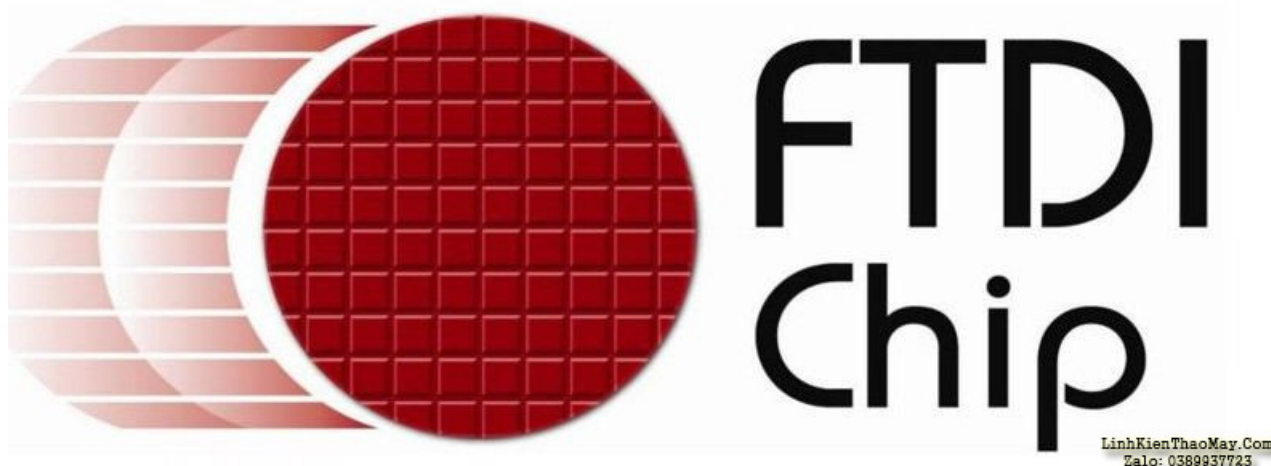


Làm thế nào để nhận ra một giả FT232RL?



Trên mạng có nhiều người phản hồi về việc chip FT232RL giả!! Thường thì cách giải quyết vấn đề này là sử dụng một chip khác có tính năng tương đương như CY7C65213, CP2102, PL2303, CH340, FT230. Nhưng không phải lúc nào cũng mua được những con chip này từ các cửa hàng linh kiện ở Việt Nam (cụ thể từ Nhật Tảo) trừ hàng cũ được “luộc” ra từ các mainboard cũ

Dưới đây là hình chụp IC chính hãng và IC được làm nhái từ “nhà hàng xóm” China





Hình. 1. Chip FT232RL gốc.





Hình. 2. Chip giả mạo FT232RL.

Nhìn vào hình trên có thể thấy rằng Chip fake nhìn còn đẹp hơn Chip chính hãng, chữ sắc nét hơn, nhìn bề mặt gia công cũng rõ ràng hơn. Vì vậy đôi khi người mua không chắc có thể phân biệt được giữa hàng chính hãng và hàng giả mạo.

Trước đây (hình như là cuối năm 2014 thì phải, mình nhớ không chính xác lắm) hãng **FTDI** phát hành một firmware cho phép phát hiện hàng giả, người dùng nếu sử dụng Windows và để chế độ là **Auto Update Drivers** thì driver sẽ được tự động tải xuống và kiểm tra xem liệu Chip có phải là chính hãng hay không??? Nếu không phải thì nó sẽ khóa Chip đó lại và không cho sử dụng nữa. Sau này do quá nhiều kể vì chuyện khóa Chip giả mà FTDI phát hành lại driver không khóa Chip giả nữa nhưng sẽ hiện thông báo cho người dùng biết là nó là đồ giả như hình dưới.



Vì vậy cần phải có những phương pháp khác đáng tin cậy hơn. Những người nhiệt tình đã tháo rời một đoạn của trình điều khiển mới và phát hiện chính xác nó làm hư hại các chip giả mạo. Trình điều khiển ghi vào EEPROM bên trong của chip tại địa chỉ 0x002 số không (chỉ là thiết bị PID), và ghi vào 0x03e mã như vậy để CRC (nằm ở địa chỉ 0x03f) đã tham gia. Trên chip gốc, các hoạt động này không dẫn đến hư hại, bởi vì EEPROM có một tổ chức 32-bit. Khi viết một từ với một địa chỉ chẵn, chỉ có bộ đệm xảy ra, và khi viết một từ tại một địa chỉ lẻ,

hai từ được ghi lại cùng một lúc. Một con chip giả mạo ghi lại mọi từ, vì vậy nó làm hư PID (trở thành 0x0000). Do đó, giả mạo chip thường được phát hiện tại kết nối đầu tiên (trong khi dữ liệu trong EEPROM là chính xác), và sau khi kết nối được xác định để chấm dứt. Trên diễn đàn [eevblog](#) là một mảnh vỡ của lái xe, cũng có một bình luận của đại diện của FTDI, nơi mà thực tế này không bị từ chối, nhưng có một lời hứa để tiếp tục hành động các phương pháp không phá hoại.

Để xem lại chip bị hư hư, bạn cần phải cài đặt một trình điều khiển sửa đổi một chút. Trong tệp tin inf, các dòng với PID_0000 được thêm vào, sau đó nó sẽ hỗ trợ cả hai phần mềm giả mạo ban đầu và “hư hư”. Nhưng chỉ trước khi cập nhật trình điều khiển đầu tiên.

Tải xuống tệp tin đã sửa đổi cho các trình điều khiển CDM20416 và CDM20814 bên dưới trong mục Tải xuống. Bằng cách tương tự, bạn có thể chỉnh sửa tệp tin thông tin cho trình điều khiển của các phiên bản khác.

Để nhanh chóng phân biệt các chip gốc khỏi hàng giả mạo, mình đã viết một tiện ích nhỏ mà cố ghi dữ liệu vào một địa chỉ EEPROM. Nếu nó hoạt động – chip là giả mạo. Sau đó tiện ích khôi phục lại giá trị trước đó.

Ngoài ra, bằng cách nhấn nút “Fix PID” tiện ích này cho phép khôi phục lại PID gốc (0x6001). Để phục hồi CRC đến địa chỉ 62 (0x03e) được viết 0. Chip giả mạo được khôi phục có thể được sử dụng bình thường nếu bạn làm việc với phiên bản trình điều khiển dưới đây 20814.

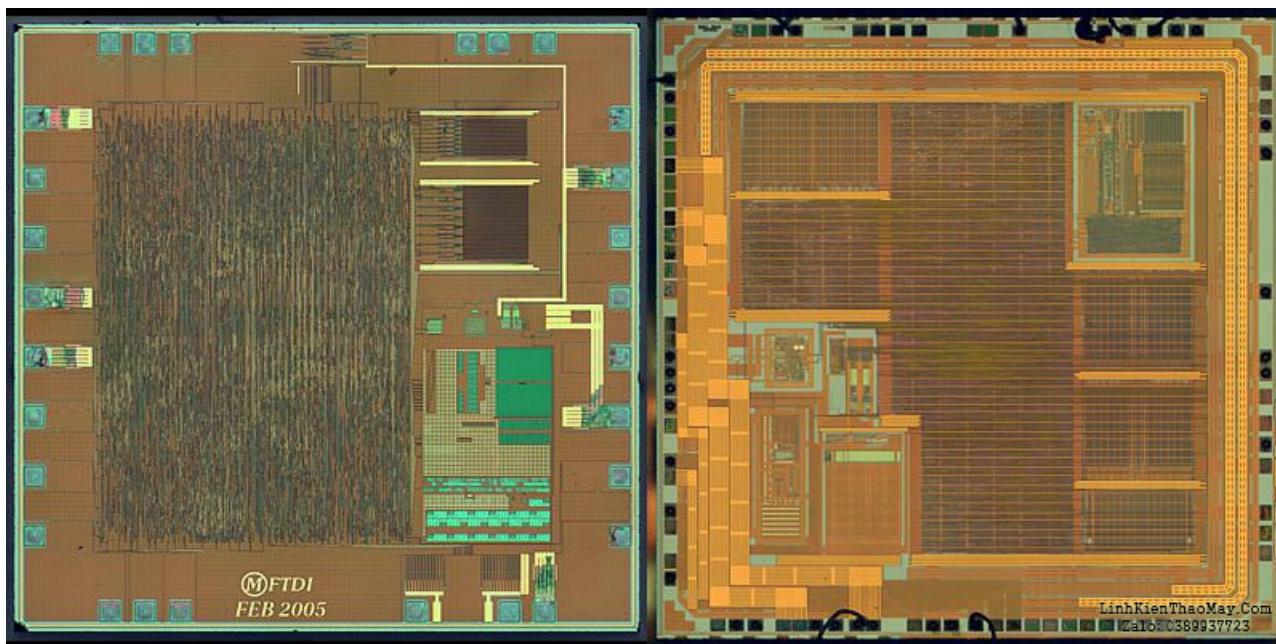
Xin chú ý! Để khôi phục lại một trình điều khiển bị hư hư chip, bạn phải cài đặt một trình điều khiển sửa đổi với các inf-file edited.



Hình. 3. Cửa sổ tiện ích phục hồi FT232RL.

By the way, tiện ích này định nghĩa FT232BM ban đầu với một EEPROM bên ngoài như FAKE. Đó là khá hợp lý, vì EEPROM bên ngoài cho phép bạn ghi lại một cách riêng biệt từ lẻ 16 bit và lẻ. Hóa ra, các phần vũng trong tab cite lái xe của riêng mình!

Đối với các thí nghiệm, mình đã lắp ráp hai bộ khung của adapter USB-UART trên FT232RL. Một cái được thu thập trên con chip gốc, một chiếc khác – giả mạo. Khi nó bật ra, có một cách dễ dàng hơn để phân biệt một giả: với chip gốc, tiêu thụ hiện nay là khoảng 9 mA, và cho một hàng giả mạo – nhiều hơn 35 mA. Các giả đã rất háu ăn! Tuy nhiên, điều này không đáng ngạc nhiên. Theo các bức ảnh của các tinh thể được hiển thị trong bài [Một cấp độ mới của giả mạo chip của Trung Quốc](#) có thể được nhìn thấy rằng đây là những chip hoàn toàn khác nhau.



Hình. 5. Topology của Chip. Chính hãng (trái) và giả (bên phải).

Phiên bản mới nhất của các trình điều khiển từ FTDI không có thiết hại PID, nhưng với sự giả, họ vẫn không có tác dụng. Các bài viết [FTDI Drivers Phá vỡ Chips Fake](#), [Một lần nữa](#) nó được báo cáo rằng các tài liệu không liên quan được đưa vào các dòng dữ liệu truyền đi, mà làm nhiễu loạn hoạt động bình thường của FT232RL stroystv giả, và khi bạn kết nối một thiết bị như vậy sẽ hiển thị một thông báo **"NON GENUINE DEVICE FOUND!"**.

[ftester.zip](#) (257 Kb) - lưu trữ với các tiện ích và các tập tin sửa đổi cho các trình điều khiển CDM20416 và CDM20814.

[ftester_source.zip](#) (17 Kb) - nguồn của tiện ích (C + + Builder 6).🌐

Các bài viết tương tự:

1. [Bếp từ China - Bật lên nguồn, xoong có từ tính, mạch nhân xoong bình thường. Đã thay thử 2 BJT 8550 8050 và 339. Không mã lỗi. chỉ nháy đèn khoảng 5 giây là tắt](#)
2. [bếp từ china - ngắt nguồn liên tục](#)
3. [bếp từ china.. - hư các phím ấn lúc dk lúc không...](#)
4. [Bếp từ supor china sdhs31-190 cs 1900w - Lỗi e1](#)
5. [Bếp từ Tcl china 088 - Mất nguồn công xuất](#)
6. [dau dia china - dau DVD mat mau chi con den trang](#)
7. [dell atx-s500w china - cam dien no cau tri chet di dodoe chinh luu](#)
8. [Đầu califonia MD188A china - Lỗi rom](#)
9. [hàng china :\)\) - báo lỗi E3 sau 1 time](#)
10. [media china MI-SV20DJ - cam dien mat tu bep khong nong](#)
11. [sp madein china axt-500 - mat nguon cap truoc](#)
12. [Thử bruteforce camera China và cái kết :D](#)