free Software"
4254058	0x40E96A	Copyright string: "copyrighted by me and others who actually wrote it."
4254443	0x40EAEB	Copyright string: "Copyright (C) 1989, 1991 Free Software Foundation, Inc."
4256293	0x40F225	Copyright string: "copyright the software, and "

Now go to the extracted file, there we see squashfs-root folder inside which we get root folders of iotgoat firmware

`cd _IoTGoat-raspberry-pi2.img.extracted`

`cd squashfs-root`

```
ls
```

```
olt@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root
File Edit View Search Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted [git::master *] [oit@ubuntu] [5:42]
> ls
1C00000.squashfs B80B6C C41DD6.xz squashfs-root

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted [git::master *] [oit@ubuntu] [5:43]
> cd squashfs-root

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [5:43]
> ls
bin dnsmasq_setup.sh lib overlay rom sbin [redacted] var
dev etc mnt proc root sys usr www

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root
```

6) Once we are here lets search for some sensitive files.

Go to /etc folder there we see passwd and shadow file

Let's find out what all we can do with that

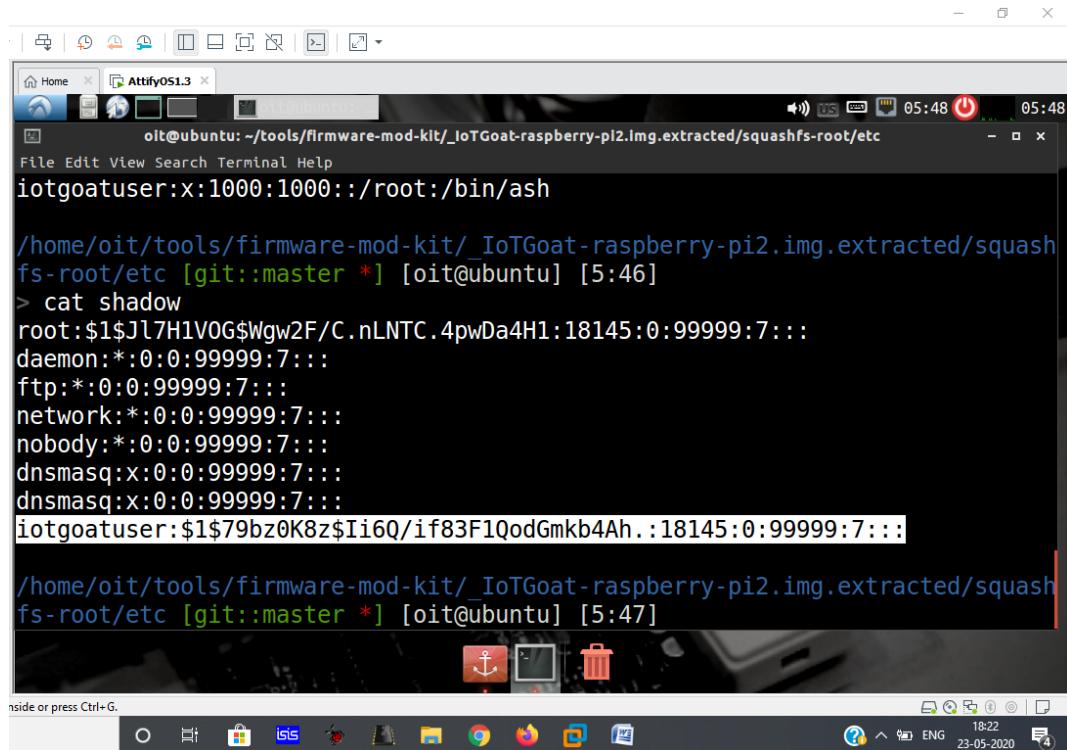
```
cat passwd
```

Here we see a user named iotgoatuser, now lets check the shadow file

```
olt@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/etc
File Edit View Search Terminal Help
dnsmasq.conf.og iproute2 preinit sysctl.d
dropbear localtime profile sysupgrade.conf
e2fsck.conf luci-uploads protocols TZ
ethers modules-boot.d rc.button uci-defaults

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/etc [git::master *] [oit@ubuntu] [5:46]
> cat passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
iotgoatuser:x:1000:1000::/root:/bin/ash
```

cat shadow



```
iotgoatuser:x:1000:1000::/root:/bin/ash

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/etc [git::master *] [oit@ubuntu] [5:46]
> cat shadow
root:$1$JL7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7:::

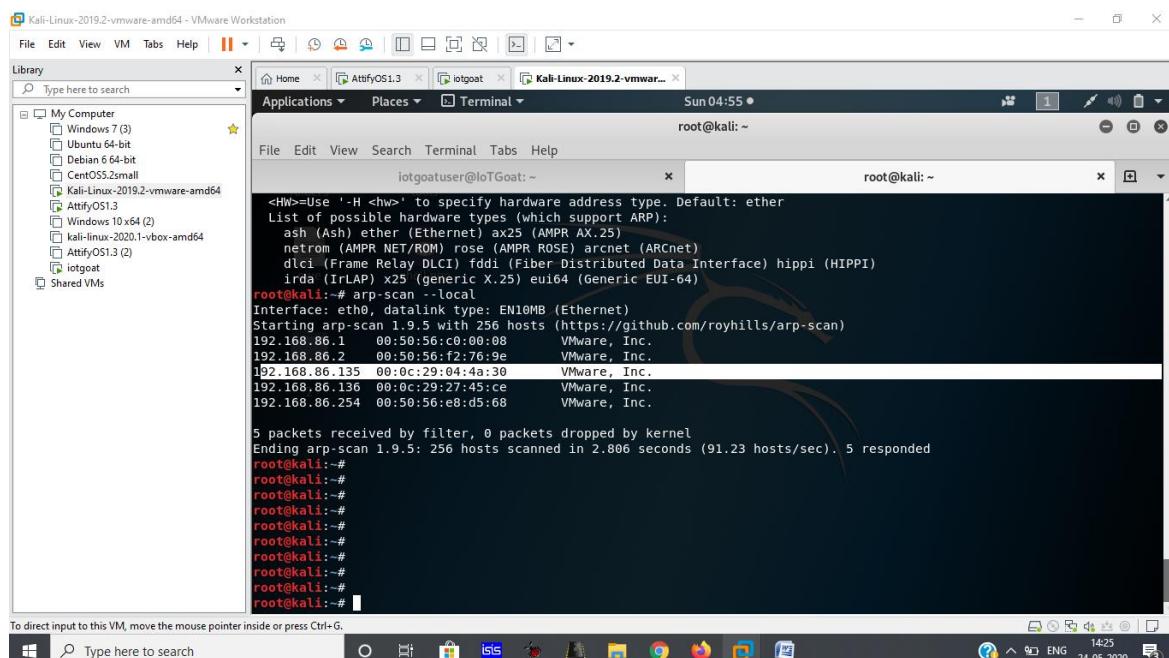
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/etc [git::master *] [oit@ubuntu] [5:47]
```

7) Download the IoTGoat vmdk file and run in Vmware

Download link : <https://github.com/OWASP/IoTGoat/releases>

After running that vmdk, go to kali and search for the IP of IoTGoat using

arp-scan --local

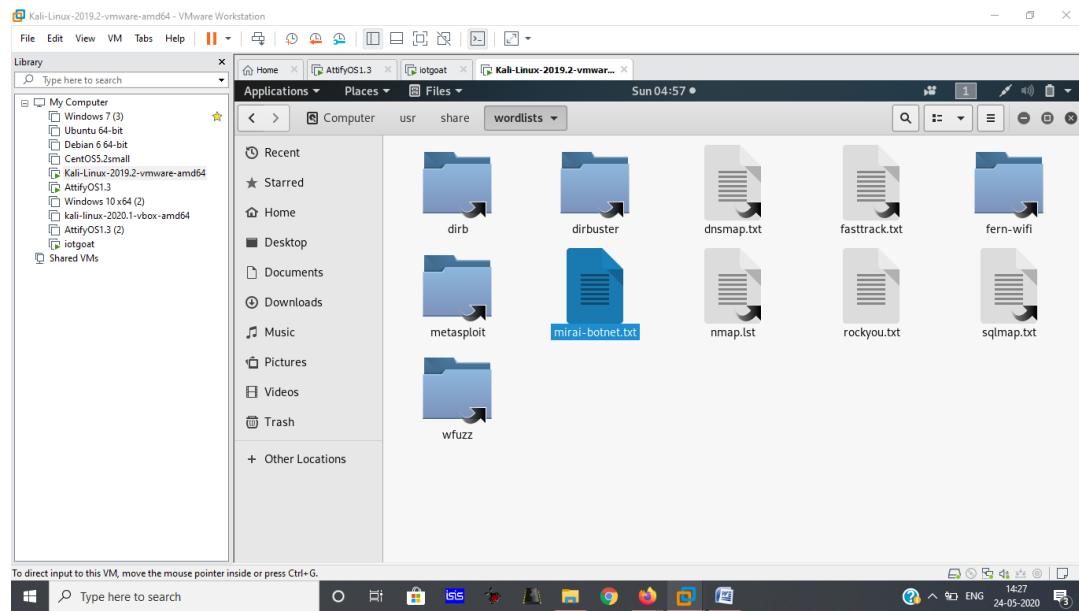


```
root@kali:~# arp-scan --local
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.86.1 00:50:56:00:08:08 VMware, Inc.
192.168.86.2 00:50:56:f2:76:9e VMware, Inc.
192.168.86.135 00:0c:29:04:4a:30 VMware, Inc.
192.168.86.136 00:0c:29:27:45:ce VMware, Inc.
192.168.86.254 00:50:56:e8:d5:68 VMware, Inc.

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.806 seconds (91.23 hosts/sec). 5 responded
```

8) We already know the username i.e. `iotgoatuser` now to fetch the password of IoTGoat download the credential list file from the following link and save it in `/usr/share/wordlists`

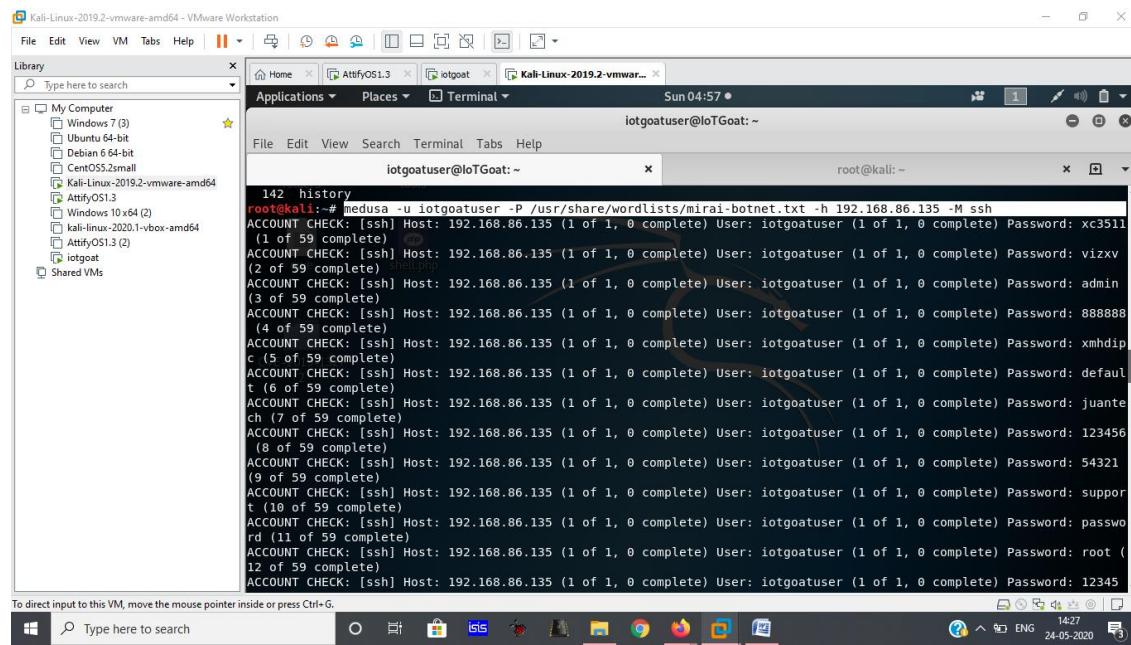
https://github.com/securing/mirai_credentials/blob/master/mirai_creds.txt



9) In order to bruteforce the password for the user `iotgoatuser` we can use hydra or medusa

I've used medusa for the following using the command

```
medusa -u iotgoatuser -P /usr/share/wordlists/mirai-botnet.txt -h <IoTGoat IP> -M ssh
```

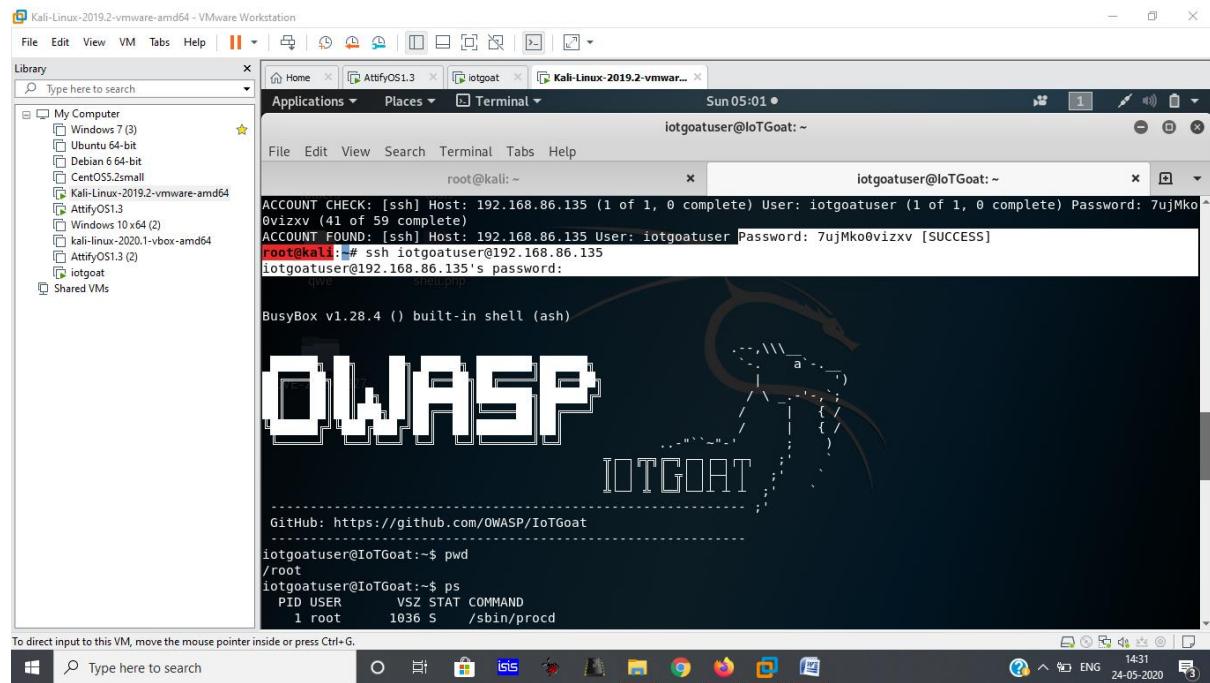


From here we got to know the password is **7ujMko0vizxv**

10) Now we can take ssh connecten of the machine using the command

```
ssh iotgoatuser@IP
```

enter password in the next step and we will get the ssh connection of the machine



11) Let's get back to our attify OS and look for some juicy information.

For emulation find the architecture

Below we see that it is **ARM** architecture by `readelf -h bin/busybox`

```
File Edit View Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:03]
> readelf -h bin/busybox
ELF Header:
  Magic: 7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class: ELF32
  Data: 2's complement, little endian
  Version: 1 (current)
  OS/ABI: UNIX - System V
  ABI Version: 0
  Type: EXEC (Executable file)
  Machine: ARM
  Version: 0x1
  Entry point address: 0x16d18
  Start of program headers: 52 (bytes into file)
  Start of section headers: 0 (bytes into file)
```

Now let's copy qemu for the ARM architecture

To see qemu for ARM path use

`which qemu-arm-static`

`cp /usr/bin/qemu-arm-static .`

`ls`

```

AttifyOS1.3 - VMware Workstation
File Edit View VM Tabs Help ━ ━ ━ ━ ━ ━ ━ ━ ━ ━ ━ ━ ━ ━ ━
Library Type here to search
My Computer
    Windows 7 (3)
    Ubuntu 64-bit
    Debian 6 64-bit
    CentOS 5.2 small
    Kali-Linux-2019.2-vmware-amd64
    AttifyOS1.3
    Windows 10 x64 (2)
    kali-linux-2020.1-vbox-amd64
    AttifyOS1.3 (2)
    iotgoat
    WIN7 bo
Shared VMS

Home AttifyOS1.3
oit@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root 10:06 10:06
File Edit View Search Terminal Help
cp: missing destination file operand after '/usr/bin/qemu-arm-static'
Try 'cp --help' for more information.

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:05]
> cp /usr/bin/qemu-arm-static .

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:05]
> ls
bin  dnsmasq_setup.sh  lib  overlay  qemu-arm-static  root  sys  usr  www
dev  etc                  mnt  proc     rom          sbin  tmp  var

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:05]
> [REDACTED]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

`sudo chroot . ./qemu-arm-static ./bin/busybox`

12) If we go to `/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/controller/iotgoat`

We see a db file

Let's open it by `sqlite3 sensordata.db`

```

AttifyOS1.3
sqlite3 sensordata.db 10:51 10:51
File Edit View Search Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/controller/iotgoat [git::master *] [oit@ubuntu] [10:32]
> ls
iotgoat.lua  sensordata.db

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/controller/iotgoat [git::master *] [oit@ubuntu] [10:32]
> sqlite3 sensordata.db
SQLite version 3.8.2 2013-12-06 14:53:30
Enter ".help" for instructions
Enter SQL statements terminated with a ";" 
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;

inside or press Ctrl+G.

```

We see plenty of email ID with birth date

A screenshot of a terminal window titled "AttifyOS1.3". The window shows the following command being run:

```
BEGIN TRANSACTION;
CREATE TABLE sensors(id INTEGER PRIMARY KEY AUTOINCREMENT, temperature NUMERIC IC, humidity NUMERIC, currdate DATE, currentime TIME, name TEXT, email TE XT, birthdate NUMERIC);
INSERT INTO "sensors" VALUES(1,22.4,68,'2020-03-24','18:56:33','johnsmith','johnsmith@gmail.com',1311977);
INSERT INTO "sensors" VALUES(2,29.7,98,'2020-03-24','18:56:43','jillsmith','jillsmith@gmail.com',4141979);
INSERT INTO "sensors" VALUES(3,31.2,28,'2020-03-24','18:57:05','walter','wal tergary@yopmail.com',32821969);
INSERT INTO "sensors" VALUES(4,16.9,38,'2020-03-24','18:57:20','WilliamRonald','billronald@yopmail.com',11141989);
INSERT INTO "sensors" VALUES(5,35,78,'2020-03-24','18:58:04','Test','TstUser@aol.com',12121990);
INSERT INTO "sensors" VALUES(6,35,88,'2020-03-24','18:58:18','Sgt','sgtmajor@us.gov',10171956);
```

13) We also see various shell script files in /lib/functions

A screenshot of a terminal window titled "AttifyOS1.3". The window shows the following command being run:

```
fs-root/usr [git::master *] [oit@ubuntu] [11:06]
> cd ..

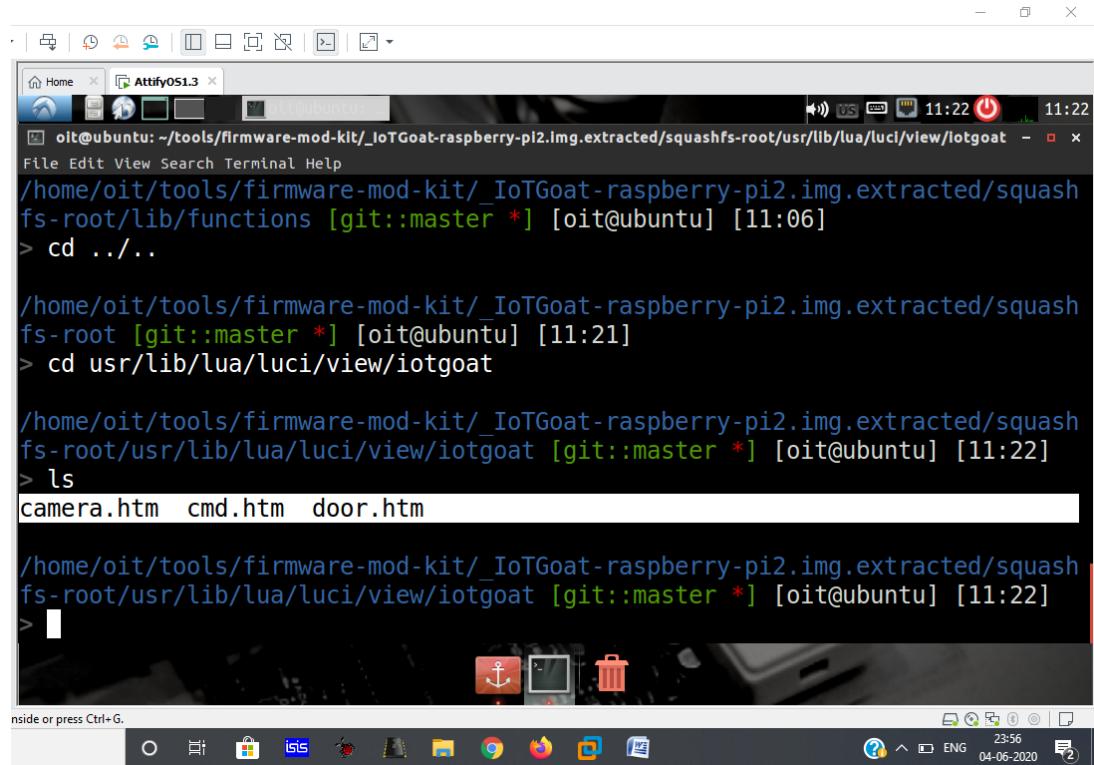
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root [git::master *] [oit@ubuntu] [11:06]
> cd lib/functions/

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/lib/functions [git::master *] [oit@ubuntu] [11:06]
> ls
fsck      network.sh    procd.sh    system.sh
leds.sh   preinit.sh   service.sh  uci-defaults.sh

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/lib/functions [git::master *] [oit@ubuntu] [11:06]
>
```

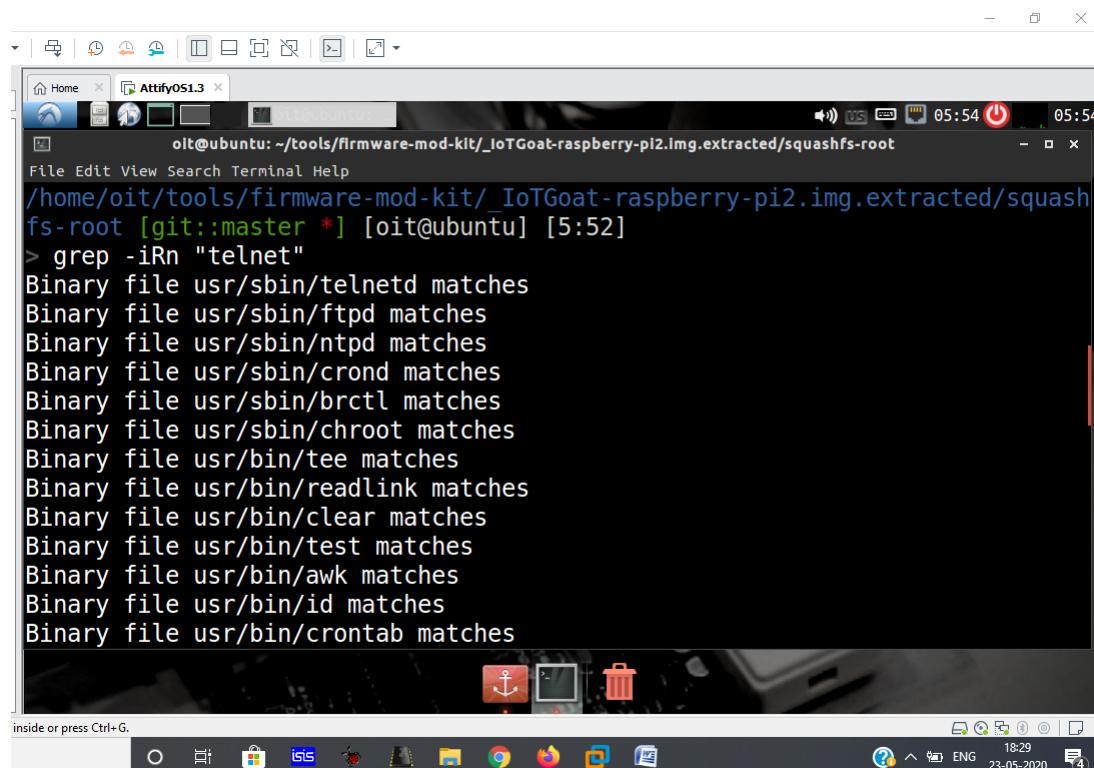
14) Go to /usr/lib/lua/luci/view/iotgoat

We can directly access them on web UI of iotgoat

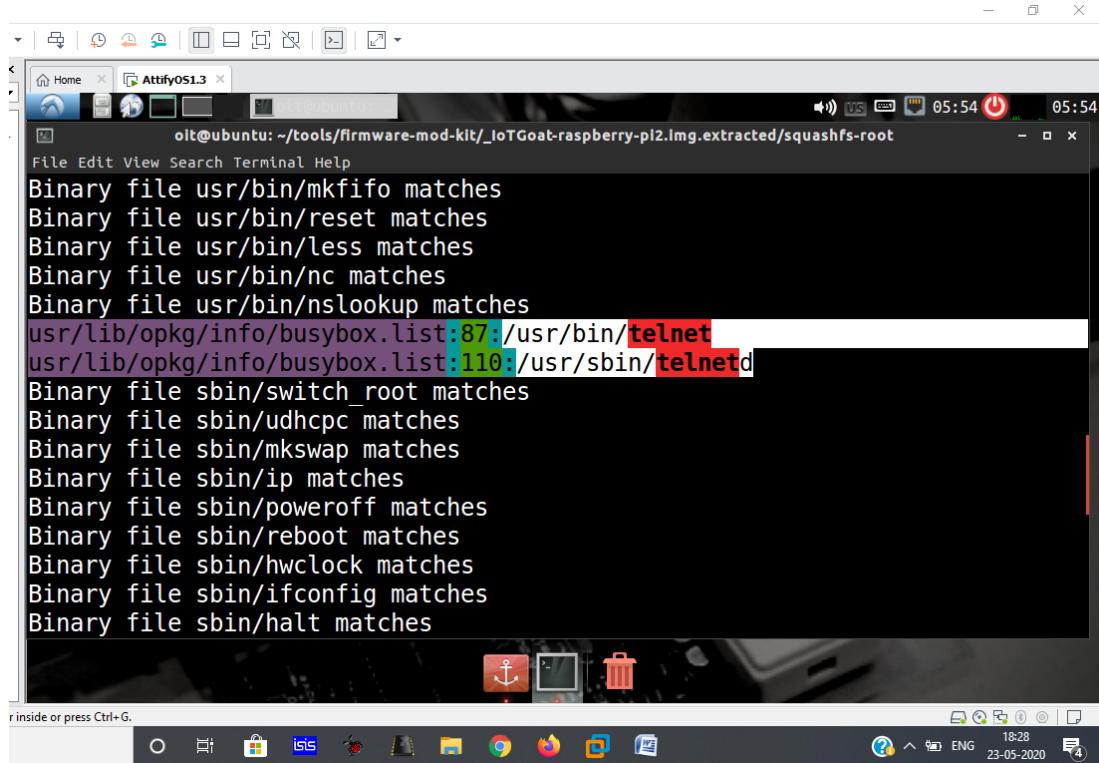


```
olt@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/view/iotgoat ~ x
File Edit View Search Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/functions [git::master *] [oit@ubuntu] [11:06]
> cd ../..
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [11:21]
> cd usr/lib/lua/luci/view/iotgoat
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/view/iotgoat [git::master *] [oit@ubuntu] [11:22]
> ls
camera.htm cmd.htm door.htm
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/lua/luci/view/iotgoat [git::master *] [oit@ubuntu] [11:22]
>
```

15) Grep telnet files we see telnet and telnetd in the following directories listed below



```
olt@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root ~ x
File Edit View Search Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root [git::master *] [oit@ubuntu] [5:52]
> grep -iRn "telnet"
Binary file usr/sbin/telnetd matches
Binary file usr/sbin/ftpd matches
Binary file usr/sbin/ntp matches
Binary file usr/sbin/crond matches
Binary file usr/sbin/brctl matches
Binary file usr/sbin/chroot matches
Binary file usr/bin/tee matches
Binary file usr/bin/readlink matches
Binary file usr/bin/clear matches
Binary file usr/bin/test matches
Binary file usr/bin/awk matches
Binary file usr/bin/id matches
Binary file usr/bin/crontab matches
```



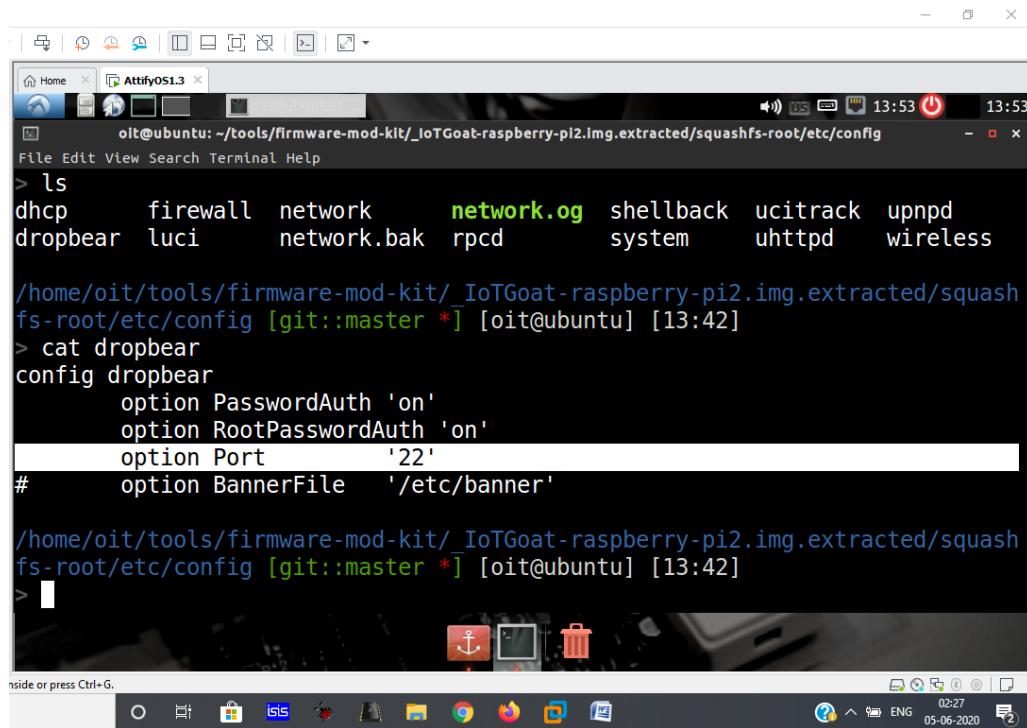
AttifyOS1.3

```
File Edit View Search Terminal Help
Binary file usr/bin/mkfifo matches
Binary file usr/bin/reset matches
Binary file usr/bin/less matches
Binary file usr/bin/nc matches
Binary file usr/bin/nslookup matches
usr/lib/opkg/info/busybox.list:87:/usr/bin/telnet
usr/lib/opkg/info/busybox.list:110:/usr/sbin/telnetd
Binary file sbin/switch_root matches
Binary file sbin/udhcpc matches
Binary file sbin/mkswap matches
Binary file sbin/ip matches
Binary file sbin/poweroff matches
Binary file sbin/reboot matches
Binary file sbin/hwclock matches
Binary file sbin/ifconfig matches
Binary file sbin/halt matches
```

16)we also have dropbear port at 22

Drobear files are located at

```
/usr/sbin/dropbear
/etc/config/dropbear
/etc/init.d/dropbear
```



AttifyOS1.3

```
File Edit View Search Terminal Help
> ls
dhcp      firewall   network      network.og    shellback  ucitrack  upnpd
dropbear   luci       network.bak  rpcd        system     uhttpd    wireless

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/etc/config [git::master *] [oit@ubuntu] [13:42]
> cat dropbear
config dropbear
  option PasswordAuth 'on'
  option RootPasswordAuth 'on'
  option Port      '22'
#  option BannerFile  '/etc/banner'

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/etc/config [git::master *] [oit@ubuntu] [13:42]
>
```

17)we can also get dropbear related files from dropbear.list

AttifyOS1.3

```
oit@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/opkg/info      14:01 14:01
File Edit View Search Terminal Help
libgcc.control          wpad-mini.control
libgcc.list              wpad-mini.list
libgcc.prem           wpad-mini.prem
libgmp.control

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/usr/lib/opkg/info [git::master *] [oit@ubuntu] [14:00]
> cat dropbear.list
/usr/bin/dbclient
/etc/dropbear/dropbear_rsa_host_key
/etc/init.d/dropbear
/usr/bin/dropbearkey
/etc/config/dropbear
/usr/sbin/dropbear

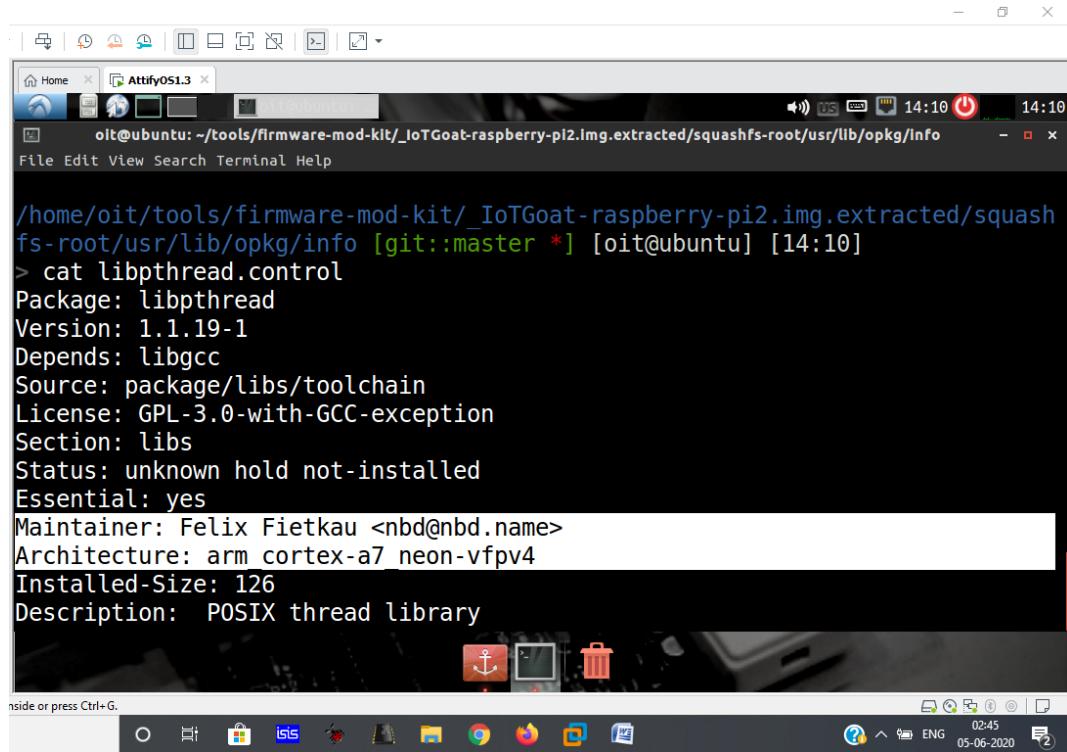
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
```

18)There were many files with email ID too, few are

AttifyOS1.3

```
oit@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/usr/lib/opkg/info [git::master *] [oit@ubuntu] [14:07]
File Edit View Search Terminal Help
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
fs-root/usr/lib/opkg/info [git::master *] [oit@ubuntu] [14:07]
> cat rpcd-mod-rrdns.control
Package: rpcd-mod-rrdns
Version: 20170710
Depends: libc, rpcd, libubox, libubus
Source: feeds/luci/libs/rpcd-mod-rrdns
License: Apache-2.0
Section: libs
Maintainer: Jo-Philipp Wich <jo@mein.io>
Architecture: arm_cortex-a7_neon-vfpv4
Installed-Size: 3367
Description: Provides rapid mass reverse DNS lookup functionality.

/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squash
```



```
Home AttifyOS1.3
File Edit View Search Terminal Help
14:10 14:10
oit@ubuntu: ~/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/opkg/info
/home/oit/tools/firmware-mod-kit/_IoTGoat-raspberry-pi2.img.extracted/squashfs-root/usr/lib/opkg/info [git::master *] [oit@ubuntu] [14:10]
> cat libpthread.control
Package: libpthread
Version: 1.1.19-1
Depends: libgcc
Source: package/libs/toolchain
License: GPL-3.0-with-GCC-exception
Section: libs
Status: unknown hold not-installed
Essential: yes
Maintainer: Felix Fietkau <nbd@nbd.name>
Architecture: arm cortex-a7 neon-vfpv4
Installed-Size: 126
Description: POSIX thread library
```

There was so much of more information present in the firmware we can traverse through.