ĐÂY LÀ MỘT BÀI VIẾT DÀI KỂ VỀ QUÁ TRÌNH MÌNH TÌM DRM Key..

Như bài trước mình có giới thiệu qua về con Box của FPT chạy Linux thuần túy…

Bài viết này mình sẽ có gắng nói thật ngắn gọn về **DRM key** của con Box này. Vậy **DRM key** là gì và chúng có tác dụng gì trong thiết bị giải trí??

Mình xin nhắc lại chút về từ khóa **DRM key** cho một vài bạn hiểu (mình cũng tìm hiểu trên mạng và tha về blog này thôi…đứng quá khích khi mình nói sai nhé, hãy comment lại cho mình biết.)

DRM key là sao và tác dụng của chúng trong thiết bị giải trí???

DRM key là từ được viết tắt của **Digital Rights Management Key** (công nghệ quản lý bản quyền số). **DRM key** cần thiết cho việc thực hiện một số chứng năng nhất định mà nhà sản xuất muốn quản lý, cụ thể ở trên Box này thì **DRM key** có tác dụng rất quan trọng trong việc phát Video/Audio chất lượng cao qua cổng HDMI (bản quyền mà).

DRM key thường thì nó là một mã số riêng biệt, nghĩa là mỗi một thiết bị thì sẽ có **DRM key** tương ứng, việc này nhằm quản lý chặt chẽ vấn đề bản quyền số. Thông thường **DRM key** nó sẽ nằm ở phân vùng bootloader do vậy phải thật sự hư nặng lắm như sét đánh, cháy nổ mới mất cái **DRM key** này. (bootloader là một đoạn mã được thực thi trước khi hệ điều hành bắt đầu
chạy và nó cho phép nhà sản xuất thiết bị quyết định những tính năng nào
người sử dụng được phép dùng hoặc bị hạn chế.)

Mất **DRM key** điều gì sẽ xảy ra.. các thiết bị khác thì mình không rõ nhưng với Box nếu như mất **DRM key** thì việc xuất hình ảnh, âm thanh chất lượng cao qua cổng HDMI hay quang sẽ = 0,,, Nói tóm lại là Box sẽ vẫn chạy và màn hình sẽ đen thui. Việc này nhằm ngăn chặn khi một ai đó cố gắng can thiệp vào phần cứng để làm một điều gì đó mà nhà sản xuất không mong muốn.

Nói dài dòng vậy thôi, giờ đi vào việc chính.

Mình có 1 con Box sử dụng mạng FPT sau này do hết hạn hợp đồng nên Box nó trở thành cục chặn giấy đúng nghĩa, cắm nguồn vẫn lên nhưng không thể làm gì được vì nó dùng mạng của FPT. Sau một thời gian mình tìm hướng đi để sử dụng được Box này thì phát hiện thêm 1 vấn đề là tất cả các cách thức truy cập vào con Box này đều bị vô hiệu hóa và kèm theo là có mật khẩu bảo vệ.
Mình cũng thử từng dò mật khẩu bằng cách nhập vào những chuỗi ký tự mà người ta hay đặt pass nhưng tất cả đều không thành công.

Sau đó mình search Google thì mình thấy chip Sigma này nó được nhiều hãng sử dụng. Và cụ thể ở đây mình có thấy 1 hãng đó là Dune. Tìm hiểu một hồi mình tìm ra cách truy cập vào Bootloader của Box và mày mò trong đó,, và cũng từ đây thì Box đồng nghĩa với việc tèo khi boot không được nữa.

Kinh nghiệm cho mình biết là nó đã bị lỗi gì đó trong con Flash mà mình hay gọi tắt là lỗi ROM.

Giải quyết vấn đề.

Với những con bị lỗi ROM thì thường cách giải quyết nhanh gọn nhẹ nhất mà dân kỹ thuật hay làm là nạp ROM. Nạp ROM là gì?? Đó là phương pháp để làm sao cho máy trở về như lúc ban đầu, thường thì mình có các nút Reset trên các thiết bị nhưng với một vài thiết bị đặc biệt thì hang sản xuất họ lại không thiết kế nút này,,, Phương pháp nạp ROM đa số đều làm cho thiết bị chạy lại thành công và các lỗi liên quan tới phần mềm đều được fix hết. một vài trường hợp vẫn không hết bệnh thì có nghĩa là rơi vào phần cứng… lúc này thì không phải liên quan tới ROM nữa mà nó có thể liên quan tới RAM, Vi xử lý, các IC giao tiếp hay cấp nguồn.

Tiến hành nạp ROM

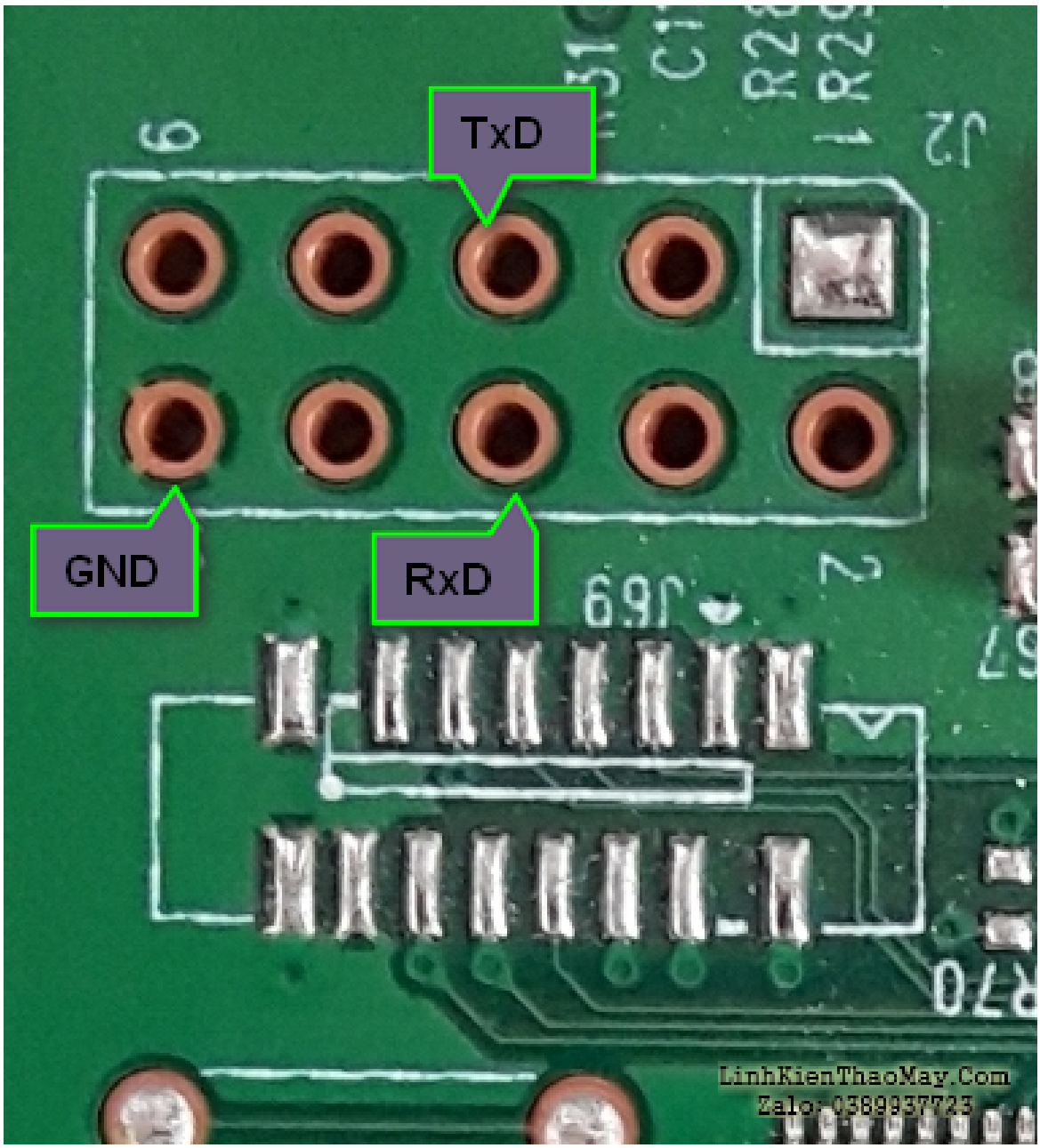
Để tiến hành nạp ROM cho một thiết bị đang bị lỗi phần mềm thì mình có nhiều bước thực hiện.

- Sử dụng máy nạp ROM chuyên dụng
- Sử dụng thao tác lệnh console thông qua các cổng giao tiếp trên board thiết bị. Thường thì đa số thiết bị sẽ cung cấp cổng Console này,, cổng này dân kỹ thuật thường hay gọi là cổng nối tiếp hay là cổng RS232…
- Sử dụng thao tác lệnh Console thông qua cổng giao tiếp đặc biệt JTAG. JTAG được làm ra để dung cho việc test PCB là chủ yếu, nhưng thông qua cổng này mình có cũng có thể nạp được ROM hay debug phần mềm.

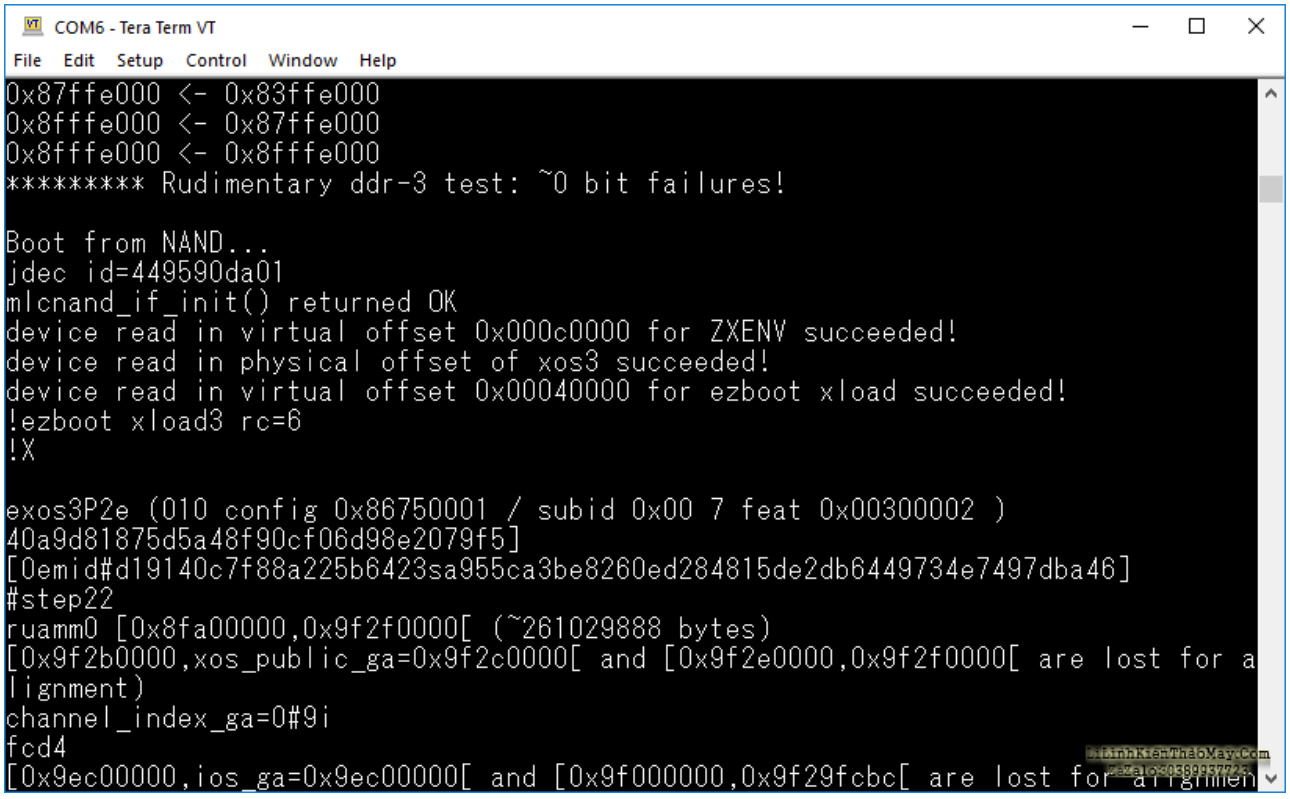
Bài viết này mình sẽ sử dụng máy nạp ROM chuyên dụng, nhờ mối quan hệ với anh em kỹ thuật mà mình mượn được một bộ nạp ROM dạng chân TSOPxx.

Bước đầu tiên thuộc **điều kiện bắt buộc phải có** là có một source tốt, có nghĩa là có 1 cái Box đang chạy OK. Mình có liên hệ trong nhóm thì có 1 anh nhà đang dùng con này và mình có xin nhờ anh đó dump file ROM hộ mình và ảnh OK.
Sau khi có ROM ok mình tiến hành Backup ROM cũ trước rồi nạp vào và,,,,cắm nguồn thì thì có boot bình thường, hiện logo FPT nhưng sau đó thì không còn hiện tượng gì xảy ra nữa, hình ảnh, âm thanh đều không có,,, trong khi đó màn hình HDMI vẫn báo có tín hiệu. == > vẫn có tín hiệu có nghĩa là box đã boot OK nhưng có vấn đề gì đó mà không hiện hình được. Tiến hành tìm kiếm thông tin thì trên mạng có một sản phẩm khác hãng có cấu trúc phần cứng tương đồng là Dune TV102, tìm kiếm thông tin về sản phẩm này thì thu được kết quả có file log của loại sản phẩm này, tìm thêm chút nữa thì thấy nó có cổng giao tiếp RS232.

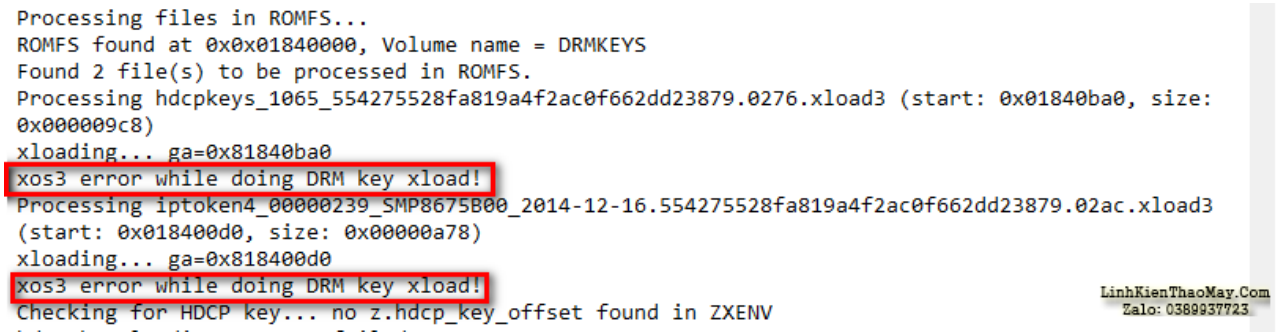
Tiến hành rà soát trên board Box để tìm cổng Console thì phát hiện ra có 2 vùng socket để trống, kết hợp kinh nghiệm thì xác định được J2 là cổng Console.



Tiến hành log vào thì chính xác là là đây là cổng Console và file log như dưới: (file log rất dài nên mình chỉ post của sổ của nó đang chạy.)
Tình cờ mình đi chợ Nhật tảo thấy họ bán ve chai con này có 70k nên hốt về một con và thật bất ngờ là nó chạy OK... chắc do hết hạn hợp đồng truyền hình như mình nên họ bỏ.
Quay lại vấn đề.



Mình thử Log vào con mới và save lại file log sau đó mình đem 2 file này ra so sánh.
Để ý thì thấy file này nó chạy tới cuối luôn và so sánh với Box OK thì hoàn toàn giống nhau.
Như vậy vấn đề nằm ở đâu???
Rà soát lại lần nữa thì ta thấy ngay gần đoạn đầu tiên khi boot thì có sự khác biệt:

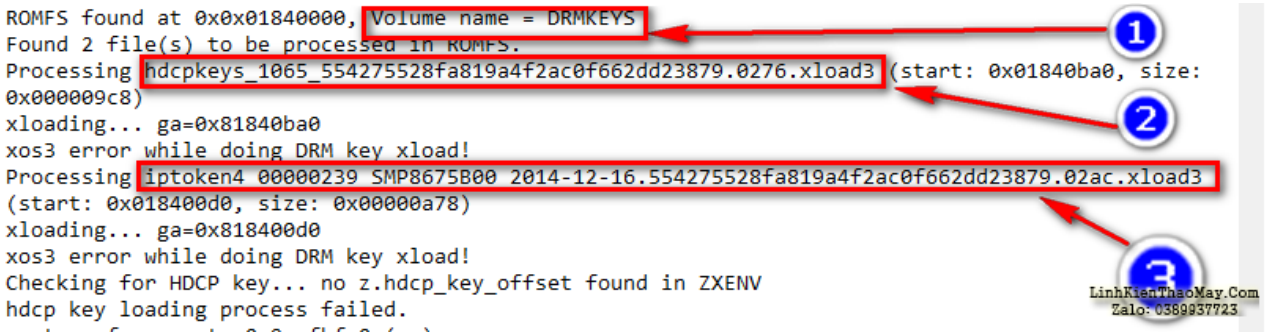


Từ khóa DRM key với Google thì mình được nhiều thông tin thú vị liên quan tới các thiết bị phát nguồn HD, cụ thể ở đây là với box. Theo như mô ta từ google thì DRM key thường được đi kèm với thiết bị HD để chống tình trạng sao chép nguồn HD, cụ thể thì ví như là phát tán phim lậu. Một ngôi nhà được ví như là Box và chì khóa nhà thì nó dĩ nhiên là giống như mật khẩu ra vào ngôi nhà đó rồi,, hehe, DRM key nó sẽ giống như cái quyền thuê nhà vậy,,, bạn chỉ được quyền sống trong căn nhà đó nhưng không cho phép mang đồ vật gì ra ngoài. Quay trở lại vấn đề về cái lỗi DRM key này, như vậy kết luận một điều là DRM key có liên quan tới hình ảnh trên màn hình HDMI không hiển thị.

Thử kết nối màn hình qua cổng AV thì hình ảnh hiện lên bình thường ?????????????????? quái lại. Như vậy là sao!!! Tìm lại chút thông tin trên mạng vẫn về DMR key thì mình thu them được chút thông tin là DRM key sẽ chỉ ngăn việc sao chép hình ảnh video chất lượng cao ra khỏi thiết bị... liên tưởng tới vấn đề của Box thì ta có thể thấy là việc cắm cổng HDMI vào màn hình thì không hiển thị và nếu cắm cổng AV thì hiển thị bình thường. như vậy kết luận một điều là DRM key ngăn không cho Video và âm thanh chất lượng cao xuất qua cổng HDMI.

Phân tích cơ chế kiểm tra DRM key để cho phép xuất hình ảnh ra cổng HDMI.

Rà soát và so sánh lại file log mình có them thông tin về DRM key, cụ thể là một chuỗi ký tự liên quan tới DMR key:



1. Một phân vùng có tên là **DRM keys**
2. Một file có tên là **hdcpkey.xxxxx**
3. Một file có tên là **iptokey.xxx**

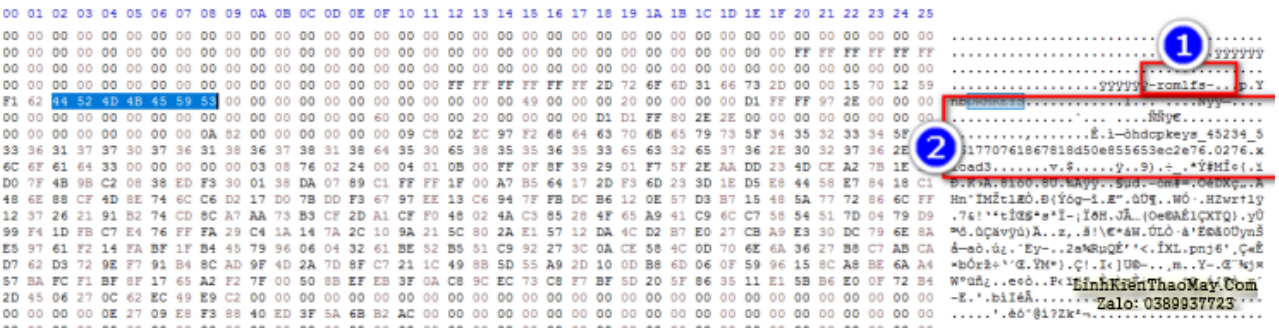
Cả 2 file này đều nằm trong phân vùng có tên là DRM keys và đều liên quan tới cụm từ DRM keys. như vậy vấn đề rõ rang nằm ở 2 file này.

Đọc và so sánh giữ 2 con Box nữa thì ta lại phát hiện một điều là 2 file hdcpkey và iptoken có các chuỗi số khác nhau (10 con Box thì sẽ có 10 file có chuỗi số khác nhau….). Như vậy mình đoán là mỗi Box sẽ có file khác nhau và không trùng lẫn được. Tới đây vấn đề gần sáng tỏ rồi.

Một Box A có chuỗi số **hdcpkey** và **iptoken** là AAA và một Box B có chuỗi số **hdcpkey** và **iptoken** là BBB. Nếu như copy source của con B qua A thì báo lỗi.. ??? Box dự vào cái gì để phát hiện ra chuỗi số của 2 file này không hợp lệ, lấy gì để so sánh 2 file này??

Thử lấy con ROM OK đóng qua board bị lỗi ROM thì vẫn là vấn đề DRM key như vậy Box so sánh 2 chuỗi file này với một chuỗi file nào đó không phải nằm trong nội dung con ROM để phát hiện ra việc can thiệp phần cứng nhằm vượt qua cơ chế DRM của hãng.

Sử dụng một chương trình Hex Editor để đọc source và tìm kiếm từ khóa DRM key liên quan.



Như vậy mình có them thông tin:

- **-rom1fs-**: đây là ký tự nhận dạng trong linux cho biết đây là một phân vùng
- **DRM keys**: tên phân vùng và ta cũng nhìn thấy là trong phân vùng này có chứa một

file **hdcpkey.xxx**. di chuyển xuống offset dưới mình cũng sẽ thấy một file nữa tên là **iptoken** nữa.

Thử thay đổi tên của 2 chuỗi này thì khi chạy sẽ báo lỗi không tìm thấy 2 file này...và màn hình thì vẫn đen thui.

Sử dụng Hex Editor tìm tới phân vùng DRM Keys này và làm theo cách thủ công là copy – paste đoạn offset thay thế, dò phân vùng này ta thu đươc kết quả là offset chứa phân vùng này là cố định đều có địa chỉ bắt đầu từ **0x154000** và kết thúc là **0x15572F** (chú ý là ứng với mỗi loại NAND khác nhau thì Offset khác nhau nhé). Sau khi thử copy-paste thì ố ồ.. cuối cùng cũng hiện hình.

Phân tích file ROM bằng công cụ binwalk thì ta thu được kết quả như hình dưới.

```
epubc@xx:~/Downloads$ binwalk B046FCB22749_BACKUP--OK.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
502700        0x7ABAC         ZBOOT firmware header, header size: 32 bytes, load address: 0x00000000, start address: 0x0
0000000, checksum: 0x62616E55, version: 0x7420656C, image size: 1701847151 bytes
509380        0x7C5C4         CRC32 polynomial table, little endian
781228        0xBEBAC         ZBOOT firmware header, header size: 32 bytes, load address: 0x00000000, start address: 0x0
0000000, checksum: 0x62616E55, version: 0x7420656C, image size: 1701847151 bytes
787908        0xC05C4         CRC32 polynomial table, little endian
1114116       0x110004        romfs filesystem, version 1 size: 217936 bytes, named "YAMON_XLOAD"
1392644       0x154004        romfs filesystem, version 1 size: 5488 bytes, named "DRMKEYS"
2228228       0x220004        romfs filesystem, version 1 size: 463536 bytes, named "xmaterial"
2700203       0x2933AB        CRC32 polynomial table, little endian
3342340       0x330004        romfs filesystem, version 1 size: 3979872 bytes, named "imaterial"
7570891       0x7385CB        gzip compressed data, from Unix, NULL date (1970-01-01 00:00:00)
14483460      0xDD0004        romfs filesystem, version 1 size: 9262048 bytes, named "MIPSLINUX_XLOAD"
```


Như vậy là mình đã hiểu sơ qua cơ chế của DRM keys và cách mình vượt qua nó. Thực sự thì còn rất nhiều điều thú vị đằng sau câu chuyện này mà mình không dám kể ra vì nó sẽ làm ảnh hưởng "miếng cơm" của một số người (mình đã được yêu cầu gỡ bổ một vài nội dung liên quan tới bản quyền).

Kết thúc phần này, phần tới mình xin nói về **Cách sử dụng binwalk để phân tích cũng như giải nén firmware**

Tác giả:
bacuaBaoNgan
– 25 tháng 11

Các bài viết tương tự:

1. Cách thiết kế các giải pháp năng lượng cho hệ thống thông tin giải trí trên ô tô Công nghệ bộ điều khiển điện áp cao
2. Câu Công Tắc Nguồn Nokia 6300 – Nokia 6300 Power Key Solution
3. dia cai win xp sp2 – khong co ma key ghi tren dia
4. đầu karaoke vietktv treo logo vietktv – em nhận của khách trong tình trạng treo logo khởi động .bác nào có phương án giải quyết xin giúp em với ,em chua bao giờ gặp trường hợp này ,mang các bác chỉ giáo
5. Giải pháp phần cứng cho iphone 6 liệt nút Home
6. Lap top hp pavilion dm3 notebook pc – Lam on chi dum..may cua minh main van chay quat van quay nhung khong len nam hinh.minh da thu cam cong VGA sang may khâc van k len man hinh .moi ng chi cho minh huong giai quyet nhe.cam on nhieu
7. laptop – xin hỏi bác pro ý kiến cho mình xài win8.1 lúc cài đặt phần mềm virut ko sao khi cài Dcom 3G lúc đầu chạy bình thường. mình thấy phần mềm virut khóa key gỡ bỏ xong khởi động lại máy bị lỗi Dcom 3G nó báo lỗi ip gì đó
8. Máy giặt deawoo 7.2 kg – Bấm power kêu ù ù. Van xả mở. Phao ko đc cấp điện .e đem thợ thay triac xả về .bấm chu hũ trình giặt bình thường nhưng lượt thứ 2 lại bị như cũ. Đem ra thợ lần 2 cũng thay triac xả rồi về vẫn vậy. Riết tiền sửa bằng tiền mua bo luôn. Huhu .nhờ các anh chỉ giáo để giải quyết 1 lần duy nhất ạ
9. máy giặt panasonic mono cửa trên ,model NA-F76VB6 – hiện tượng bật máy bấm start thì van xả kéo luôn và báo lỗi h21 (em xin được giúp đỡ cách giải quyết)
10. Mở service monitor. – mình có đề nghị này: các thầy nên bổ sung phần mở service cho monitor như trong phần tivi vậy để cho các bạn tham khảo. Phần này, mình nghĩ chắc nhiều người cũng như mình rất cần phần này để trị mấy con monitor mà không phải trả lại cho khách.
11. Tivi TCL model TD 2127ARH, ic vi xử lí TCL-A1V01, ic giải mả TB 1238AN, ic âm thanh TDA7496 – Phần đài(dùng cáp SCTV) hình đẹp, nhưng tiếng bị rè(em đã đổi hệ DK, BG), em đã thay ic ic giải mả TB 1238AN, ic công tắc 4053, hàn lại mạch, nhưng vẫn bị rè. Phần AV tiếng tốt, nhưng không có hình
12. XIN CHÀO TẤT CẢ AE TRÊN DIỄN ĐÀN – minh có em HLV PRO 300 8 sò to hư 1 vế tình trạng là 1 vế bị ù như là chập sò vậy nhưng mà sò ko hư mình cô lập tầng công xuất ra do các diện áp 2 vế ổn dịnh nhưng cắm sò vào là ù rơ le vẫn đóng mình xin ý kiến của ae cho phương án giải quyết