

```
e:\Settings\downloads$ binwalk 4m.bin

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
13680        0x3570       U-Boot version string, "U-Boot 1.1.4 (Jul  8 2014 - 17:52:55)"
13728        0x35A0       CRC32 polynomial table, big endian
15016        0x3AA8       uImage header, header size: 64 bytes, header CRC: 0x8FC3AF98, created: 2014-07-08 09:52:55
, image size: 34735 bytes, Data Address: 0x80010000, Entry Point: 0x80010000, data CRC: 0x26216032, OS: Linux, CPU: MIPS
, image type: Firmware Image, compression type: lzma, image name: "u-boot image"
15080        0x3AE8       LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size
: 90860 bytes
131584       0x20200      LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size:
3556396 bytes
1308192      0x13F620     Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2196018 bytes, 1102
inodes, blocksize: 262144 bytes, created: 2016-02-02 11:57:02
3538944      0x360000     JFFS2 filesystem, big endian
```

Binwalk là một công cụ cho phép mình phân tích một hoặc nhiều tập tin. Nó cho phép mình nhận dạng tập tin hoặc những đoạn code được nhúng vào trong Firmware. Binwalk sử dụng thư viện libmagic, vì vậy nó tương thích với các [Magic Signature](#) được tạo ra cho tiện ích tập tin Unix.

Mình chỉ mới làm quen với chương trình này được khoảng thời gian rất ngắn nhưng mình thấy nó thật sự hữu ích cho ai muốn tìm hiểu phân tích Firmware.

Thông tin chi tiết về nó các bạn có thể truy cập vào:

Trang chủ: <http://binwalk.org>

Git: <https://github.com/ReFirmLabs/binwalk>

Cài đặt: <https://github.com/ReFirmLabs/binwalk/blob/master/INSTALL.md>

Trích xuất các tập tin từ Kernel của Box FPT

Đầu tiên các bạn tải Kernel về bằng cách truy cập vào địa chỉ sau đây:

<http://fbox-fw.fpt.vn/rom8675B00/v2.3.41/FPT-KERNEL.bin> (phiên bản này hình như hơi cũ thì phải,, nhưng mình nghĩ FPT nó không update cái Kernel này làm gì,, có thì nó chỉ update Apps thôi.)

Sau khi tải về và lưu ở đâu đó, của mình thì lưu tại /Downloads, các bạn thử dùng Binwalk phân tích xem thế nào, mình thử phân tích thì nó như hình dưới.

```
epubc@xx:~/Downloads$ binwalk FPT-KERNEL.bin

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          romfs filesystem, version 1 size: 9262048 bytes, named "MIPSLINUX_XLOAD"
```

Như vậy tập tin FPT-KERNEL.bin thực chất là một file ảnh (romfs dạng một phân vùng có tên là MIPSLINUX_XLOAD). Để chắc ăn mình thử mở bằng 010 Editor xem thế nào và hình dưới cũng cho mình kết quả y chang như Binwalk phân tích.

```

Edit As: Hex Run Script Run Template: ROMFS.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 2D 72 6F 6D 31 66 73 2D 00 0D 53 E0 BA FD E6 59 -romifs-..Sa0yaY
0010h: 4D 49 50 53 4C 49 4E 55 58 5F 58 4C 4F 41 44 00 MIPS_LINUX_XLOAD.
0020h: 00 00 00 49 00 00 00 20 00 00 00 00 D1 FF FF 97 ...I...Nyy-
0030h: 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....NNye
0040h: 00 00 00 60 00 00 00 20 00 00 00 00 D1 D1 FF 80 .....SHx0b+
0050h: 2E 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 vmlinux_xload.zb
0060h: 00 00 00 02 00 00 00 00 00 0D 53 48 D7 F4 DE 2B f.....
0070h: 76 6D 6C 69 6E 75 78 5F 78 6C 6F 61 64 2E 7A 62 FNIB.....
0080h: 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..ú#....(S....
0090h: 49 42 11 01 00 10 00 00 00 84 90 7E 00 84 ..ÿ...ÿÿ.e.z3
00A0h: B8 F9 23 9E 00 00 05 02 28 53 8D 00 00 00 00 00 {°.uâq1*.It;\b-
00B0h: 03 01 01 FF 00 00 04 01 FF FF 1F 00 65 B8 7A 33 Úsé.}Zep(900"¥¶¶
00C0h: 7B B0 02 75 E3 71 ED 2A B7 CC 86 3B 5C DE AD 94 ,N`W0y@Iu.?.d.,|
00D0h: DC 73 E9 19 7D 5A A2 70 28 39 F5 FB 93 A5 B6 B6 ñ;08>ú-Æn¶'A'-.p
00E0h: 82 4E 88 57 F3 79 A9 CF FA 8F 3F 0F 64 03 82 A6 és.bÂÿ.p#[.0x.a`
00F0h: F1 3B DA 38 9B FA 97 C6 6E B6 91 C5 92 AD 13 DE 0| °y.+Fw..j0 <§
0100h: E9 73 9D 62 C2 86 11 DE 23 5B 8D F8 AB 1A 61 88 Iá +61.@Q0{7a..
0110h: 4F 7C 20 BA 79 9D F7 46 77 16 09 6A D4 A0 3C A7 ?3qA0.e.enÿd²áo
0120h: CF E1 AF 20 2B 36 EC 07 A9 51 F6 7B 37 E1 1E 1C af=...gc00ta."y
0130h: A6 3F 33 71 C3 D6 16 E8 85 65 F1 FD 64 B2 E2 F3 .yie.4A:(RF«0Uæ0
0140h: E4 66 3D 1D 90 13 67 63 D2 F5 74 E6 0B AF 23 79 .,?.%s5)f³A¶b%
0150h: 15 79 EF 65 2E BC C4 3A 28 52 46 AB D9 D9 E6 D2 æ0ñ%1)ÇB.36µ1 ¶0
0160h: 90 2C 3F 1A 0C B2 25 9A 35 29 83 B3 C3 B6 62 89 v.ÆL7...µV#6...[ÐÇ
0170h: 9C 4F F1 25 EC 29 C7 DF 7F 33 36 B5 6C 60 B6 F5 -ú)ey'bfÇ°YB#HÁ+
0180h: 76 0C C6 89 4C 37 04 85 B5 56 23 36 85 5B D0 C7 saU.0[JIo³].0±.L
0190h: AC FA 29 65 79 27 DE 83 C7 BA 9F 42 C6 48 C3 2B %~*.J..|æçü....
01A0h: 73 E4 55 9D D5 5B 4A CC 6F B3 5D B7 D8 87 1A 4C .....
01B0h: BE 98 95 0B 4A 0A 07 A6 D7 E6 E7 FA 00 00 00 00 .....
01C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
01F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0230h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0240h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0250h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0260h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0270h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0280h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Oái,,, hình như phân vùng này còn chứa một file gì đó với định dạng .zbf (vmlinux_xload.zbf). Chắc hẳn nhất là thử mount vào /tmp để xem thôi.

```

epubc@xx:~/Downloads$ ls /tmp
vmlinux_xload.zbf

```

Rồi,, y rằng. Mở sao đây? Binwalk chứ sao.

```

epubc@xx:~/Downloads$ binwalk vmlinux_xload.zbf
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          ZBOOT firmware header, header size: 32 bytes, load address: 0x84000000, start address: 0x84007E90, checksum: 0x9E23F988, version: 0x02050000, image size: 9261804 bytes
1896         0x768       gzip compressed data, maximum compression, from Unix, last modified: 1970-01-01 00:00:00 (null date)

```

Như vậy nhìn vào những gì Binwalk phân tích thì ta thấy file này chứa ZBOOT và tại offset 0x768 có chứa dữ liệu nén bằng gzip. mình không quan tâm tới offset chứa ZBOOT mà chỉ quan tâm tới phần data gzip kia thôi. Trích xuất nó ra xem thế nào.

```

// epubc@xx:~/Downloads$ dd if=vmlinux_xload.zbf of=1896.gz bs=1896 skip=1
1896+1 records in
1896+1 records out
9260800 bytes (9.3 MB, 8.8 MiB) copied, 0.0238957 s, 388 MB/s

```

Nếu như may mắn thì mình có thể giải nén được data này ra và xem trong đó là cái gì.

```

9260800 bytes (9.3 MB, 8.8 MiB) copied, 0.0220007 s, 421 MB/s
epubc@xx:~/Downloads$ gzip -d 1896.gz
gzip: 1896.gz: decompression OK, trailing garbage ignored

```

Có vẻ giải nén ra được rồi nhưng không có gì cả,, chỉ là 1 file không tên tuổi.



Mình thử dump string xem có gì không thì thấy khá nhiều thông tin thú vị (cái này các bạn tự tìm hiểu nhé....)

Binwalk tiếp xem sao.

```
epubc@xx:~/Downloads$ binwalk 1896
```

DECIMAL	HEXADECIMAL	DESCRIPTION
5226576	0x4FC050	Linux kernel version "2.6.35.9-32-sigma (hiengnuy@sv-linuxcentos84) (gcc version 4.3.2 (Sourcery G++ Lite 4.3-51)) #174 PREEMPT Mon Oct 12 14:58:15"
5248232	0x5014E8	gzip compressed data, maximum compression, from Unix, last modified: 2014-12-11 07:36:53
5381040	0x5218B0	CRC32 polynomial table, little endian
5769416	0x5808C8	Unix path: /dev/vc/0
5822768	0x58D928	Ubiquiti firmware header, third party, -CRC32: 0x75657565, version: "_DOWNGRADE"
6026644	0x5BF594	Neighborly text, "NeighborSolicitsIPv6 ah init: can't add xfrn type"
6026664	0x5BF5A8	Neighborly text, "NeighborAdvertisementsadd xfrn type"
6324784	0x608238	Certificate in DER format (x509 v3), header length: 4, sequence length: 24708
6606848	0x64D000	gzip compressed data, maximum compression, from Unix, last modified: 2015-10-12 07:58:08

Lại thấy một data bị nén nữa,,, nhưng lần này file 1896 có vẻ cho mình nhiều thông tin hơn nữa.

dd phát nữa xem sao.

```
epubc@xx:~/Downloads$ dd if=1896 of=6606848.gz bs=6606848 skip=1
```

0+1 records in
0+1 records out
6606848 bytes (6.3 MB, 6.1 MiB) copied, 0.0135253 s, 469 MB/s

TRUNG TÂM SỬA CHỮA ĐIỆN TỬ QUẢNG BÌNH

MR. XÔ - 0901.679.359 - 80 Võ Thị Sáu, Phường Quảng Thuận, tx Ba Đồn, tỉnh Quảng Bình

GIÁ RẺ

NHANH CHÓNG

LINH KIỆN CHÍNH HÃNG



TRUNG TÂM SỬA CHỮA ĐIỆN TỬ XÔ NGUYỄN

- Dịch vụ sửa chữa điện tử tại nhà
- Cung cấp linh kiện điện tử
- Tư vấn lắp đặt nhà thông minh

Đc: Quảng Thuận, tx Ba Đồn,
tỉnh Quảng Bình - 0901.679.359

Tiếp tục giải nén ra xem thế nào.

```
epubc@xx:~/Downloads$ gzip -d 6606848.gz
```

gzip: 6606848.gz: decompression OK, trailing garbage ignored

```
epubc@xx:~/Downloads$ binwalk 6606848
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	ASCII cpio archive (SVR4 with no CRC), file name: "/dev", file name length: "0x00000005", file size: "0x00000000"
116	0x74	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/pts", file name length: "0x00000009", file size: "0x00000000"
236	0x4C	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/ptmx", file name length: "0x00000009", file size: "0x00000000"
368	0x170	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/tts", file name length: "0x00000009", file size: "0x00000000"
488	0x1E8	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/tts/0", file name length: "0x0000000B", file size: "0x00000009"
624	0x270	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/tts/1", file name length: "0x0000000B", file size: "0x00000009"
768	0x2F8	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/tts/2", file name length: "0x0000000B", file size: "0x00000009"
896	0x380	ASCII cpio archive (SVR4 with no CRC), file name: "/dev/tts/3", file name length: "0x0000000B", file size: "0x00000009"
1032	0x408	ASCII cpio archive (SVR4 with no CRC), file name: "/bin", file name length: "0x00000005", file size: "0x00000000"
1148	0x47C	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/ntv2_m2pl", file name length: "0x00000013", file size: "0x00000037"
14964	0x3A74	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/fgrep", file name length: "0x0000000B", file size: "0x00000000"
15096	0x3AF8	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/stty", file name length: "0x0000000A", file size: "0x00000000"
15224	0x3B78	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/linux32", file name length: "0x0000000D", file size: "0x00000000"
15356	0x3BFC	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/sed", file name length: "0x00000009", file size: "0x00000000"
15484	0x3C7C	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/hostname", file name length: "0x0000000D", file size: "0x00000000"
15616	0x3D00	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/mtd_setenv2str.bash", file name length: "0x0000001A", file size: "0x00000000"
15832	0x4000	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/kexec", file name length: "0x00000006", file size: "0x00000000"
15864	0x4004	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/ntcc", file name length: "0x0000000A", file size: "0x00000000"
15892	0x4008	ASCII cpio archive (SVR4 with no CRC), file name: "/bin/rm", file name length: "0x00000005", file size: "0x00000000"

Tài liệu này được tải từ website: <http://linhkienthaomay.com>. Zalo hỗ trợ: 0389937723

XONG,,, lần này thì đã có dữ liệu để xem rồi.

```
epubc@xx:~/Downloads$ tree 6606848/
6606848/
├── 1 -> ../../bin/busybox
├── 1f -> ../../bin/busybox
├── 6 -> ../../ttyS0
├── 1 -> ../../ttyS1
├── 10-usb-storage
├── 2 -> ../../ttyS2
├── 3 -> ../../ttyS3
├── a
├── li
├── ansi
├── archop
├── arping -> ../../bin/busybox
├── awk -> ../../bin/busybox
├── badblocks
├── basename -> ../../bin/busybox
├── bash
├── bbconfig -> busybox
├── bin
├── blkid
├── boot_auth
├── bunzip2 -> ../../bin/busybox
├── busybox
├── bzipcat -> ../../bin/busybox
├── cat -> busybox
├── catv -> busybox
├── check_for_update_SDK.sh
├── check_for_update.sh
├── chgrp -> busybox
├── chlpID
├── chmod -> busybox
├── chown -> busybox
├── chroot -> ../../bin/busybox
├── chrt -> ../../bin/busybox
├── chvt -> ../../bin/busybox
├── CK_FPT_8656_prod_oen_otp_cpu_ff01_pubkey.pem
├── cksum -> ../../bin/busybox
├── cksumdir.bash
├── cksumlist.bash
├── clear -> ../../bin/busybox
├── cmp -> ../../bin/busybox
├── cp -> busybox
├── cpio -> busybox
├── crond -> ../../bin/busybox
├── crontab -> ../../bin/busybox
├── cs_rootfs_config.gz
├── cs_rootfs_source -> /tango/toolkit/snp8674/fpt/snp8675B/toolkit_otp/build/cs_rootfs_1.3.0
└── cs_rootfs_version
```

Tác giả:

[bacuaBaoNgan](#)

- 29 tháng 11

Các bài viết tương tự:

- [1. âm ly 8 sò \(4 sò 1 vẽ\)tối hôm trước hát bình thường kéo dài vài tiếng ok,,sáng hôm sau trời âm khách bật máy ko có nghe dc j,,,khách say cứ để vài phút,,,lúc sau em lên kiểm tra BA om nóng,,,rơ le ko đóng, fuse ko nổ cho\) - em sửa con này tính ra dc 1 tháng,,nhà ông này hay hát hò karaoke,,,lần trước cũng chết công suất đứt fuse,,rơ le ko đóng,,,thay cũng đúng loại cầu chì ampe và công suất,,,lần đó cũng hát bình thường hôm sau trời âm là chết công suất nổ fuse](#)
- [2. Amply công suất\(cục đẩy\), sử dụng 40 còng, mỗi main sử dụng 1 tranfor 25A - 01 main hát tốt, 01 main không nghe, em đã kiểm tra điện thế cấp cho các còng và điện thế cấp cho ic 4558 đều đầy đủ, role đóng và tiếp xúc tốt.](#)
- [3. bếp từ loại 2 cuộn dây,,bếp này có 2 cuộn dây có mô tơ bơm nước để khi đang ăn nước cạn thì ấn nút bơm thêm nước vào ăn,,2 cuộn dây dc 1 rơ le 12vol điều khiển - lúc đầu chết công suất,,,kèm tra thay thế giờ nguồn ko lên,,ktra BA xung hỏng? thử cấp ra 3 điện áp \(5 vol cpu,12vol rơ le,12vol mô tơ hút](#)
- [4. bếp từ prince - nổ cầu chì hư công suất,,,đã thay vào và kiểm tra các tụ lọc tốt,,trở tại chân g công suất tốt,,cảm biến tốt,,,cắm nguồn sau khi thay báo lên nguồn nút bấm lệnh ok,,,vẫn có xung thăm dò kèm tiếng kêu và hiển thị nhưng khi đặt nồi lên là nổ cầu chì và hư công suất,,2 đã thay 2 lần công suất và cầu chì,vẫn chưa ra bệnh,,,đặt nồi lên là nổ cầu chì hư công suất](#)

5. Cách khắc phục lỗi. 1:không stand by được 2:stand by sau 2-5s thì quay trở lại màn hình log 3:Mở biểu tượng stand by. 4: mục system trong windows task manager chêm dụng trên 20% cpu khiến hiệu suất hoạt động máy giảm sút (lỗi 2 là nguyên nhân cơ bản) khi mắc lỗi này máy sẽ gặp vấn đề về stand by-computer sleep. - Ai đang gặp những lỗi trên vui lòng liên hệ với tiny mino trên facebook <http://facebook.com/tiny.mino.3> hoặc LH: 016577082380 để được hướng dẫn.
6. dạ em có con quạt hơi nước hiện tượng các nút ok riêng nút nguồn ko hư hỏng bấm ko tác dụng,,,khi bấm nút tắt ko tác dụng bấm nút này đèn led hiển thị của các nút yếu đi,,,mạch in dẫn tới nút ăn thẳng vào vi xử lý ko qua trở,,,,em chưa kiểm tra nguồn - laojq quạt này(quạt hơi nước) cắm nguồn bấm nút chức năng số(tốc độ),hoặc quay hoặc hẹn giờ hoặc tạo âm vãn bình thường riêng nút tắt ko tắt dc,,,nguyên bản là tắt dc nhưng giờ là ko tắt dc
7. em có cái thẻ học nghề trực tuyến 2 triệu chưa dùng - ai cần e để lại cho
8. Gunners MD-9999 - lúc khách đem tới đĩa k chạy . e kt thì chết 3kon đi ốt , 4004 bên boos hình . thay xong cho chạy thử được nhưng nó lên đĩa vẫn chạy .nhưng pị đứng nhạc . tắt đi để nguội . pật lên lại chạy cứ thế
9. Mạch toshiba B1100 - Giat xả bình thường đến lúc vắt còn 3phút thì dừng rồi tự động lên 17 phút xả lại cứ như vậy liên tục.ấn vắt không thì vắt xong lại lên 12phút và xả
10. Máy giặt lg inverter - Lỗi ae . Lúc lỗi lúc không. Những lúc không lỗi bấm giặt cấp nước vào rồi thôi. Máy cứ trơ ra k làm việc
11. máy giặt panasonic F70A6 lồng đứng - + máy bật nguồn để khoảng 30s máy tự động kéo xả .nhưng khi bật chạy thì lại ngắt xả và cấp nuocs giat bình thường nhưng đến lần giat thứ 2 thì lại tự động kéo xả và cấp nuocs nhưng khi nhấc canh của hoặc án tạm dừng sau đó bấm lại thì lại haotj động bình thường
12. Tea2025b sử dụng với mạch stereo - Tự nhiên 1 bên của e k còn nghe thấy nữa e đã ktra kĩ hết đầu input ổn cả lúc sau thử thì cả 2 bên đều k thấy rì cả e đã thay 2 con 16v450uf nhưng vẫn bị.