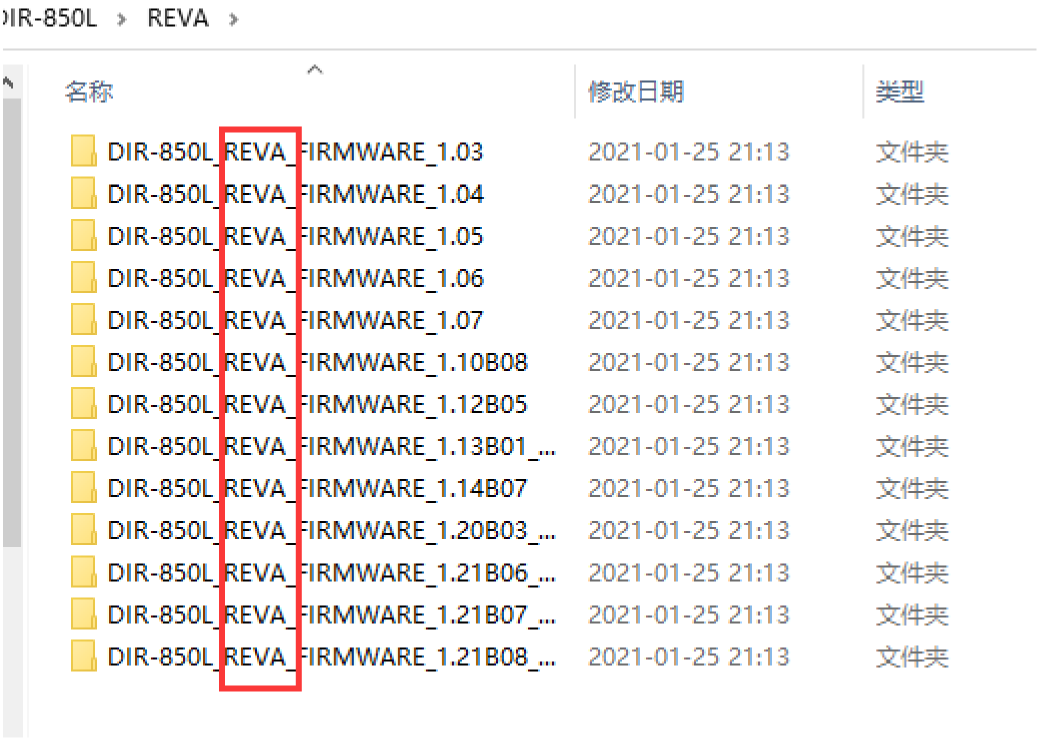
DIR-850L固件解包打包

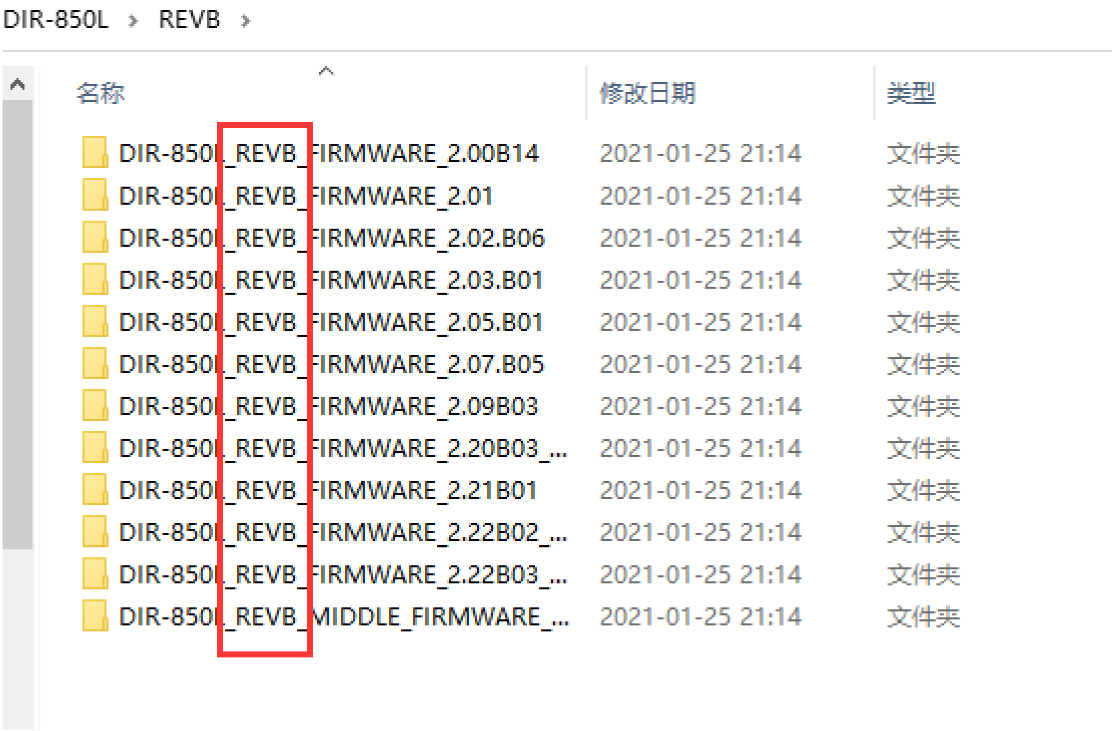
前期分析

在网上下载了DIR-850L的所有固件版本，得知其分为两种硬件型号，A和B



IR-850L › REVA ›

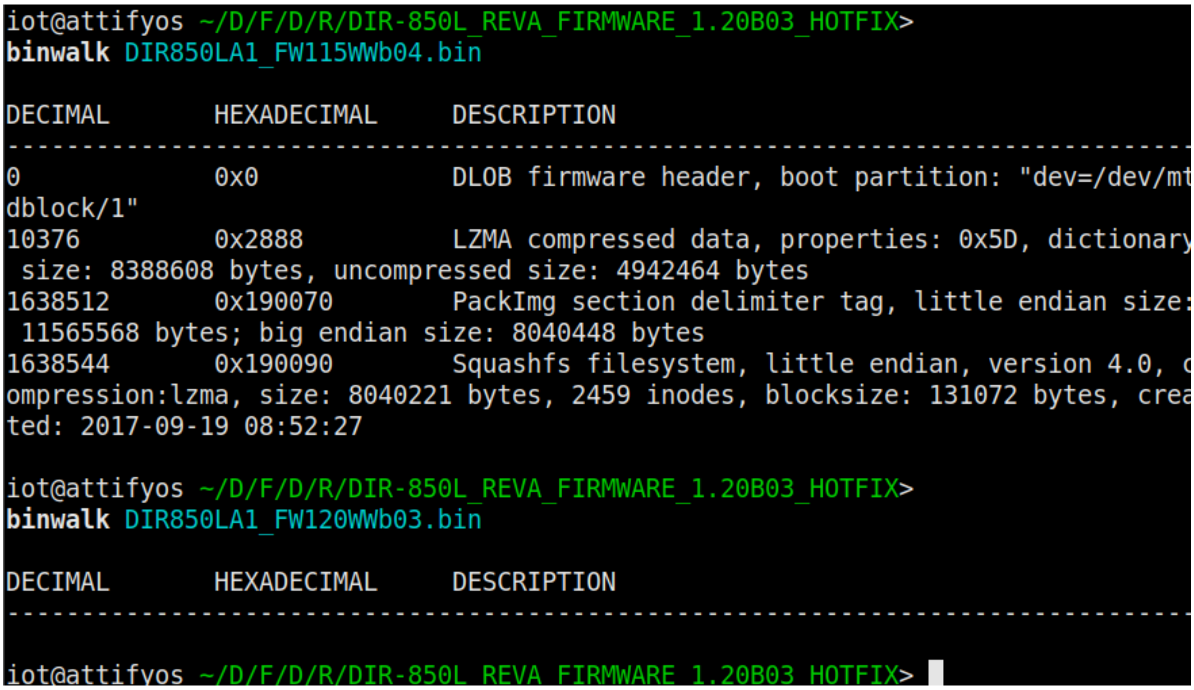
名称	修改日期	类型
DIR-850L_REVA_FIRMWARE_1.03	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.04	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.05	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.06	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.07	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.10B08	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.12B05	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.13B01_...	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.14B07	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.20B03_...	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.21B06_...	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.21B07_...	2021-01-25 21:13	文件夹
DIR-850L_REVA_FIRMWARE_1.21B08_...	2021-01-25 21:13	文件夹



DIR-850L › REVB ›

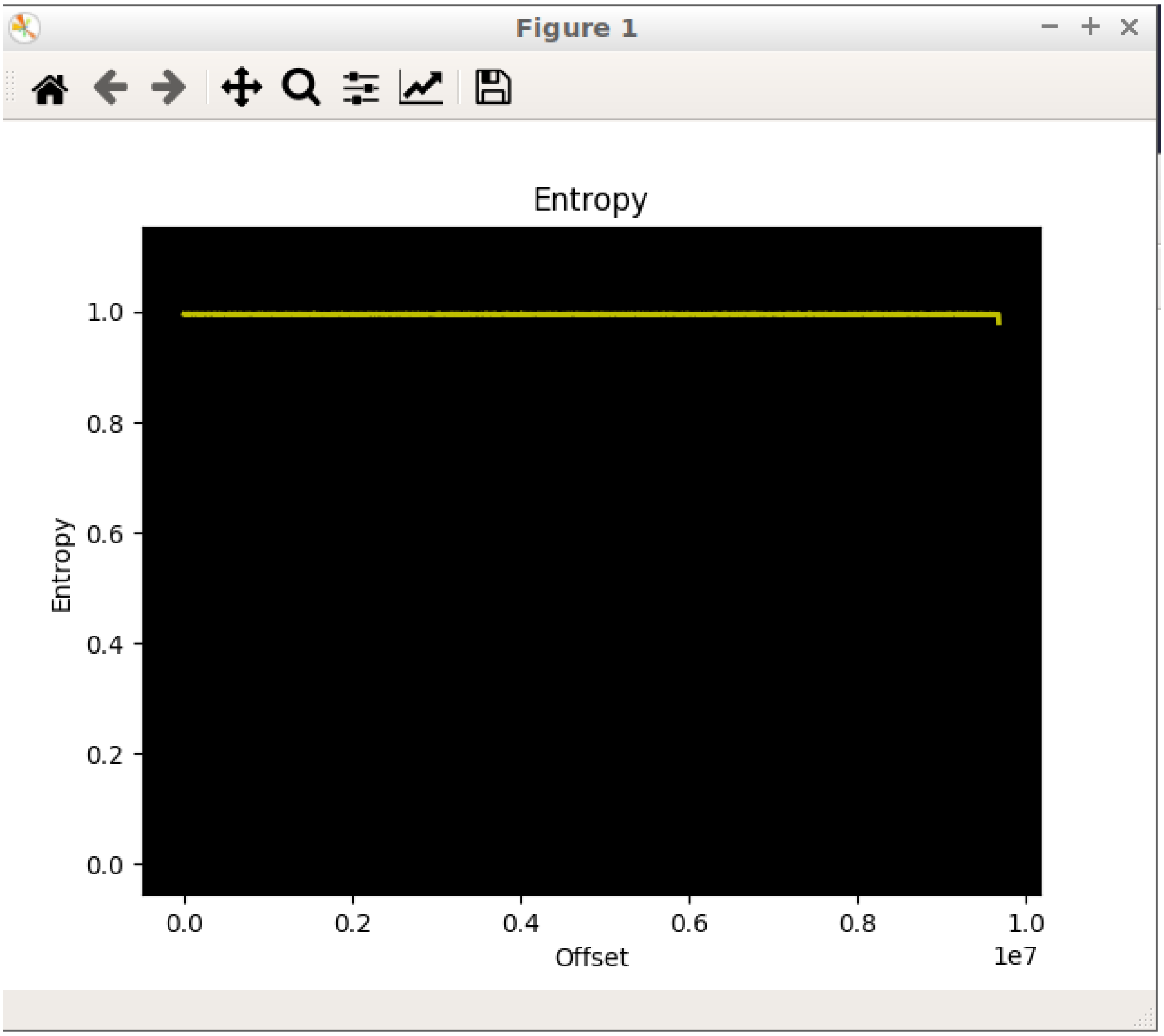
名称	修改日期	类型
DIR-850L_REVB_FIRMWARE_2.00B14	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.02.B06	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.03.B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.05.B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.07.B05	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.09B03	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.20B03_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.21B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.22B02_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.22B03_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_MIDDLE_FIRMWARE_...	2021-01-25 21:14	文件夹

先看A系列，用binwalk从低版本到高版本逐个分析，到`DIR850LA1_FW115WWb04.bin`的时候，是有结果的，再下一个版本，`DIR850LA1_FW120WWb03.bin`是没有结果的

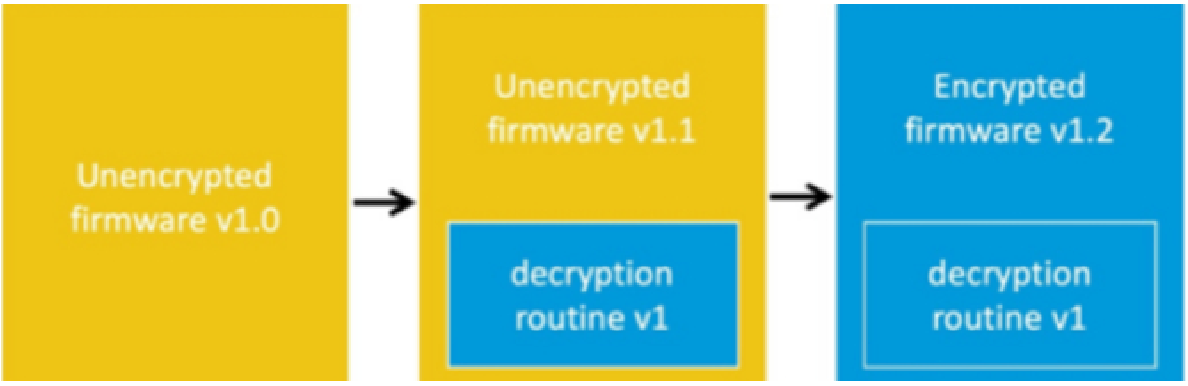


```
iot@attifyos ~/D/F/D/R/DIR-850L_REVA_FIRMWARE_1.20B03_HOTFIX>
binwalk DIR850LA1_FW115WWb04.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mt
dblock/1"
10376         0x2888          LZMA compressed data, properties: 0x5D, dictionary
 size: 8388608 bytes, uncompressed size: 4942464 bytes
1638512       0x190070        PackImg section delimiter tag, little endian size:
 11565568 bytes; big endian size: 8040448 bytes
1638544       0x190090        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 8040221 bytes, 2459 inodes, blocksize: 131072 bytes, crea
ted: 2017-09-19 08:52:27

iot@attifyos ~/D/F/D/R/DIR-850L_REVA_FIRMWARE_1.20B03_HOTFIX>
binwalk DIR850LA1_FW120WWb03.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

iot@attifyos ~/D/F/D/R/DIR-850L_REVA_FIRMWARE_1.20B03_HOTFIX>
```

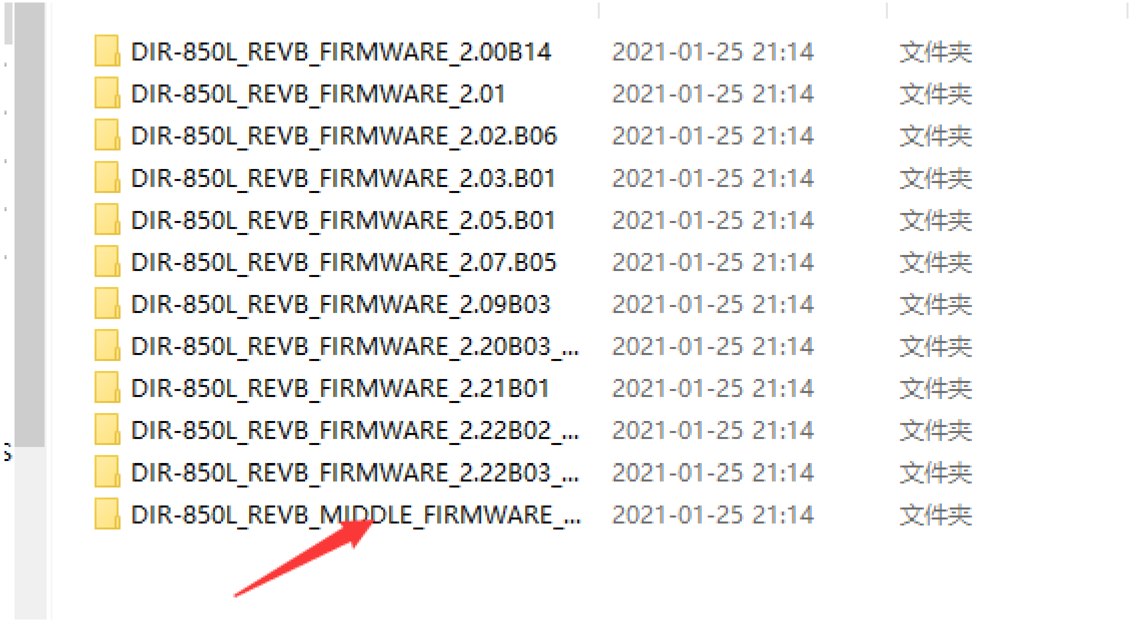
随后试了之后的版本，也是没有结果，那么猜测应该是被加密了，binwalk -E 分析熵值，看到恒为1，确认是加密了。



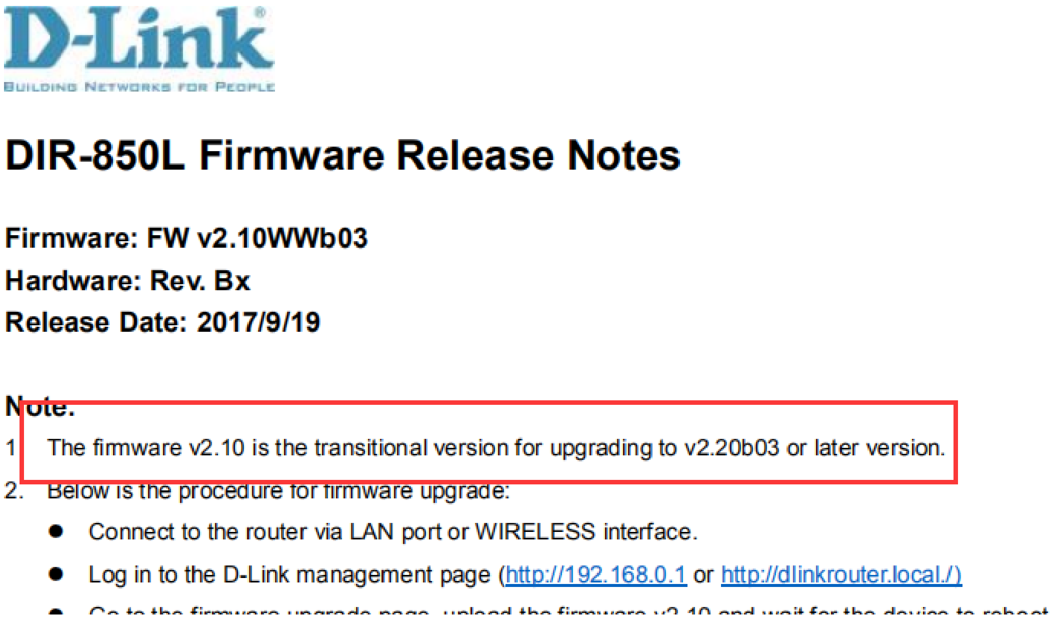
那么A型号符合这种情形：设备固件在出厂时未加密，也未包含任何解密程序。解密程序与较新版本（v1.1）中未加密版本的固件一起提供，以便将来进行加密固件更新。此后发布的固件为加密固件。



再来看B系列，这个型号的固件安全性做得很好，粗略的看了几个，都是加密的，但是有个意外之喜，这个固件有个middle关键字，配套的发行说明也提到这是个过渡版本



DIR-850L_REVB_FIRMWARE_2.00B14	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.02.B06	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.03.B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.05.B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.07.B05	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.09B03	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.20B03_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.21B01	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.22B02_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_FIRMWARE_2.22B03_...	2021-01-25 21:14	文件夹
DIR-850L_REVB_MIDDLE_FIRMWARE_...	2021-01-25 21:14	文件夹



D-Link
BUILDING NETWORKS FOR PEOPLE

DIR-850L Firmware Release Notes

Firmware: FW v2.10WWb03
Hardware: Rev. Bx
Release Date: 2017/9/19

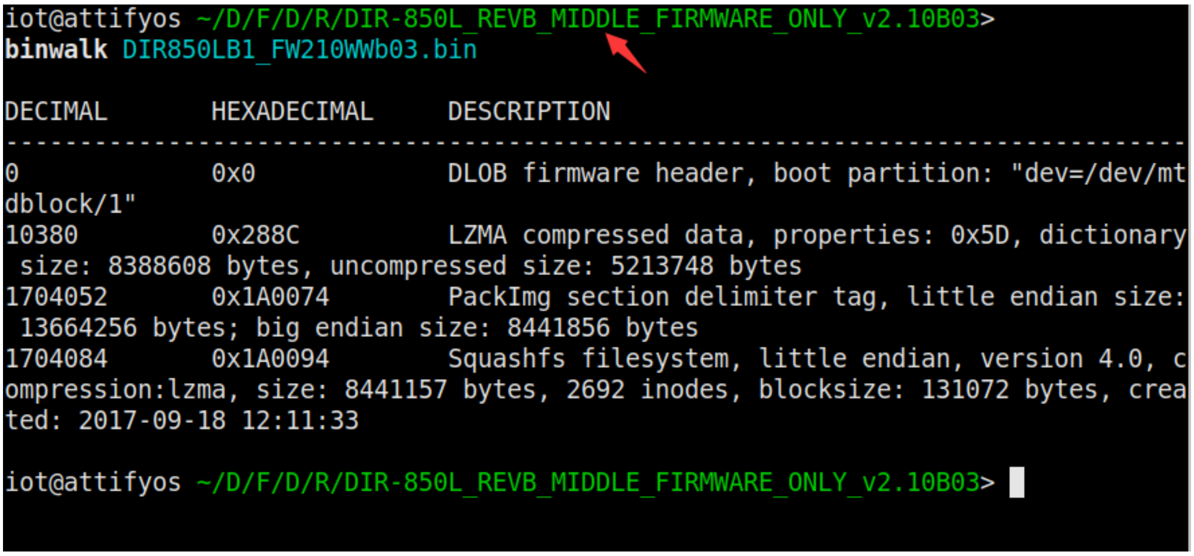
Note:

1 The fimware v2.10 is the transitional version for upgrading to v2.20b03 or later version.

2. Below is the procedure for firmware upgrade:

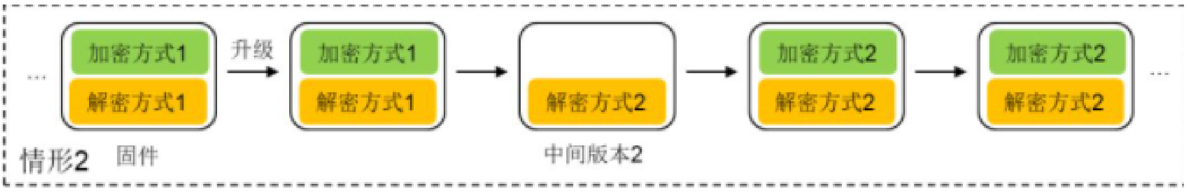
- Connect to the router via LAN port or WIRELESS interface.
- Log in to the D-Link management page (http://192.168.0.1 or http://dlinkrouter.local./)
- Go to the firmware upgrade page, upload the firmware v2.10 and wait for the device to reboot

使用binwalk分析一下，是可以拿到文件系统的



```
iot@attifyos ~/D/F/D/R/DIR-850L_REVB_MIDDLE_FIRMWARE_ONLY_v2.10B03>
binwalk DIR850LB1_FW210WWb03.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mt
dblock/1"
10380         0x288C          LZMA compressed data, properties: 0x5D, dictionary
 size: 8388608 bytes, uncompressed size: 5213748 bytes
1704052       0x1A0074        PackImg section delimiter tag, little endian size:
 13664256 bytes; big endian size: 8441856 bytes
1704084       0x1A0094        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 8441157 bytes, 2692 inodes, blocksize: 131072 bytes, crea
ted: 2017-09-18 12:11:33

iot@attifyos ~/D/F/D/R/DIR-850L_REVB_MIDDLE_FIRMWARE_ONLY_v2.10B03>
```

存在某个中间版本的固件，其自身没有加密，内部提供方式 2 进行解密。这就是过渡版本

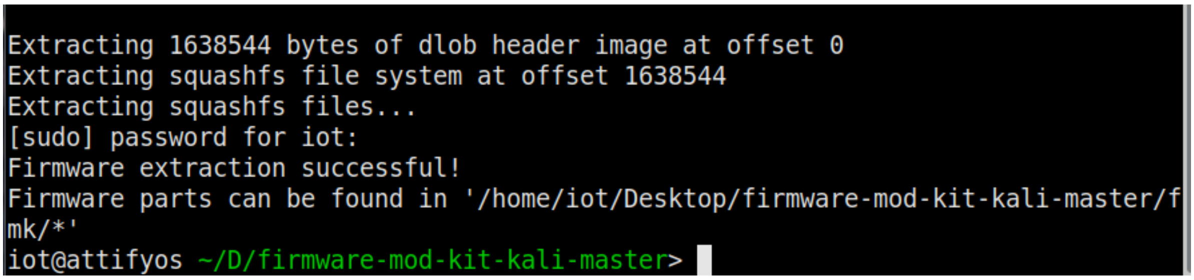


在https://pierrekim.github.io/blog/2017-09-08-dlink-850l-mydlink-cloud-0days-vulnerabilities.html一文中介绍了如何解密850L固件，这个在后边做一演示。

解包打包未加密固件（FMK工具）

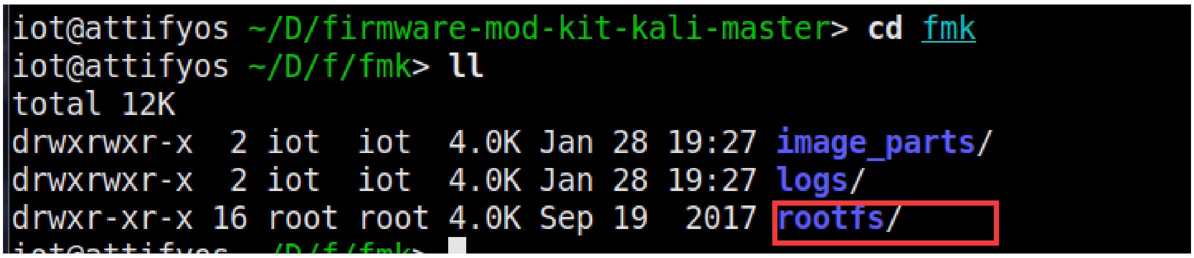
在FMK工具目录下，执行命令，解开固件包

```
./extract-firmware.sh /home/iot/Desktop/FIRMWARE/DIR-850L/REVA/DIR-850L_REVA_FIRMWARE_1.20B03_HOTFIX/DIR850LA1_FW115WWb04.bin  #固件路径
```



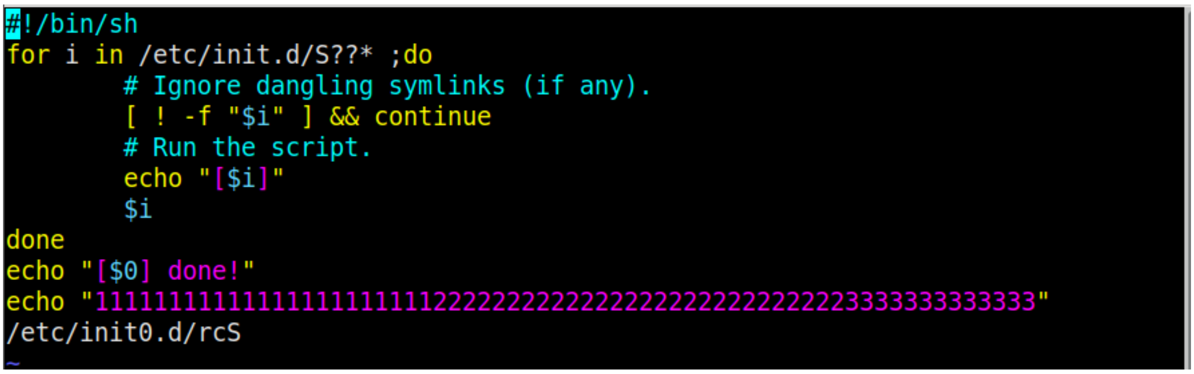
```
Extracting 1638544 bytes of dlob header image at offset 0
Extracting squashfs file system at offset 1638544
Extracting squashfs files...
[sudo] password for iot:
Firmware extraction successful!
Firmware parts can be found in '/home/iot/Desktop/firmware-mod-kit-kali-master/f
mk/*'
iot@attifyos ~/D/firmware-mod-kit-kali-master>
```

在fmk目录下，有三个文件夹，rootfs为文件系统



```
iot@attifyos ~/D/firmware-mod-kit-kali-master> cd fmk
iot@attifyos ~/D/f/fmk> ll
total 12K
drwxrwxr-x  2 iot  iot  4.0K Jan 28 19:27 image_parts/
drwxrwxr-x  2 iot  iot  4.0K Jan 28 19:27 logs/
drwxr-xr-x 16 root root 4.0K Sep 19  2017 rootfs/
iot@attifyos ~/D/f/fmk>
```

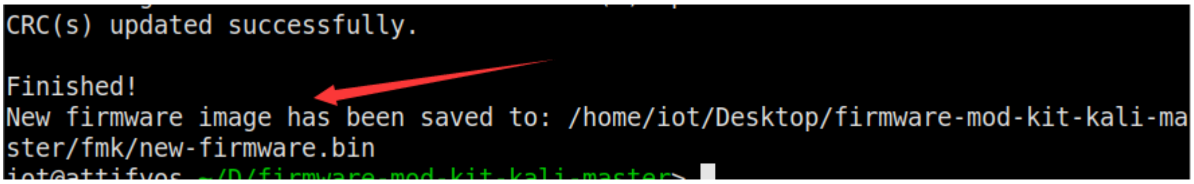
修改启动文件rootfs/etc/init.d/rcS



```
#!/bin/sh
for i in /etc/init.d/S??* ;do
        # Ignore dangling symlinks (if any).
        [ ! -f "$i" ] && continue
        # Run the script.
        echo "[$i]"
        $i
done
echo "[$0] done!"
echo "1111111111111111111111112222222222222222222222222222222222223333333333333"
/etc/init0.d/rcS
~
```

随后在fmk工具目录下输入

```
./build-firmware.sh -min
```



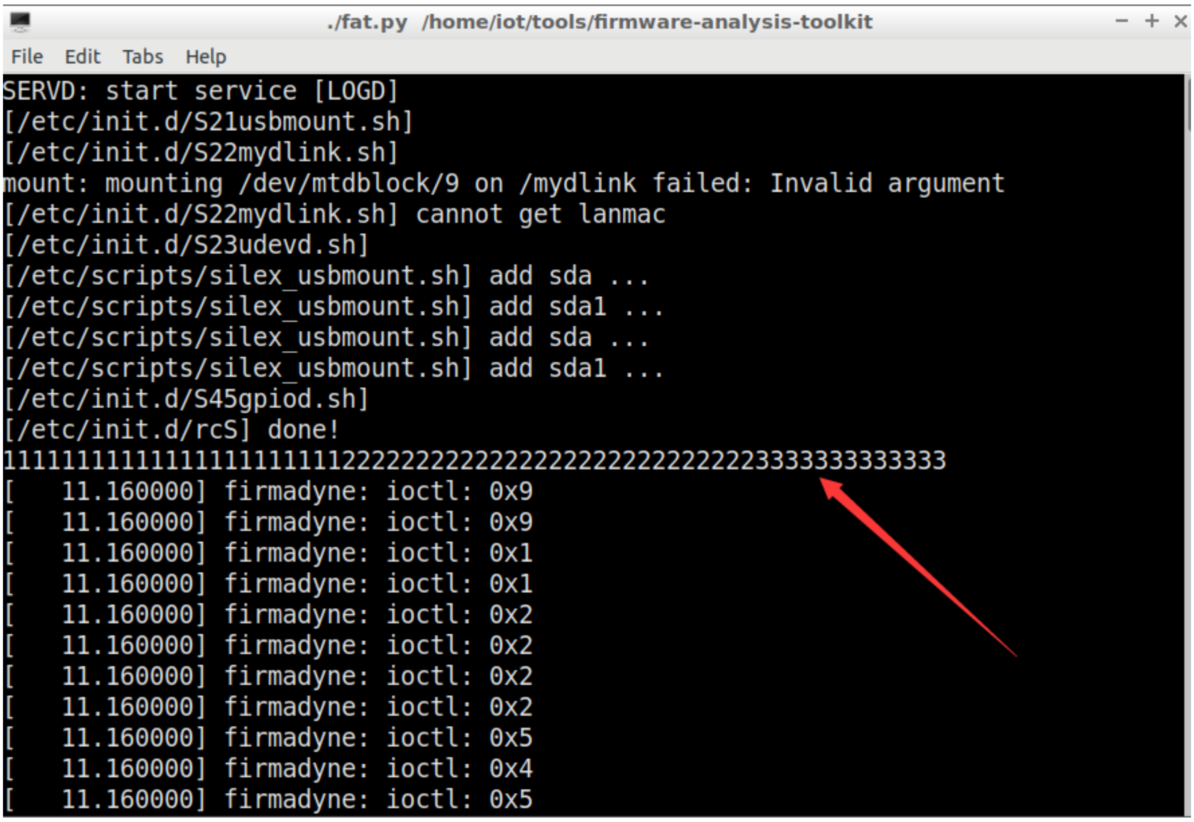
```
CRC(s) updated successfully.

Finished!
New firmware image has been saved to: /home/iot/Desktop/firmware-mod-kit-kali-ma
ster/fmk/new-firmware.bin
iot@attifyos ~/D/firmware-mod-kit-kali-master>
```

在fmk目录下已经生成了新固件，用binwalk解一下包，可以看到rcS文件已经修改

```
binwalk -e new-firmware.bin
```

使用fat工具包（firmware-analysis-toolkit）模拟new-firmware.bin,看到输出了改的东西

```
./fat.py /home/iot/Desktop/firmware-mod-kit-kali-master/fmk/new-firmware.bin
```



```
SERVD: start service [LOGD]
[/etc/init.d/S21usbmount.sh]
[/etc/init.d/S22mydlink.sh]
mount: mounting /dev/mtdblock/9 on /mydlink failed: Invalid argument
[/etc/init.d/S22mydlink.sh] cannot get lanmac
[/etc/init.d/S23udevd.sh]
[/etc/scripts/silex_usbmount.sh] add sda ...
[/etc/scripts/silex_usbmount.sh] add sda1 ...
[/etc/scripts/silex_usbmount.sh] add sda ...
[/etc/scripts/silex_usbmount.sh] add sda1 ...
[/etc/init.d/S45gpiod.sh]
[/etc/init.d/rcS] done!
1111111111111111111111112222222222222222222222222222222222223333333333333
[   11.160000] firmadyne: ioctl: 0x9
[   11.160000] firmadyne: ioctl: 0x9
[   11.160000] firmadyne: ioctl: 0x1
[   11.160000] firmadyne: ioctl: 0x1
[   11.160000] firmadyne: ioctl: 0x2
[   11.160000] firmadyne: ioctl: 0x2
[   11.160000] firmadyne: ioctl: 0x2
[   11.160000] firmadyne: ioctl: 0x2
[   11.160000] firmadyne: ioctl: 0x5
[   11.160000] firmadyne: ioctl: 0x4
[   11.160000] firmadyne: ioctl: 0x5
```

解密固件

REVB型号在过渡版本之前，也就是直到DIR-850L_REVB_FIRMWARE_2.09B03/DIR850LB1_FW209WWb03.bin，都采用的是同一种加密解密方法

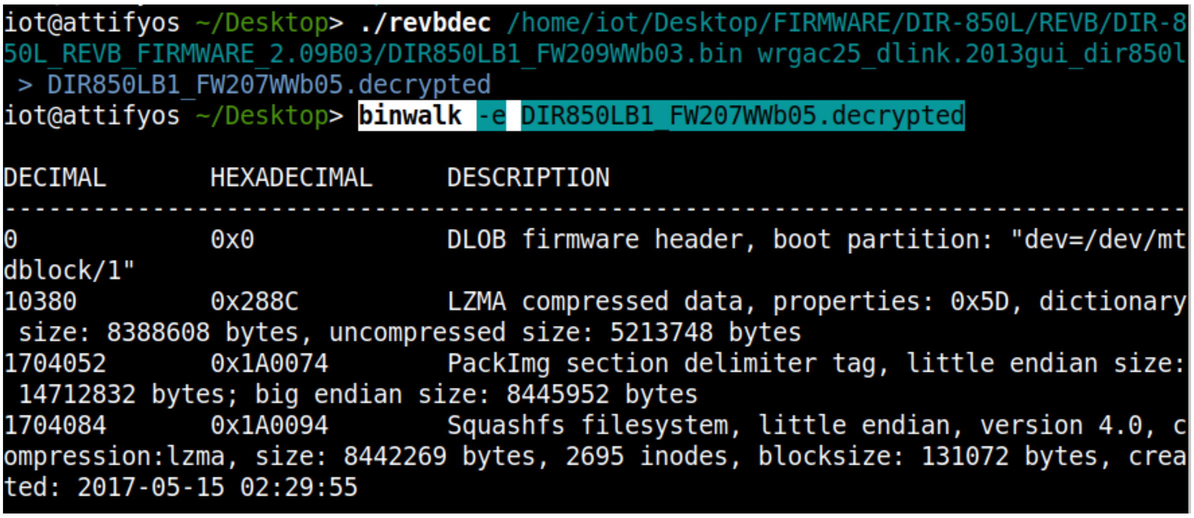
加密程序

```
/*
 * Simple tool to decrypt D-LINK DIR-850L REVB firmwares
 *
 * $ gcc -o revbdec revbdec.c
 * $ ./revbdec DIR850L_REVB_FW207WWb05_h1ke_beta1.bin
wrgac25_dlink.2013gui_dir850l > DIR850L_REVB_FW207WWb05_h1ke_beta1.decrypted
 */

#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#define USAGE "Usage: decimg <filename> <key>\n"

int main(int    argc,
         char   **argv)
{
        int     i, fi;
        int     fo = STDOUT_FILENO, fe = STDERR_FILENO;

        if (argc != 3)
        {
                write(fe, USAGE, strlen(USAGE));
                return (EXIT_FAILURE);
        }

        if ((fi = open(argv[1], O_RDONLY)) == -1)
        {
                perror("open");
                write(fe, USAGE, strlen(USAGE));
                return (EXIT_FAILURE);
        }

        const char *key = argv[2];
        int kl = strlen(key);

        i = 0;
        while (1)
        {
                char buffer[4096];
                int j, len;
                len = read(fi, buffer, 4096);
                if (len <= 0)
                        break;
                for (j = 0; j < len; j++) {
                        buffer[j] ^= (i + j) % 0xFB + 1;
                        buffer[j] ^= key[(i + j) % kl];
                }
                write(fo, buffer, len);
                i += len;
        }

       return (EXIT_SUCCESS);
}
```

编译一下，解密，尝试用binwalk解包

```
gcc -o revbdec revbdec.c  #编译
./revbdec DIR850LB1_FW209WWb03.bin wrgac25_dlink.2013gui_dir850l >
DIR850LB1_FW207WWb05.decrypted   #解密
binwalk -e DIR850LB1_FW207WWb05.decrypted   #解包
```

成功拿到文件系统，同理也可以用FMK工具解包打包，但是要刷进路由器，还需要再用同样的算法加密，这里暂时还没有实现加密。



```
iot@attifyos ~/Desktop> ./revbdec /home/iot/Desktop/FIRMWARE/DIR-850L/REVB/DIR-8
50L_REVB_FIRMWARE_2.09B03/DIR850LB1_FW209WWb03.bin wrgac25_dlink.2013gui_dir850l
 > DIR850LB1_FW207WWb05.decrypted
iot@attifyos ~/Desktop> binwalk -e DIR850LB1_FW207WWb05.decrypted

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mt
dblock/1"
10380         0x288C          LZMA compressed data, properties: 0x5D, dictionary
 size: 8388608 bytes, uncompressed size: 5213748 bytes
1704052       0x1A0074        PackImg section delimiter tag, little endian size:
 14712832 bytes; big endian size: 8445952 bytes
1704084       0x1A0094        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 8442269 bytes, 2695 inodes, blocksize: 131072 bytes, crea
ted: 2017-05-15 02:29:55
```

其他加密的版本解密方式个人暂时还没有实现，查阅资料中。