Replicant - Issue #1937

Liberate the bcm4334 wifi/bluetooth firmware

06/13/2019 03:52 AM - Kurtis Hanna

Status:	New	**Start date:**	06/13/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Wi-Fi	**Estimated time:**	0.00 hour
Target version:	Replicant 6.0	**Spent time:**	0.00 hour
Resolution:		**Device:**	

Description

The driver for this chip seems to already be free software and is in the mainline linux kernel: https://redmine.replicant.us/issues/1836

Cypress now owns the rights to the bcm4334 chips' firmware. To my knowledge, Cypress is more likely to say yes to a request that they release the source code to this firmware with a free software license than Broadcom would have been. I don't believe anyone has formally asked Cypress to do this. Since this chip is in a lot of Replicant's supported devices, it would make sense for our project to formally ask this of them.

The non-free firmware binary seems to be available here:
https://github.com/OpenELEC/wlan-firmware/blob/master/firmware/brcm/brcmfmac4334-sdio.bin

There were some efforts to hack this chip's firmware in the past, but it seems to not have gone anywhere...

https://forum.xda-developers.com/showpost.php?p=52499037&postcount=5
https://github.com/cociorbaandrei/bcmon
https://recon.cx/2013/video/Recon2013-Ruby%20feinstein%20Omri%20Ildis%20Yuval%20Ofir.mp4
https://recon.cx/2013/slides/Recon2013-Omri%20Ildis%2c%20Yuval%20Ofir%20and%20Ruby%20Feinstein-Wardriving%20from%20your%20pocket.pptx
https://bcmon.blogspot.com/
Some of this work seems to have been done by this developer, who we could maybe contact for help if we also want to hack the chip's firmware: https://github.com/shooteshoote@gmail.com

History

#1 - 07/30/2019 07:25 PM - Kurtis Hanna

Some more information about this has been added to our wiki: https://redmine.replicant.us/projects/replicant/wiki/WiFi#section-6

Also, here's a link to a bcm4334 devkit of sorts: https://store.embeddedworks.net/wlan670/#tab-label-additional

#2 - 08/02/2019 05:00 PM - Anonymous

I'm not a hardware guy, but in my opinion, a more direct way to create a dev kit is to buy a few of these:
https://www.aliexpress.com/item/32871146311.html

Then, buy an appropriate BGA to DIP adapter (the bcm4334 is strange (10x11), I'm not sure if getting a bigger one (11x11) would do the trick), and solder the bcm4334 to it (this step requires BGA soldering skills, which as I understand, aren't very common), wire it up properly and start hacking:
https://www.proto-advantage.com/store/index.php?cPath=4000

By the way, the pinout of the bcm4334 is labeled on page 90 of the datasheet:
https://www.cypress.com/file/298706/download