Practical-3

AIM: Use the Binwalk tool

1. To check Firmware is encrypted

2. To explore filesystem using linux commands

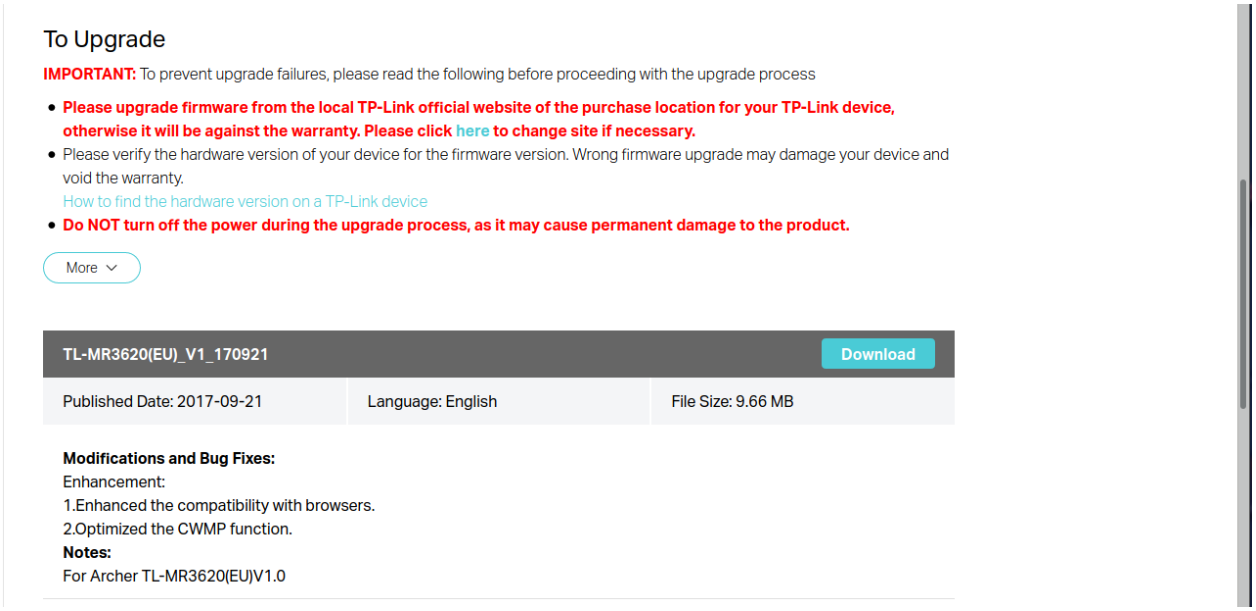
Objective:
Utilize the Binwalk tool to determine if the firmware is encrypted and, if not, explore the extracted filesystem using Linux commands to analyze its contents and structure.

BINWALK:

Binwalk is a powerful open-source tool used for analyzing, extracting, and reverse-engineering firmware images. It is commonly used by security researchers and embedded system developers to inspect firmware for hidden files, encryption, and potential vulnerabilities.

FIRMWARE TL-MR3620:

Step 1 : First download the Firmware **[TL-MR3620]**

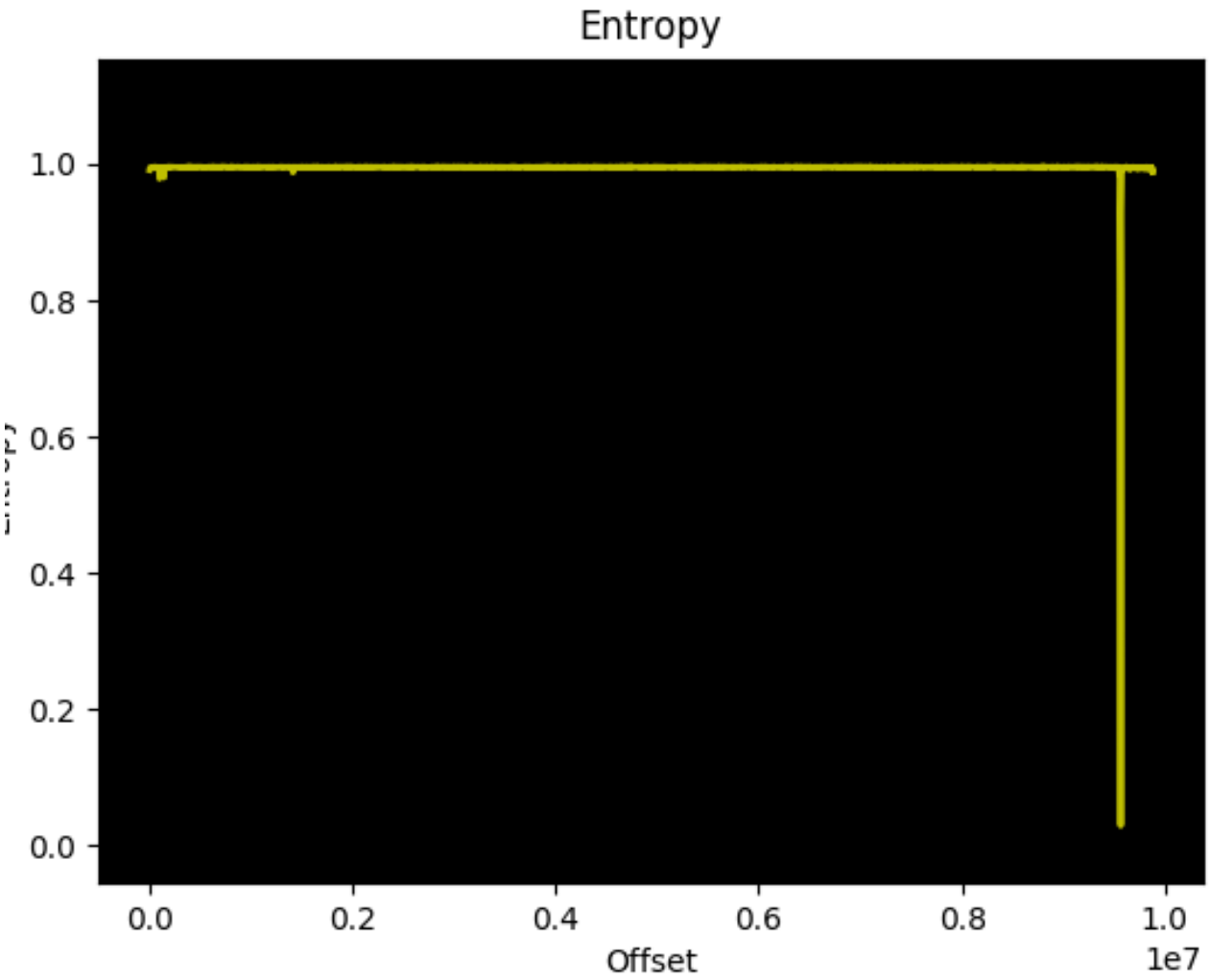


Step 2 : Use Binwalk tools to check whether firmware is encrypted or not type commands like **[binwalk -E (firmware file.zip)]**. Firmware - [TL-MR3620] is not encrypted.

```
iot@attifyos ~> Desktop/
iot@attifyos ~/Desktop> binwalk -E '/home/iot/Downloads/TL-MR3620(EU)_V1_170921.
zip'

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Rising entropy edge (0.991295)
9560064       0x91E000        Falling entropy edge (0.817129)
9575424       0x921C00        Rising entropy edge (0.994398)

(python3:7741): dbind-WARNING **: 20:51:42.042: Error retrieving accessibility b
us address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.a11y.Bus was
 not provided by any .service files
```



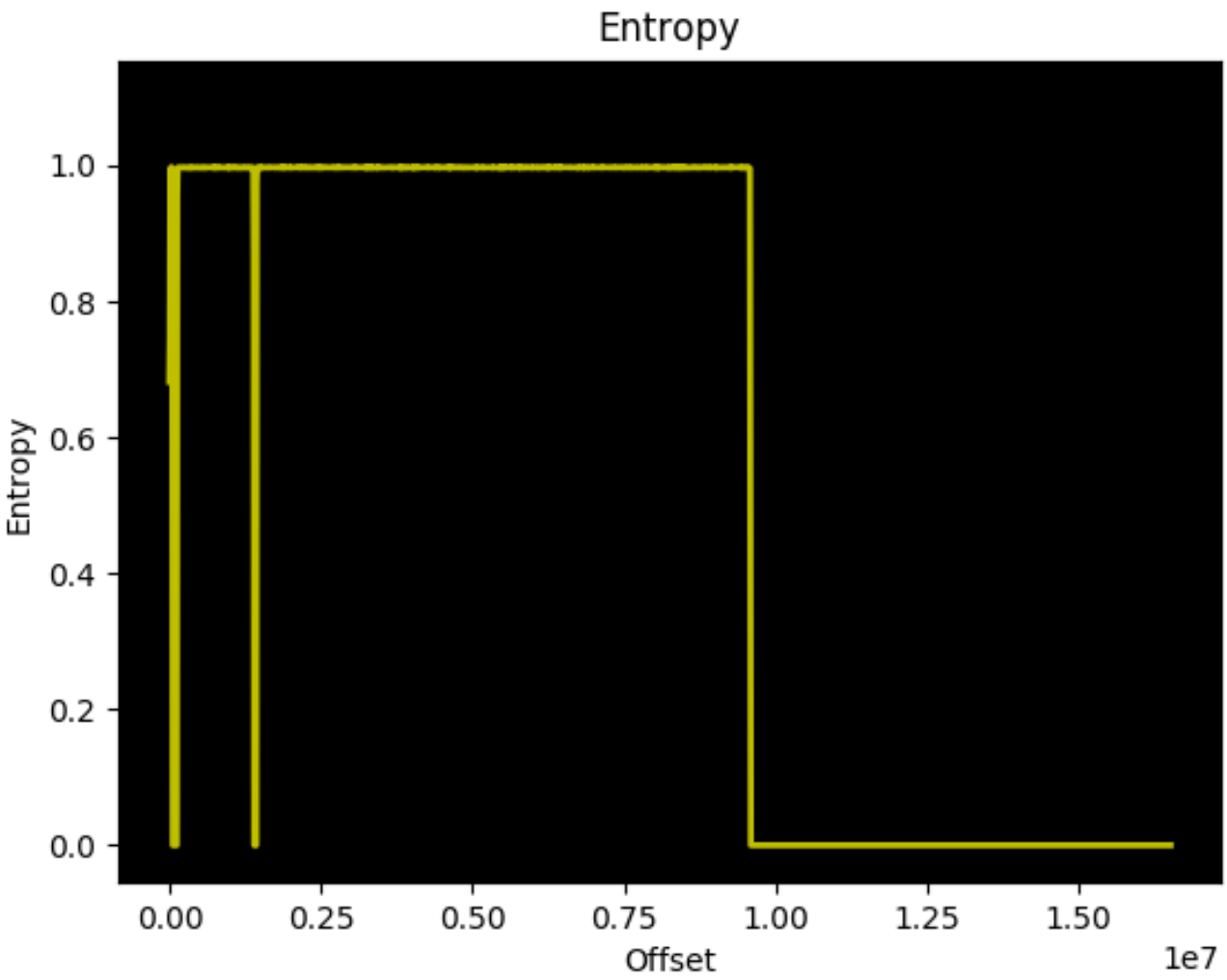
Step 3 : Then do extracted Firmware command type like

[binwalk -E (firmware file.bin)]

```
iot@attifyos ~/Desktop> binwalk -E '/home/iot/Downloads/TL-MR3620v1_1.1.0_0.9.1_
up_boot(170921)_2017-09-21_15.30.50.bin'

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Falling entropy edge (0.681729)
16384         0x4000          Rising entropy edge (0.993286)
57344         0xE000          Falling entropy edge (0.000000)
131072        0x20000         Rising entropy edge (0.956129)
1400832       0x156000        Falling entropy edge (0.000000)
1441792       0x160000        Rising entropy edge (0.973112)
9584640       0x924000        Falling entropy edge (0.562223)

(python3:10302): dbind-WARNING **: 21:00:11.771: Error retrieving accessibility
bus address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.a11y.Bus wa
s not provided by any .service files
```



Step 4 : Then do zip command type like

[binwalk -e (firmware file.zip)]

```
root@attifyos:/home/iot# binwalk -e '/home/iot/Downloads/TL-MR3620(EU)_V1_170921
.zip'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compre
ssed size: 98749, uncompressed size: 112046, name: GPL License Terms.pdf
98800         0x181F0         Zip archive data, at least v2.0 to extract, compre
ssed size: 9472066, uncompressed size: 16515584, name: TL-MR3620v1_1.1.0_0.9.1_u
p_boot(170921)_2017-09-21_15.30.50.bin
9570959       0x920A8F        Zip archive data, at least v2.0 to extract, compre
ssed size: 316289, uncompressed size: 373590, name: How to upgrade TP-LINK Wirel
ess AC Router(New VI).pdf
9887714       0x96DFE2        End of Zip archive, footer length: 22

root@attifyos:/home/iot#
```

Step 5 : Then do bin command type like

[binwalk -e (firmware file.bin)]

```
root@attifyos:/home/iot# binwalk -e '/home/iot/Downloads/TL-MR3620v1_1.1.0_0.9.1_
up_boot(170921)_2017-09-21_15.30.50.bin'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
15648         0x3D20          U-Boot version string, "U-Boot 1.1.4-gff2db3d2-dirt
y (Sep  7 2017 - 16:02:09)"
15712         0x3D60          CRC32 polynomial table, big endian
17016         0x4278          uImage header, header size: 64 bytes, header CRC: 0
xDB7C0DA, created: 2017-09-07 08:02:12, image size: 38979 bytes, Data Address: 0x
80010000, Entry Point: 0x80010000, data CRC: 0xA398C211, OS: Linux, CPU: MIPS, im
age type: Firmware Image, compression type: lzma, image name: "u-boot image"
17080         0x42B8          LZMA compressed data, properties: 0x5D, dictionary
size: 8388608 bytes, uncompressed size: 92052 bytes
132096        0x20400         LZMA compressed data, properties: 0x6D, dictionary
size: 8388608 bytes, uncompressed size: 3712888 bytes
743021        0xB566D         MySQL MISAM index file Version 10
1442304       0x160200        Squashfs filesystem, little endian, version 4.0, co
mpression:xz, size: 8145972 bytes, 638 inodes, blocksize: 262144 bytes, created:
2017-09-21 04:43:03
```

Step 6 : Then [TL-MR3620] we go to this firmware file system using the Linux command. Command type : **cd(extracted file)/ls/cd squashfs-root/ls/cd etc/ls/cat passwd.bak** This file shows to username or password of this firmware

```
root@attifyos:/home/iot# cd '/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-0
9-21_15.30.50.bin.extracted'
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted# ls
160200.squashfs  20400  20400.7z  42B8  42B8.7z  squashfs-root
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted# cd squashfs-root/
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted/squashfs-root# ls
bin  dev  etc  lib  linuxrc  mnt  proc  sbin  sys  tmp  usr  var  web
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted/squashfs-root# cd etc/
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted/squashfs-root/etc# ls
cloud              iptables-stop        ppp                  TZ
default_config.xml  iqos                reduced_data_model.xml  vsftpd.conf
fstab              minidlna.conf        resolv.conf          vsftpd_passwd
group              mode_switch.conf.bin  samba
init.d             passwd               services
inittab            passwd.bak           support_3g_list
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
in.extracted/squashfs-root/etc# cat passwd.bak
admin:$1$$iC.dUsGpxNNJGeOm1dFio/:0:0:root:/:/bin/sh
dropbear:x:500:500:dropbear:/var/dropbear:/bin/sh
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.root
root@attifyos:/home/iot/Desktop/_TL-MR3620v1_1.1.0_0.9.1_up_boot(170921)_2017-09-21_15.30.50.b
```

FIRMWARE DIR-300:

Step 1 : First download the Firmware **[DIR-300]**

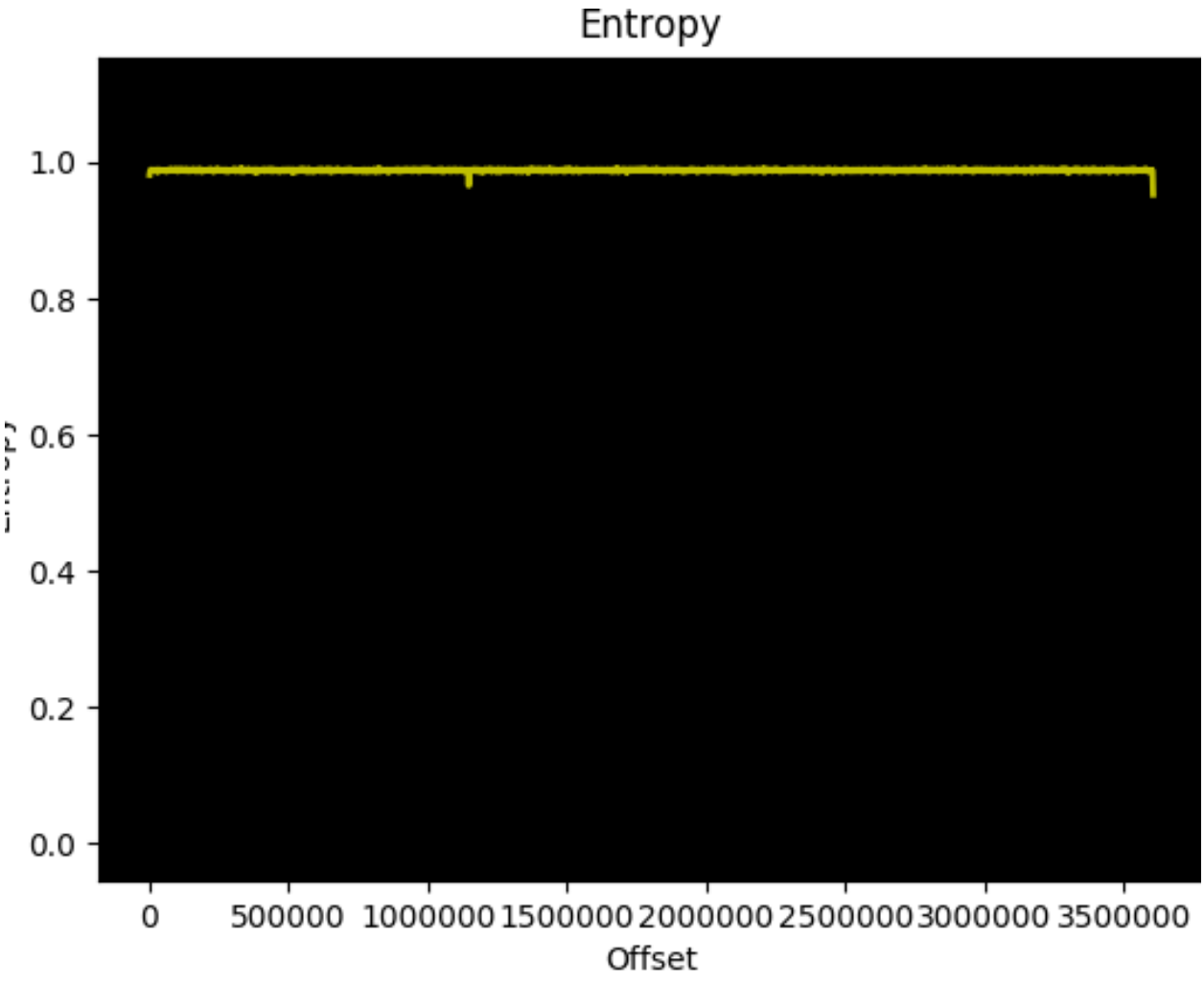
Overview Specifications **Downloads**

No	Description	Title	Type	File Size	
1	Firmware	DIR-300 H/W Ver.D1 F/W Ver. 1.0.11	bin	0 MB	
2	Firmware	DIR-300 A1 F/W v1.04_WW	bin	0 MB	
3	Firmware	DIR-300 Bx FW v2.14	zip	3.61 MB	
4	Datasheet	DIR-300 Datasheet	pdf	1.24 MB	
5	Firmware	DIR-300 B5 FW v2.15	bin	3.64 MB	

Step 2 : Use Binwalk tools to check whether firmware is encrypted or not type commands like **[binwalk -E (firmware file.zip)]**.

```
root@attifyos:/home/iot# binwalk -E '/home/iot/Downloads/DIR_300Bx_FW214WWB04_bi
n_5a72dd6d182f1.zip'

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Rising entropy edge (0.981846)
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

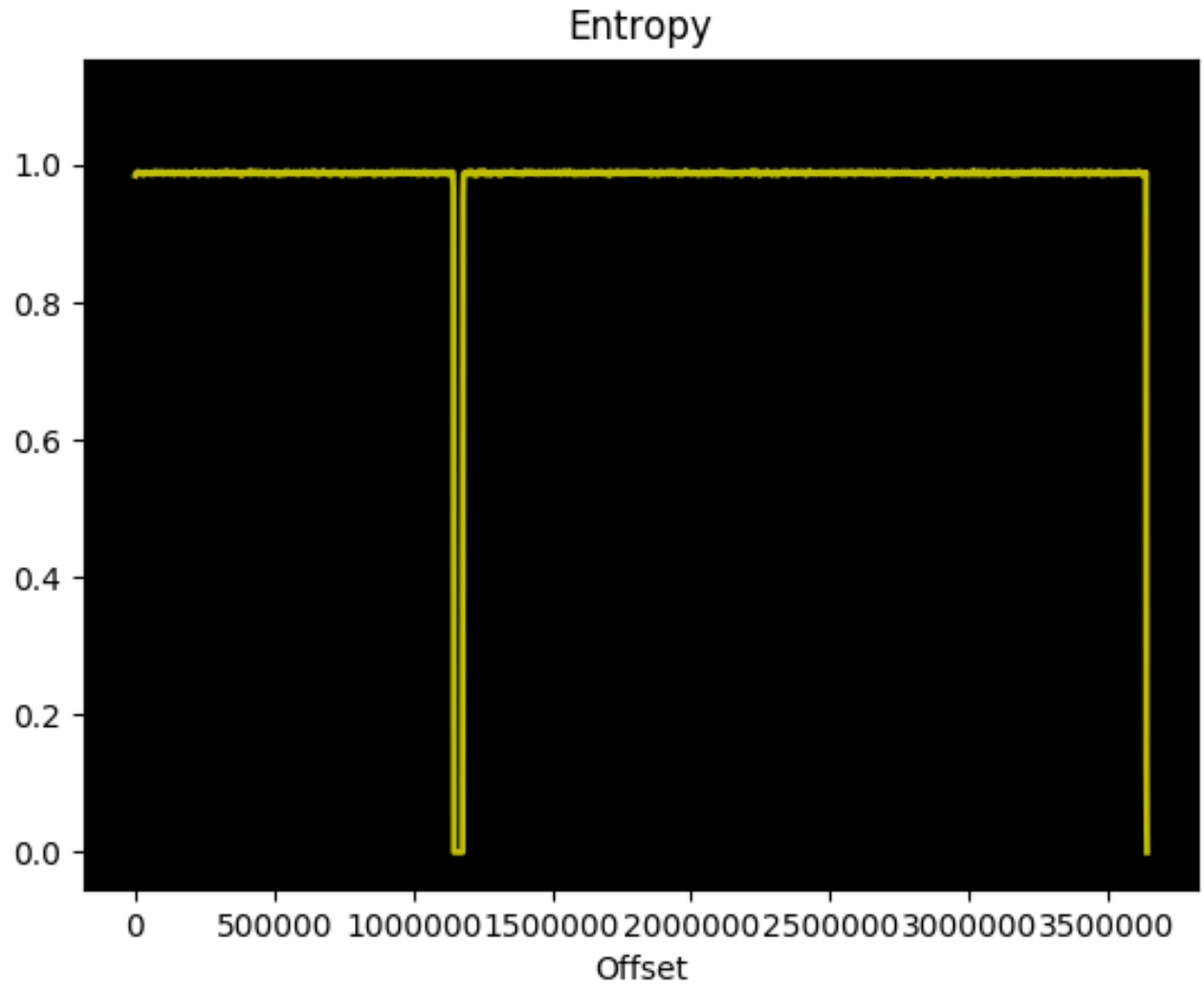


Step 3 : Then do extracted Firmware command type like

[binwalk -E (firmware file.bin)]

```
root@attifyos:/home/iot# binwalk -E '/home/iot/Downloads/DIR-300Bx_FW214WWB04.bi
n'

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Rising entropy edge (0.985033)
1146880       0x118000        Falling entropy edge (0.000000)
1179648       0x120000        Rising entropy edge (0.952699)
3639296       0x378800        Falling entropy edge (0.122303)
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



Step 4 : Then do zip command type like
[binwalk -e (firmware file.zip)]

```
root@attifyos:/home/iot# binwalk -e '/home/iot/Downloads/DIR_300Bx_FW214WWB04_bi
n_5a72dd6d182f1.zip'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, name:
DIR-300Bx_FW214WWB04.bin
75            0x4B            DLOB firmware header, boot partition: "dev=/dev/mt
dblock/2"
3607854       0x370D2E        Zip archive data, at least v1.0 to extract, name:
__MACOSX/
3607909       0x370D65        Zip archive data, at least v2.0 to extract, name:
__MACOSX/._DIR-300Bx_FW214WWB04.bin
3608407       0x370F57        End of Zip archive, footer length: 22
```

Step 5 : Then do bin command type like
[binwalk -e (firmware file.bin)]

```
root@attifyos:/home/iot# binwalk -e '/home/iot/Downloads/DIR-300Bx_FW214WWB04.bi
n'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mt
dblock/2"
108           0x6C            LZMA compressed data, properties: 0x5D, dictionary
 size: 33554432 bytes, uncompressed size: 3479564 bytes
1179756       0x12006C        PackImg section delimiter tag, little endian size:
 9446656 bytes; big endian size: 2461696 bytes
1179788       0x12008C        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 2459698 bytes, 1473 inodes, blocksize: 131072 bytes, crea
ted: 2013-03-29 08:00:49
```

Step 6 : Then [DIR-300] we go to this firmware file system using the Linux command. Command type : **cd(extracted file)/ls/cd squashfs-root/ls/cd etc/ls/**

```
root@attifyos:/home/iot# cd '/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin
.extracted'
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted# ls
12008C.squashfs  6C  6C.7z  squashfs-root
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted# cd
squashfs-root/
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted/squa
shfs-root# ls
bin  dev  etc  home  htdocs  lib  mnt  proc  sbin  sys  tmp  usr  var  www
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted/squa
shfs-root# cd etc/
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted/squa
shfs-root/etc# ls
config    hosts    iproute2     RT5350_AP_1T1R_V1_0.bin  templates
defnodes  init0.d  ppp          scripts                  TZ
events    init.d   resolv.conf  services
root@attifyos:/home/iot/Downloads/_DIR-300Bx_FW214WWB04.bin.extracted/squa
```

Conclusion: In this practical, we know how to download firmware and see firmware encrypted or not and if firmware are not encrypted then how to check the firmware file system using the Linux command.