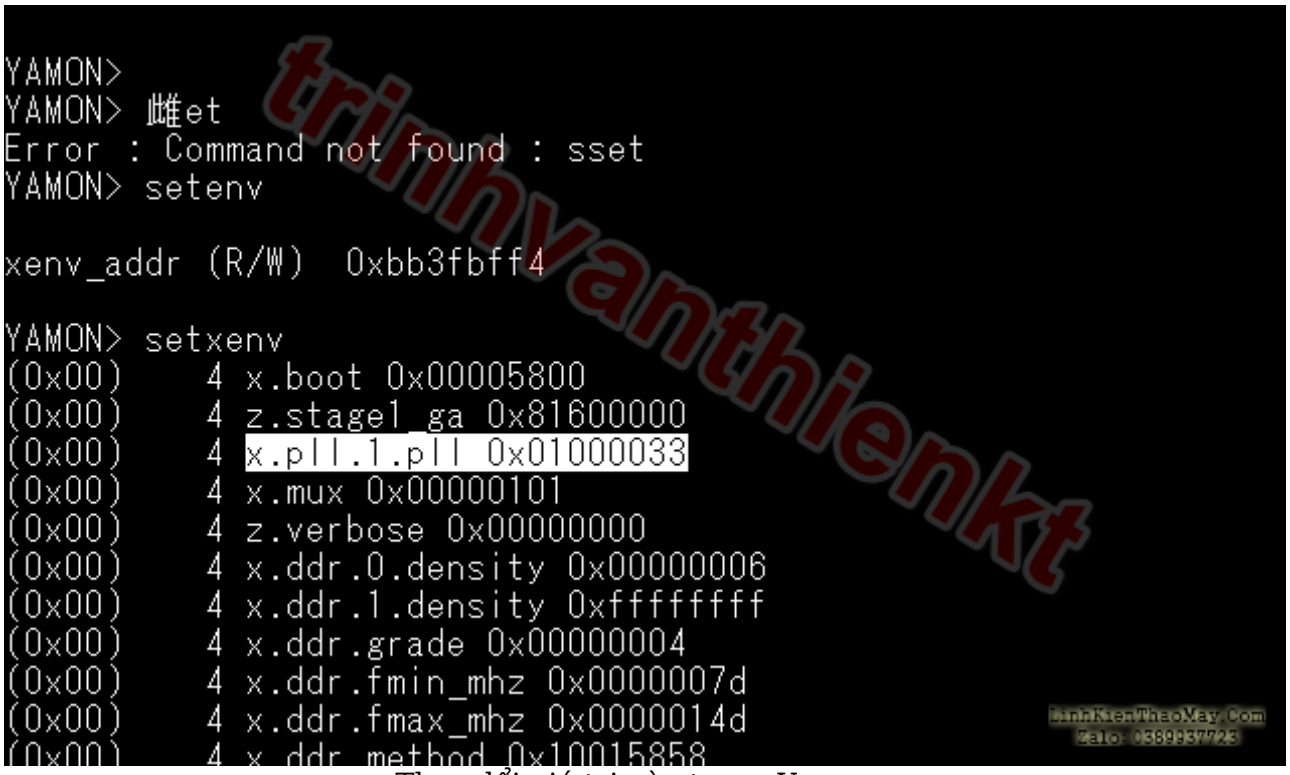
Mình thử "**overclock**" nho nhỏ trên con **IPTV HD Set-top Box** (PLAY HD) và thấy nó làm việc một cách ok.

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

Để tiến hành "overclock" thì bạn có thể gõ lệnh trực tiếp trong Box sau khi login với quyền Root. Hoặc không bạn cũng có thể thực hiện tác vụ này thông qua Bootloader của Box (Yamoon):



Thay đổi giá trị này trong Yamoon

setxenv_mtd.sh 0 -b x.pll.1.pll 0x01000033

Tần số được thay đổi từ 702 MHz lên thành 810 MHz trong lần khởi động kế tiếp.

Giá trị 3B tương đương với giá trị của bộ lõi nhân tần số PLL (27 MHz) theo công thức:

(HEXcode + 1) * 27 / CPU_Mux = (3B + 1) * 27 / 2 = 810 MHz

Bình thường thì giá trị 3B này là ok “đẹp” do vậy không nên chỉnh vượt quá giá trị 3B này tránh trường hợp Box của bạn không thể đọc được nội dung của con ROM (NAND Flash) do vậy sẽ dẫn tới Box bị Brick.

```
YAMON> setxenv -b x.pll.1.pll 0x0100003b
Original value: 0x01000033
New value: 0x0100003b
Please flush(using nflash/pflash write command) the updated transient XENV block
(memory location: 0xbb3fbff4, maximum size: 0x00004000) to the location desired
for permanent storage.
YAMON> $commit
```

Tham số trước khi thay đổi tần số:

```
Thu Mar 10 14:24:58 ICT 2016
Configured for SMP867x, detected SMP8671 (revision ES2).
Detected CPU/System/DSP Frequencies: 702.00/351.00/351.00MHz
SMP86xx Enabled Devices under Linux/XENV 0x9f3fbff4 = 0x001002f8
 Ethernet Ethernet1 IR FIP I2CM I2CS USB
Desired kernel memory size: 0x04000000
Max. DRAM0/1 size allowed: 0x0fa00000/0x00000000
```

Gốc

Tham số sau khi thay đổi tần số:

```
Configured for SMP867x, detected SMP8671 (revision ES2).
Detected CPU/System/DSP Frequencies: 810.00/405.00/405.00MHz
SMP86xx Enabled Devices under Linux/XENV 0x9f3fbff4 = 0x001002f8
 Ethernet Ethernet1 IR FIP I2CM I2CS USB
Desired kernel memory size: 0x04000000
Max. DRAM0/1 size allowed: 0x0fa00000/0x00000000
```

Đã nâng xung lên

Các bài viết tương tự:

1. [Phần 1] Giải quyết DRM key
2. [Phần 2] Sử dụng công cụ Binwalk để phân tích Firmware
3. Cài đặt NodeJS trên seedbox không có quyền root
4. Cài đặt Transmission Web Control lên NAS
5. Dump Firmware Hikvision Camera với SPI Flash Hardware Protocol
6. FPT Box HD FIRMWARE_VERSION=3.1.5
7. Giải nén file dune_service_XXXX.dsf của Dune
8. Hướng dẫn dump firmware ESP8266, ESP32 với UART
9. Phân tích lỗ hổng RCE tràn bộ đệm của TP-Link TL-WR940N
10. Thử bruteforce camera China và cái kết :D
11. Thử chiếm quyền kiểm soát các thiết bị thông minh IOT của hãng Akuvox
12. Tìm hiểu modbus và thử xâm nhập hệ thống truyền tải điện lưới quốc gia