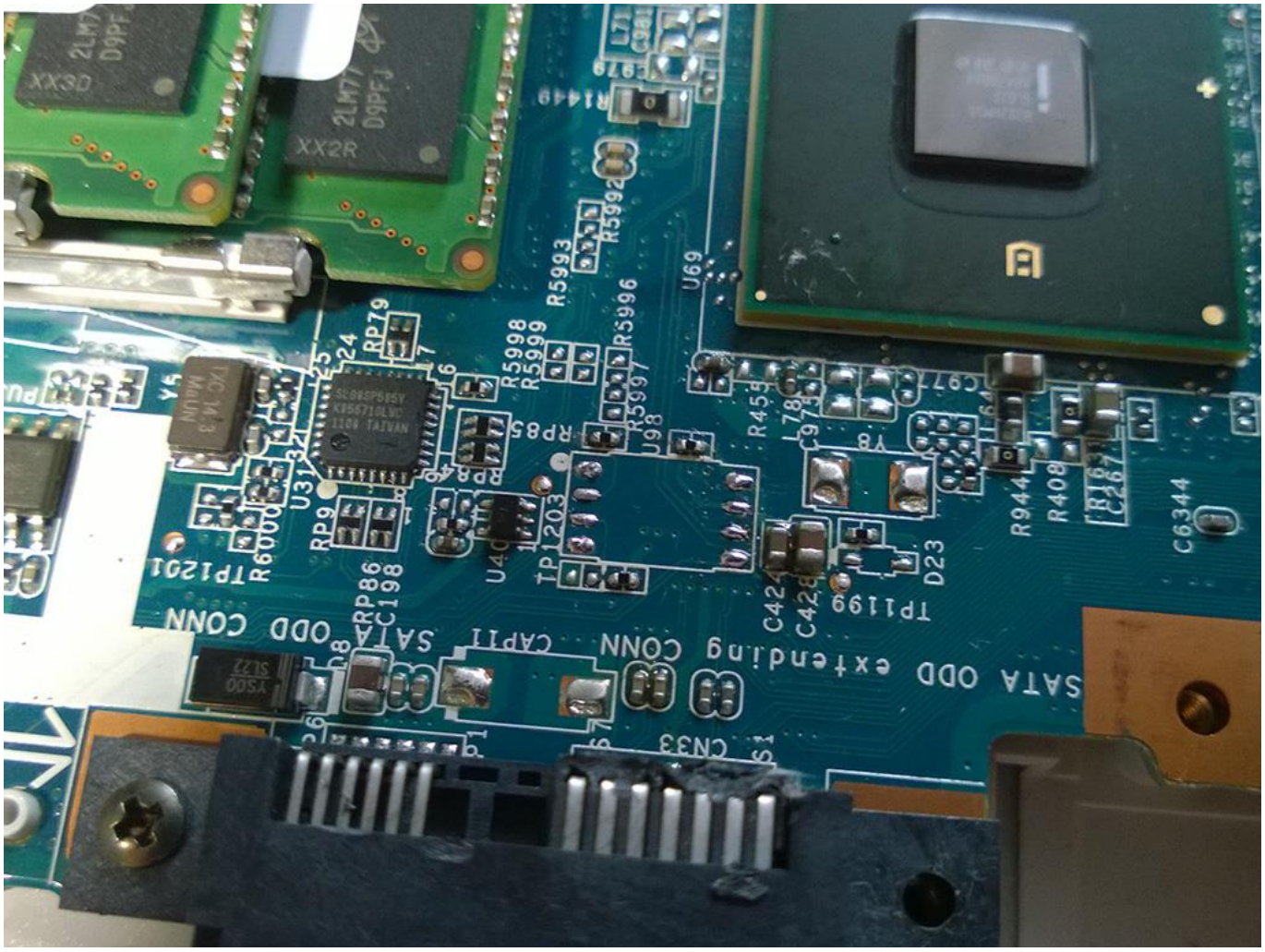
JACKSOFT LABS

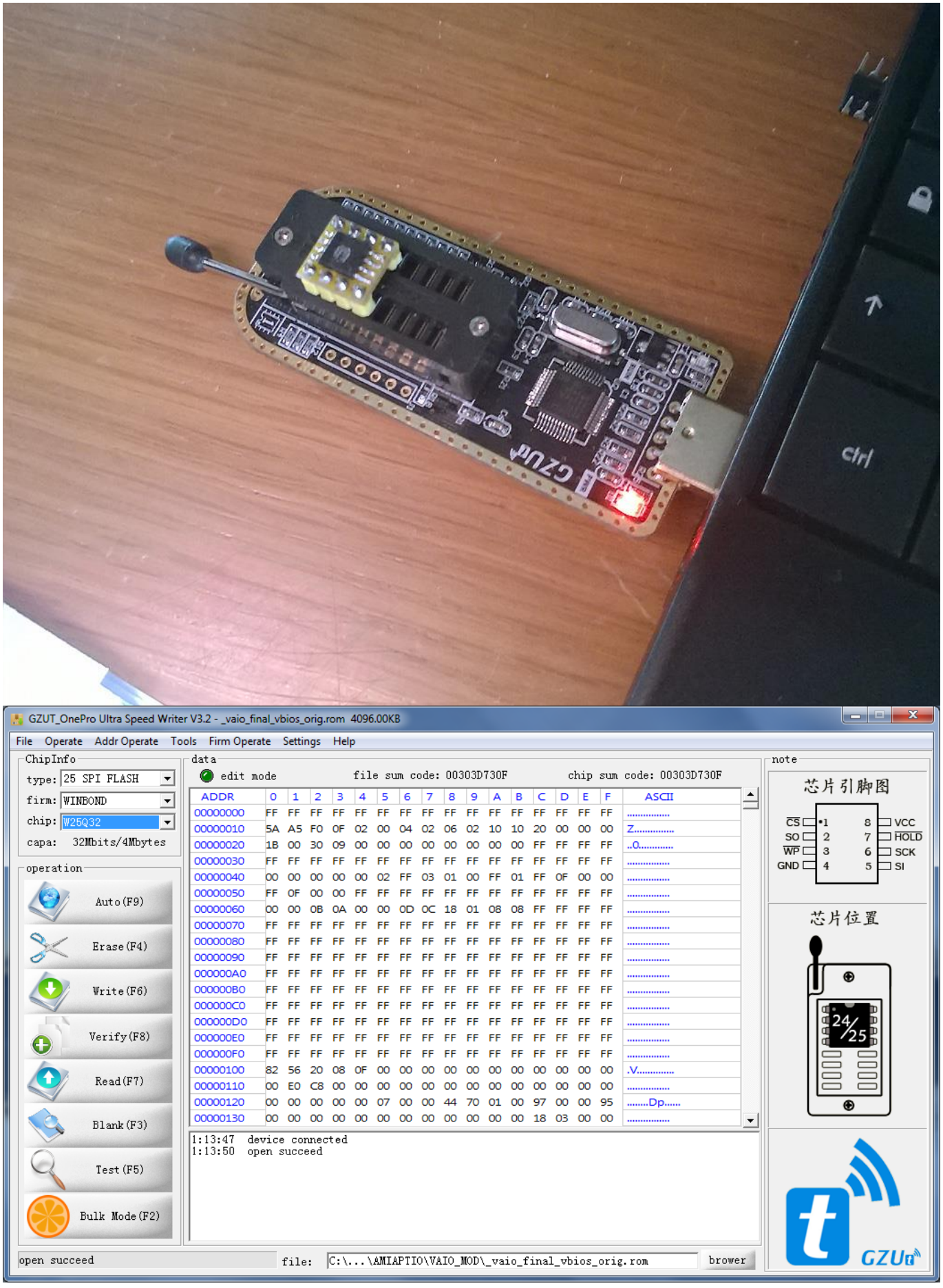
VAIOGEDDON

Update x1

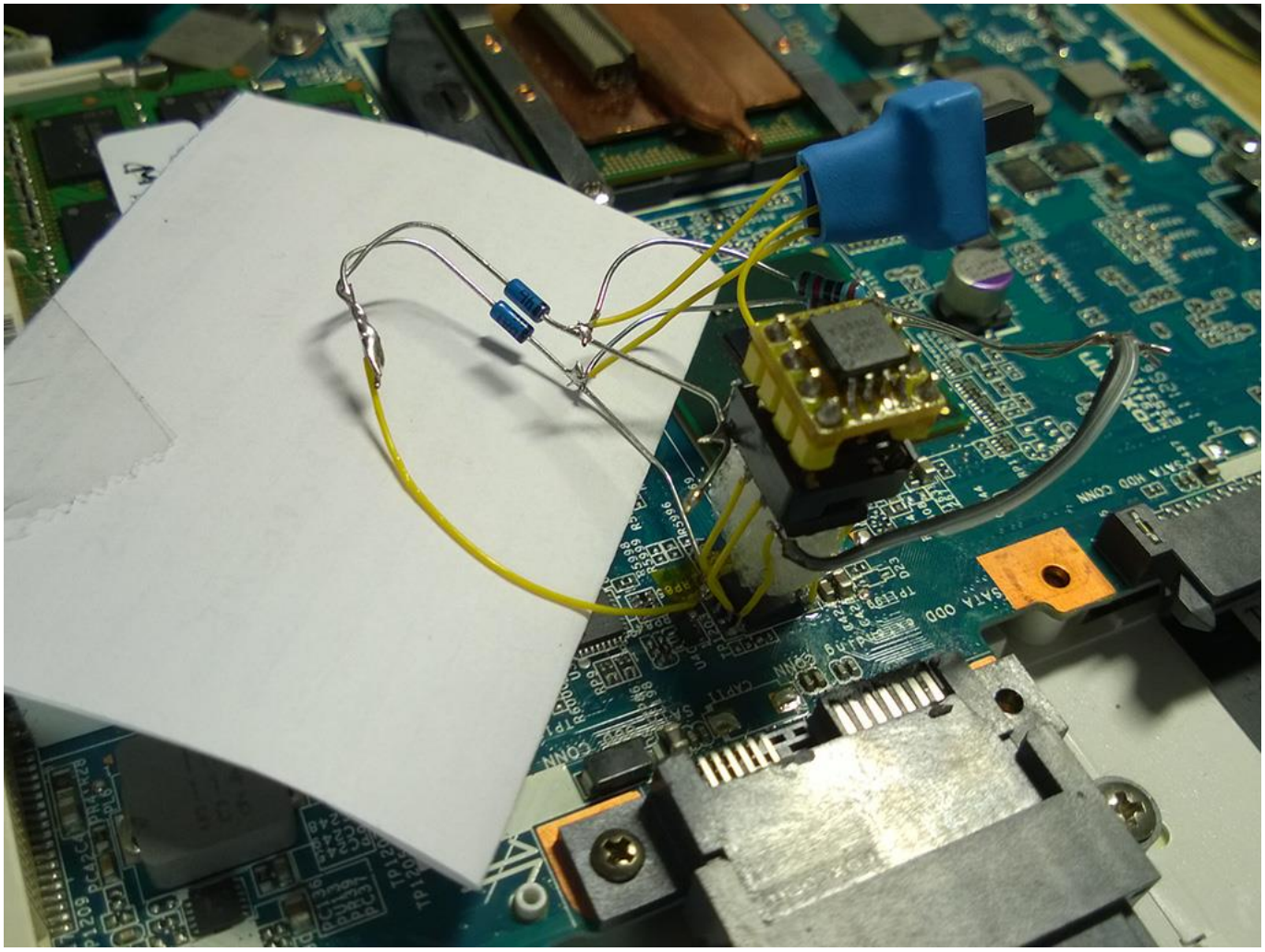
Do you remember when Sony denied me support for my VAIO laptop?
After some research I've found a way to do some modifications and discovers on my VAIO BIOS. Thanks to my partner in science I've bought, for a bunch of euros, a very good USB SPI reader/writer and finally decided to make a full dump of my BIOS just to try some mods and updates.

My first attempt was to dump the BIOS with the laptop set to Off and, as a result, I only got bad dumps. After looking a YouTube guide I decided to remove the chip and do a full dump again. And I got, finally, good dumps.




GZUT_OnePro Ultra Speed Writer V3.2 - _vaio_final_vbios_orig.rom 4096.00KB
File Operate Addr Operate Tools Firm Operate Settings Help
ChipInfo
type: 25 SPI FLASH
firm: WINBOND
chip: W25Q32
capa: 32Mbits/4Mbytes
operation
Auto(F9)
Erase(F4)
Write(F6)
Verify(F8)
Read(F7)
Blank(F3)
Test(F5)
Bulk Mode(F2)
data
edit mode
file sum code: 00303D730F
chip sum code: 00303D730F
ADDR 0 1 2 3 4 5 6 7 8 9 A B C D E F ASCII
00000000 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000010 5A A5 F0 0F 02 00 04 02 06 02 10 10 20 00 00 00 Z.....
00000020 1B 00 30 09 00 00 00 00 00 00 00 00 FF FF FF FF ..0.....
00000030 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000040 00 00 00 00 00 02 FF 03 01 00 FF 01 FF 0F 00 00
00000050 FF 0F 00 00 FF FF FF FF FF FF FF FF FF FF FF FF
00000060 00 00 0B 0A 00 00 0D 0C 18 01 08 08 FF FF FF FF
00000070 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000080 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000090 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000D0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000100 82 56 20 08 0F 00 00 00 00 00 00 00 00 00 00 00 .V.....
00000110 00 E0 C8 00 00 00 00 00 00 00 00 00 00 00 00 00
00000120 00 00 00 00 00 07 00 00 44 70 01 00 97 00 00 95 ....Dp....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 18 03 00 00
1:13:47 device connected
1:13:50 open succeed
note
芯片引脚图
CS 1 8 VCC
SO 2 7 HOLD
WP 3 6 SCK
GND 4 5 SI
芯片位置
24/25
GZUt
open succeed
file: C:\...\AMIAPTIO\VAIO_MOD_vaio_final_vbios_orig.rom
brower

But since I have to flash and test many variants of the BIOS mod, why don't we add another "feature"? If you have read the Dreamcast BIOS hack article you will probably remember that I decided to put a second flash memory on the mainboard to have a Dual-BIOS solution! (the original flash memory with the original BIOS, the second flash memory with the development/final BIOS mod.)



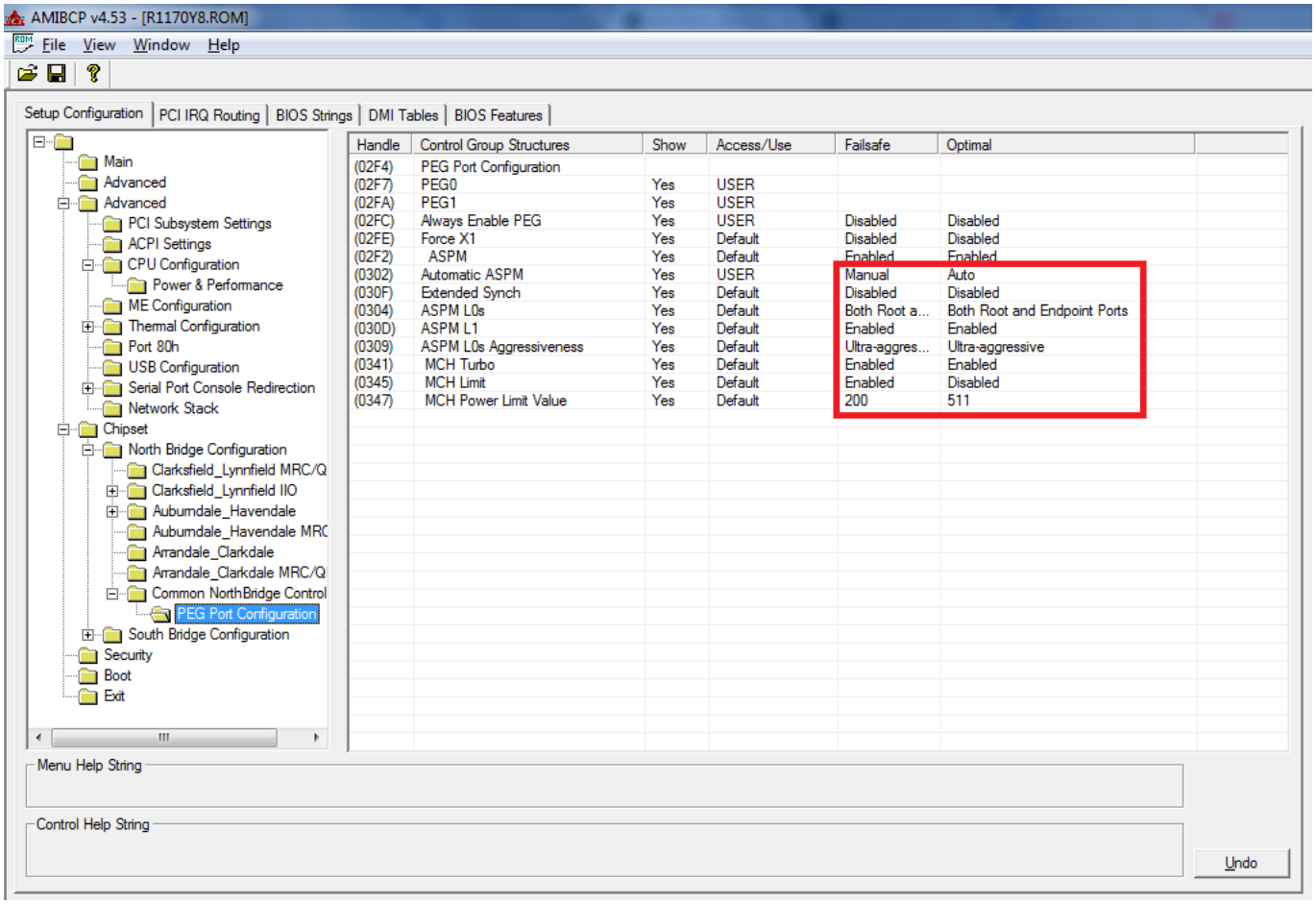
With a bit of research I found that the BIOS is divided in two parts. The first part is the ME Region and the second is the AMI Aptio BIOS. Some other OEMs have the ME Region in a second flash.

Note: The BIOS is a unique file of 4096KB, I virtually split it in two parts of 2048KB each just to easily understand how my VAIO BIOS is made.

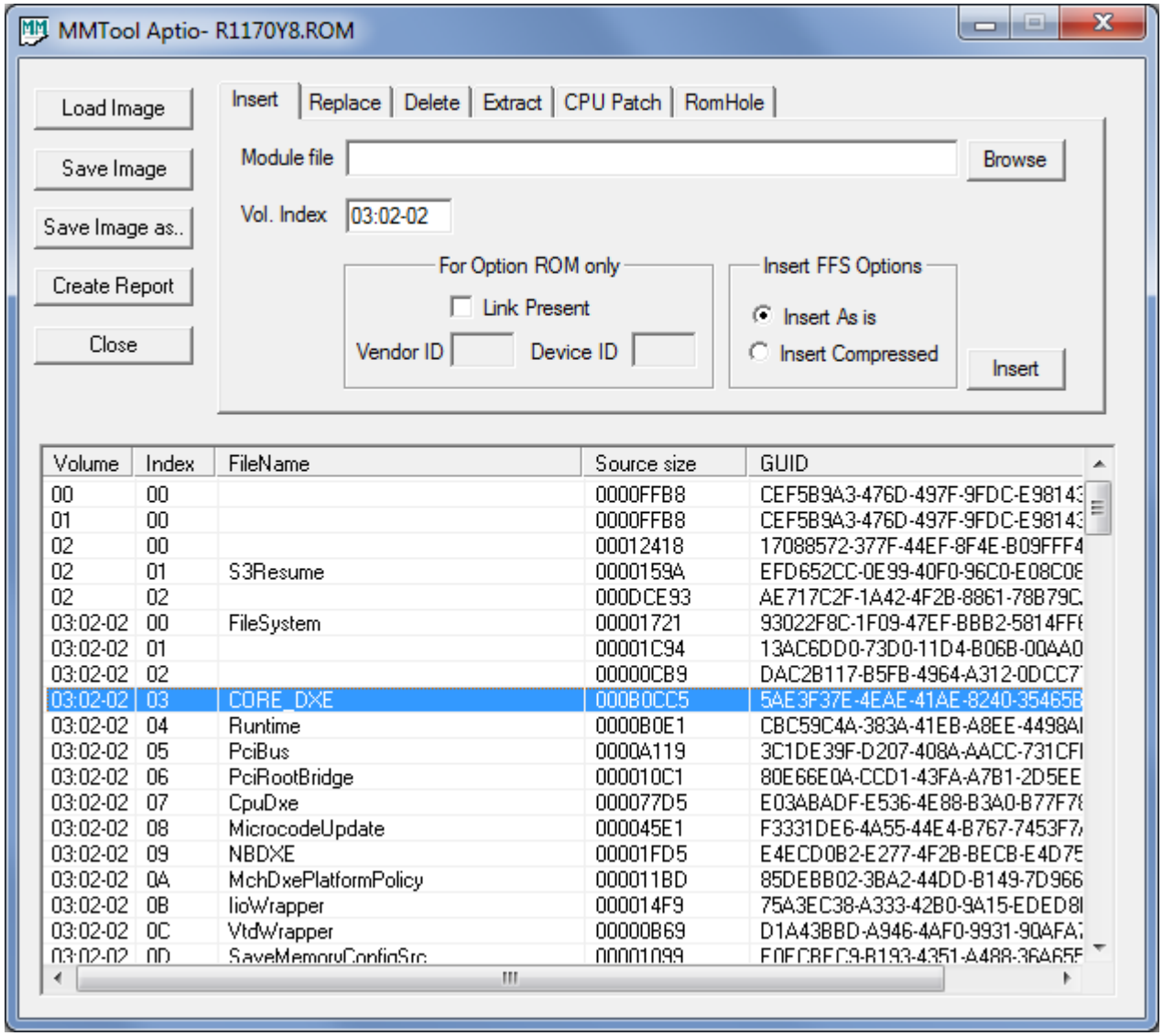
The ME (Management Engine) region is a firmware provided by Intel to manage communications between the chipset, the devices and the OS and, on some VAIO models, is not directly upgradable. The full SPI dump has given me the ability to update it, thanks also to some tutorials found in a forum.

To begin with, we're going to have a look at the second part, the AMI Aptio BIOS.

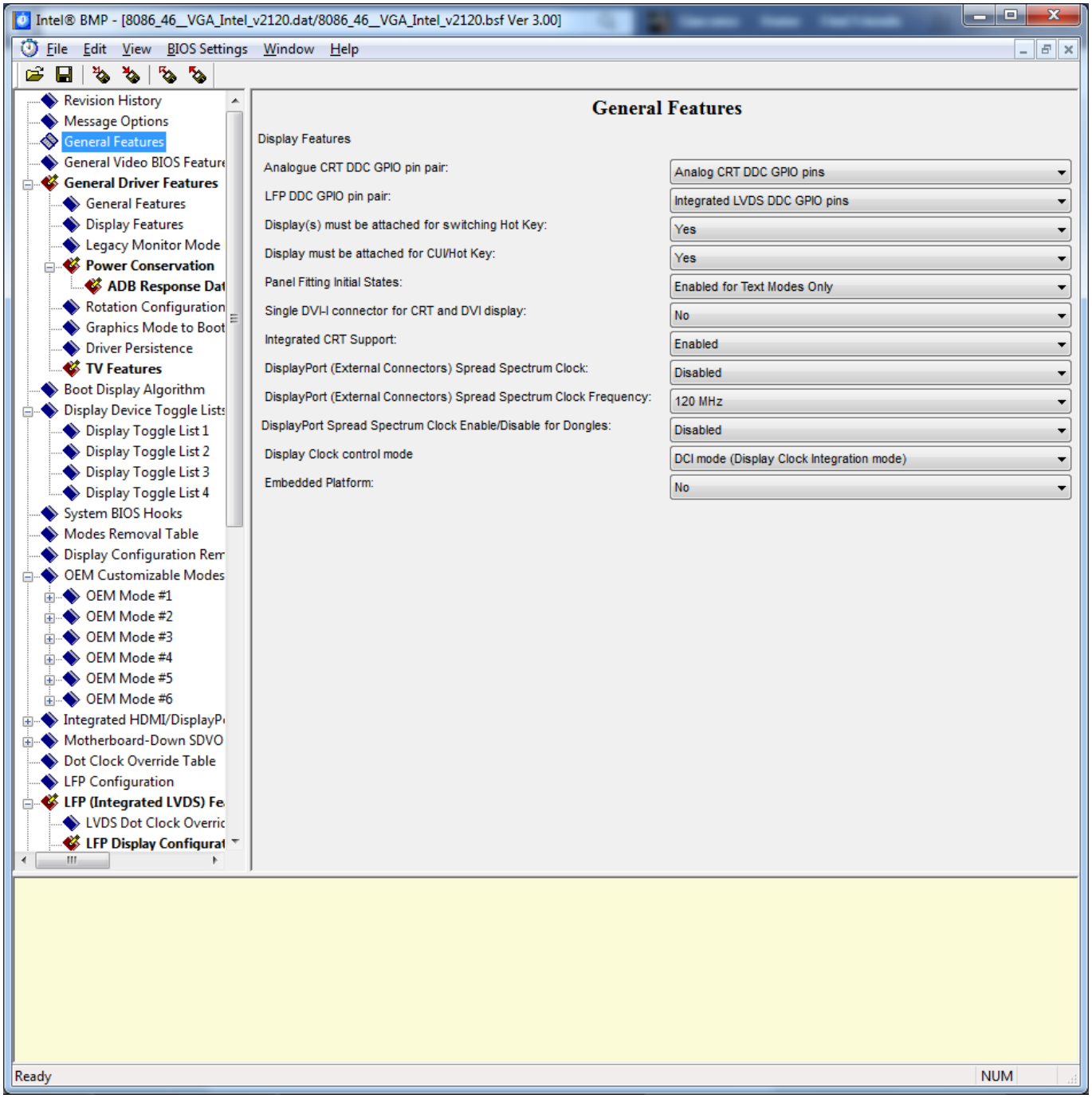
A reliable dump is very important, because I'm certain I can modify all that I want (to the best of my knowledge. First I've opened the ROM image with AMIBCP. AMIBCP (AMI BIOS Configuration Program) is a tool that let the dev/user to modify the existent menu in the AMI Aptio BIOS, to set new default values and to hide/show some menus. I've just unlocked some menus and changed default settings to some limits that could improve performances a bit (also regarding VT-D function… If you're a VAIO user you sure know what I mean).



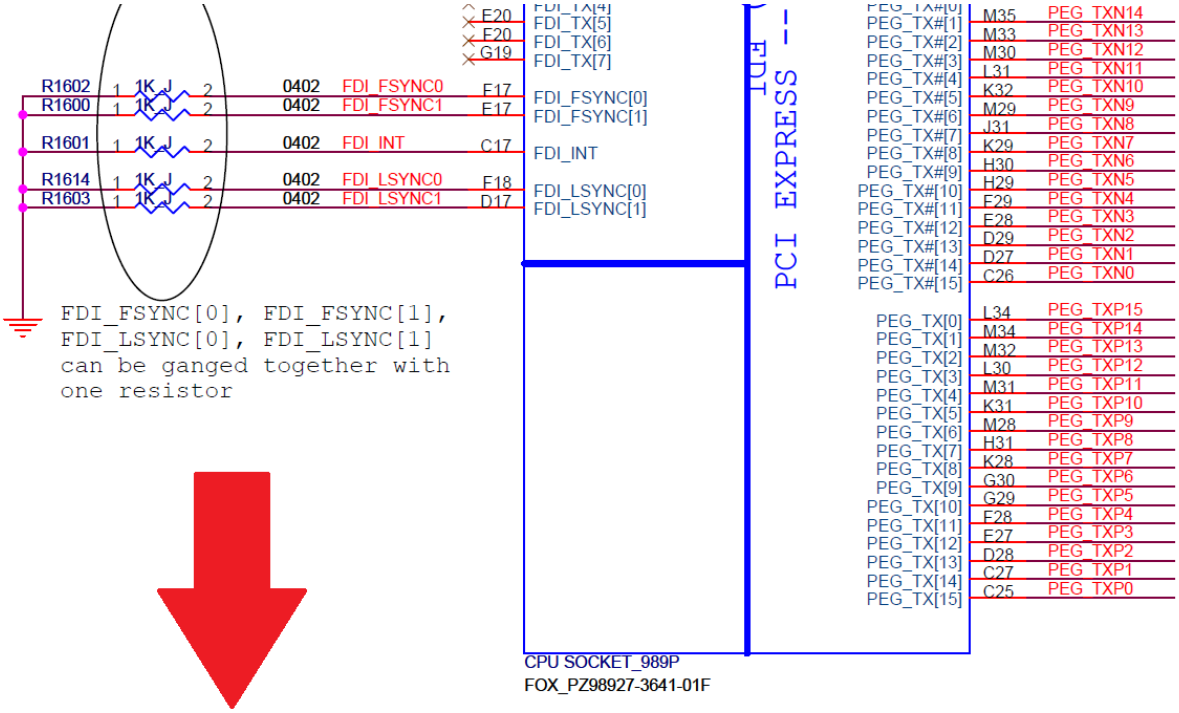
I will not write here how many things I've changed and tested with a lot of reflashing, I spent about 1 month to consider my work as "final".
Once I was done with this, I decided to upgrade, wherever possible, my O-ROM modules and to do this I used AMI MMTool Aptio.



Valid O-ROM modules were Intel HD Graphic, ATI Mobility Radeon (HD5650) and Marvell LAN. I found a good guide for Intel HD O-ROM modifications/upgrades, because it needs to be set before replacing in ROM file.



But that's not all. By looking at some other BIOSes with my same CPU, I've found that the Intel HD Graphic O-ROM module name is "8086, 46" (8086 is Intel's VendorID, 46 is ProductID), mine had two O-ROM (VBIOS, in this case), both with the same config, and the module name was "8086, fff" and "8086, ffe". What's that? After two weeks of hard research and tests I found that the Intel HD Graphics NEVER existed! Why? Simple! SONY PERMANENTLY DISABLED IT VIA HARDWARE!!!




```
For Disable Arrandale Graphic
In addition, FDI_RXN_[7:0] and FDI_RXP_[7:0] can be left floating on the PCH.
FDI_TX[7:0] and FDI_TX#[7:0] can be left floating on the Arrandale. The
GFX_IMON,FDI_FSYNC[0], FDI_FSYNC[1], FDI_LSYNC[0], FDI_LSYNC[1], and FDI_INT
signals on the Arrandale side should be tied to GND (through 1-kΩ ±5% resistors).
FDI_FSYNC[0], FDI_FSYNC[1], FDI_LSYNC[0], FDI_LSYNC[1] can be ganged together with
one resistor.
```

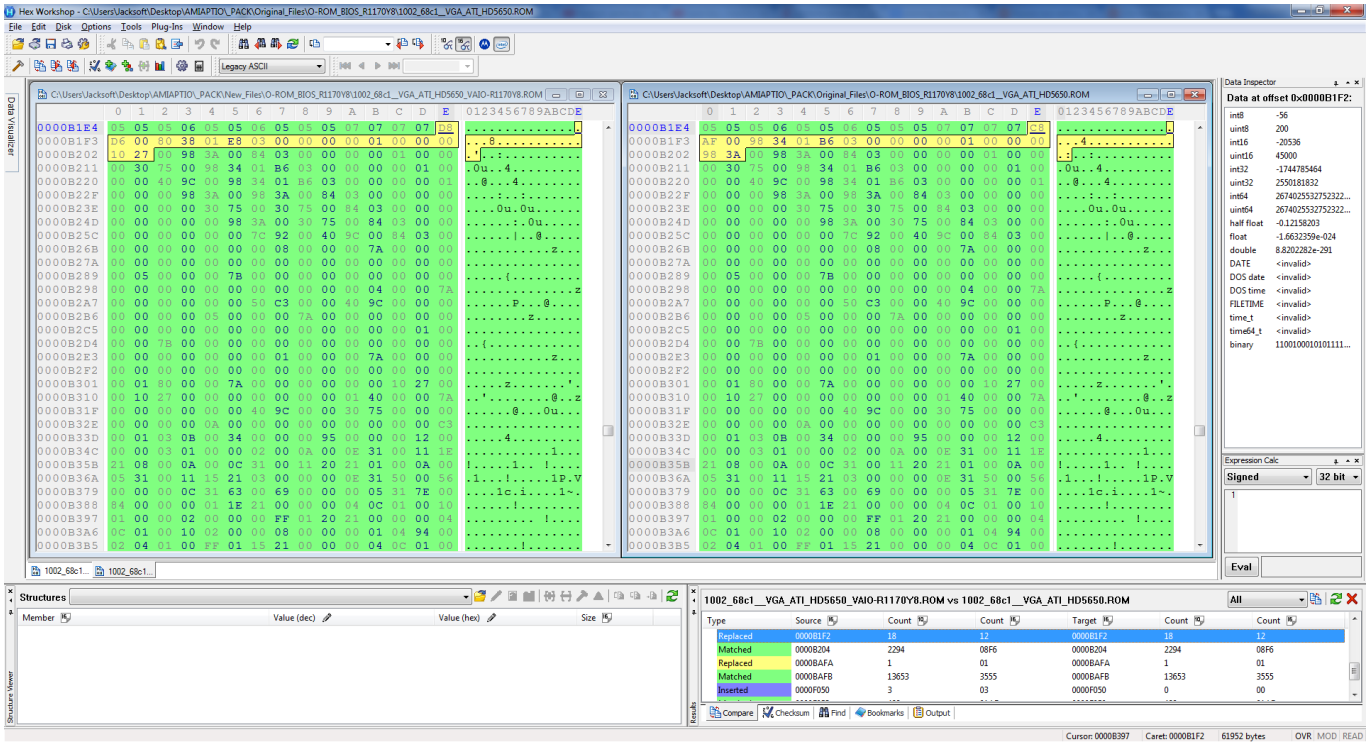
Why Sony would disable switchable graphics? Why not a software solution (in BIOS) but a hardware one? Of course, Sony will never tell us why.
After this I've looked for the ATI Mobility Radeon HD5650 O-ROM module (VBIOS, also in this case) and I found that another, but older, VAIO model have the same GPU, so I searched for the BIOS on the internet and dumped the VBIOS. I've also found VBIOSes about HD5650 on other laptop brands, more recent than mine, but I had some troubles with video outputs: that's because Intel HD was permanently disabled as described before, so I've made some test just with the other VAIO VBIOS.

I've found no differences and improvements but some people on the internet suggested me to remain with the stock VBIOS because the older one could have different VRAM timings and other parameters that could make my machine unstable or damage it, and so I rolled back to the stock VBIOS.

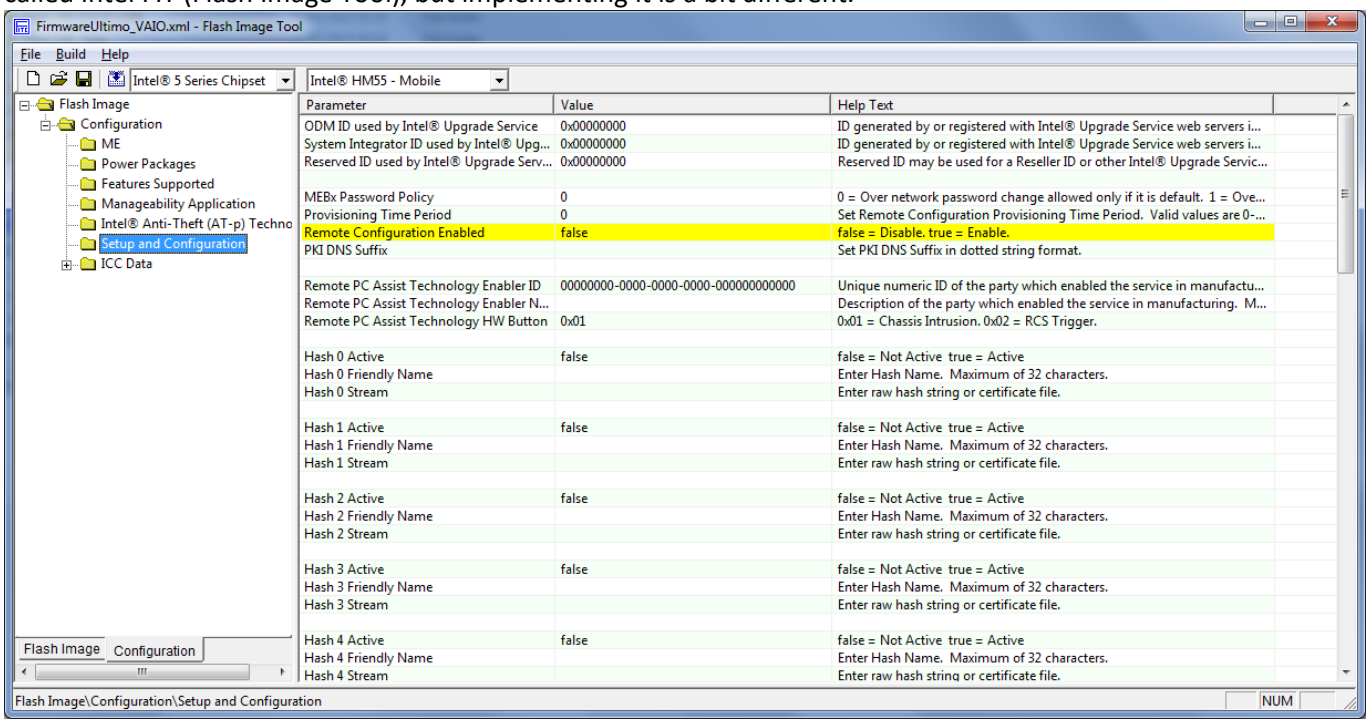
Sony not only has disabled Intel HD GPU, but also DOWNCLOCKED the ATI one!

I asked myself: why not having the Intel HD too, as it does not use much power when on battery?

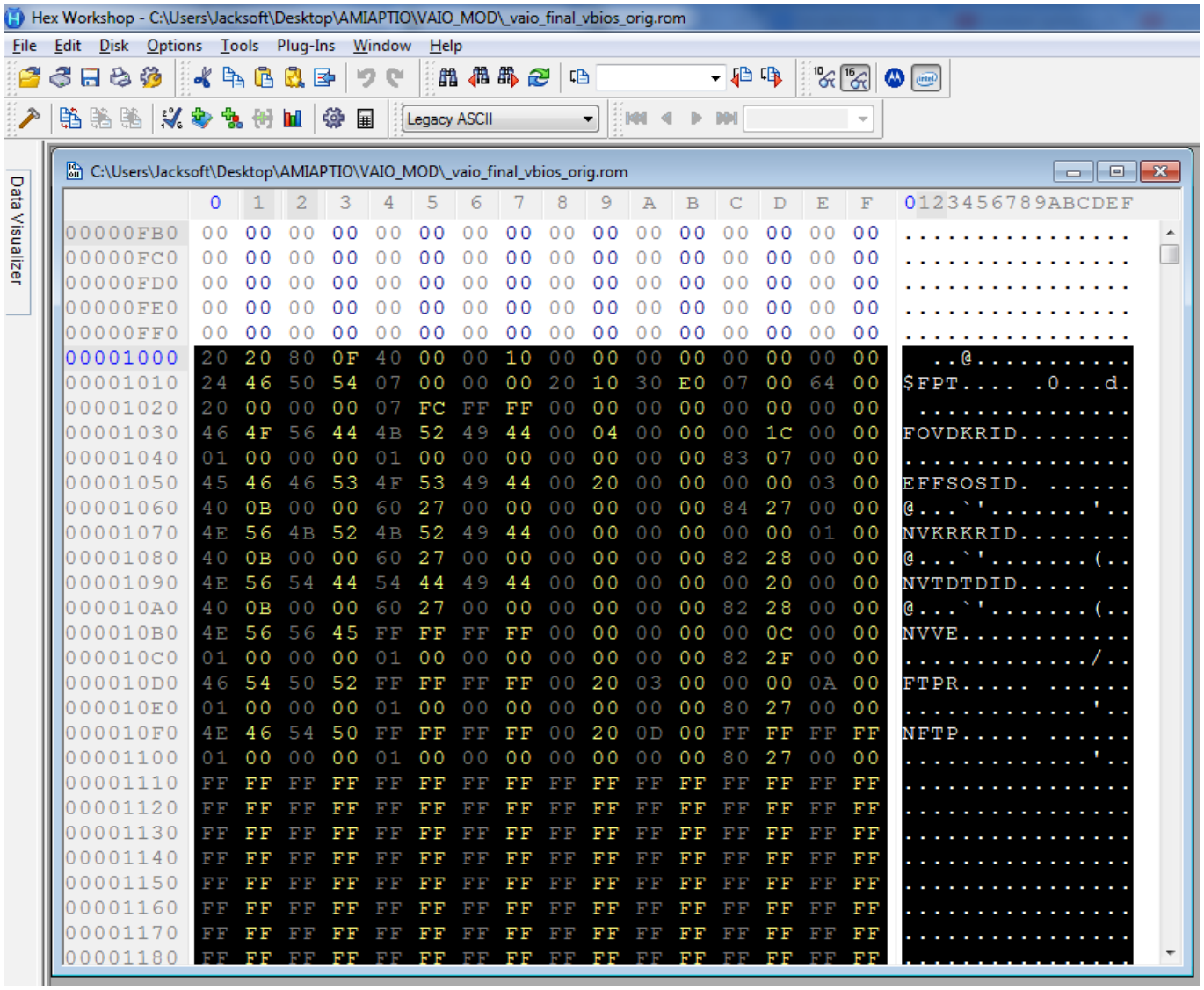
After reading many forums and doing a lot of research I've found how to increase stock clocks (450MHz for GPU @ 0.90V and 790MHz VRAM) with RBE (Radeon BIOS Editor) and some Hex editing to the right frequencies, same as ALL OTHER LAPTOPS BY OTHER BRANDS! (550MHz for GPU @ 1.00V and 800MHz VRAM). It was hard because I've never managed things like this (the voltage table made PowerPlay always stuck on max frequencies), but hey! Now I can have more FPS in games! :D



Now the simplest part, Marvell LAN O-ROM.
By looking at Marvell LAN I've found that it was an "alpha" build. It worked very well, never a problem, but why not a stable? Never an update by Sony… Not a problem, I'll dump from another BIOS ;)
After a bit of search I've discovered that EVGA made a 400$ motherboard that use the same Ethernet chip (Woah!). Grabbed the updated BIOS from official support site, opened with MMTool, grabbed the new O-ROM and replaced in my modded BIOS. It works perfectly :D
I've also updated some CPU microcodes. Maybe they are not essential, because OSes like Windows just update microcodes via Windows Update, so they will be loaded on boot.
Let's go back to the first part of the BIOS, ME firmware update.
As I said before, I've found no differences between the old and the new firmware, but why we shouldn't update it? Like Intel HD Graphic here we have a tool that can read the original values and copy to the new vanilla firmware, called Intel FIT (Flash Image Tool), but implementing it is a bit different.



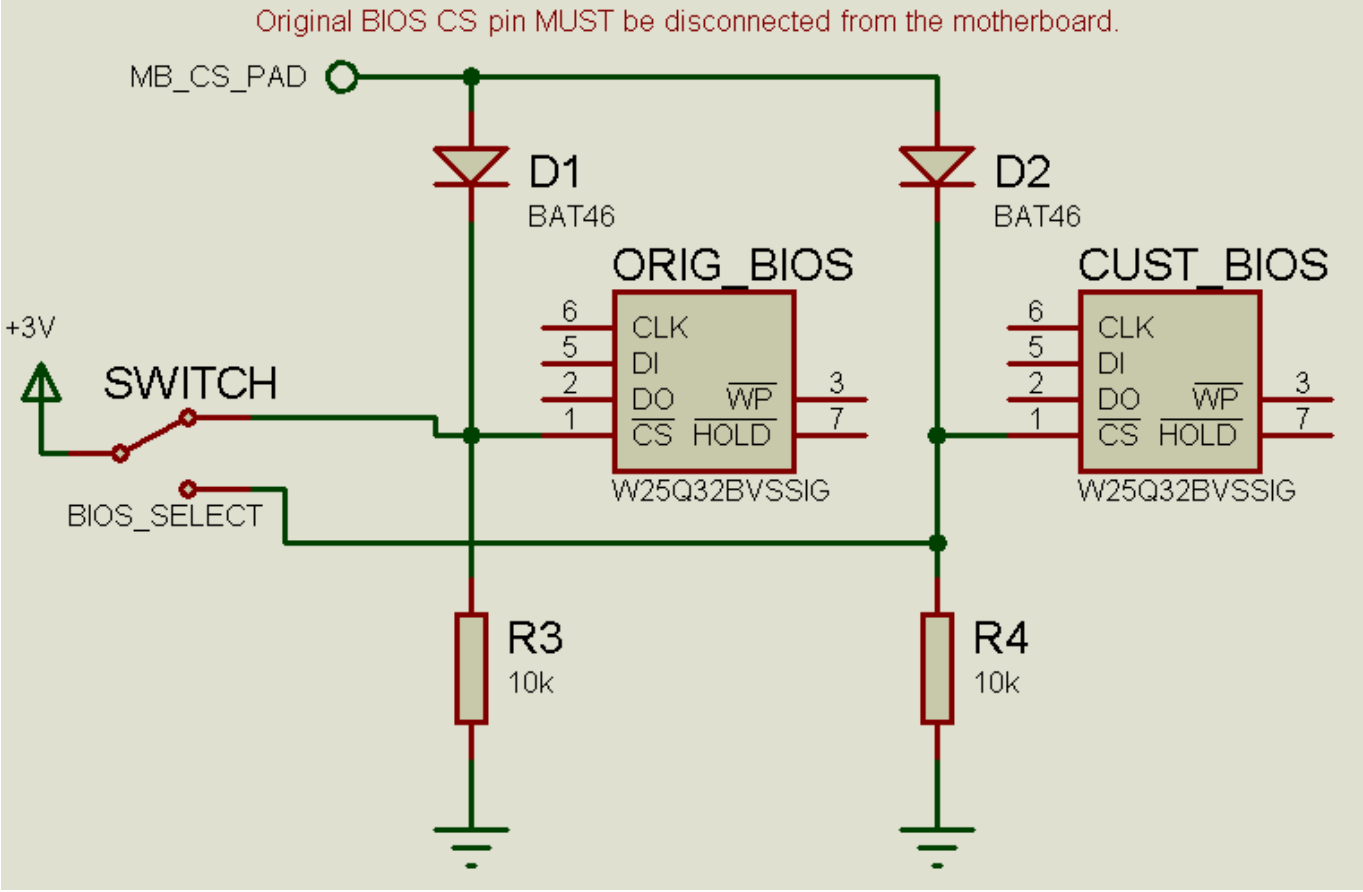
As suggested on some forums, the only way to do this is hex-editing, in my case, the first part of the BIOS. The only important thing is to select the right output format, so you can obtain the firmware file in the right size and then replace easily the older one.

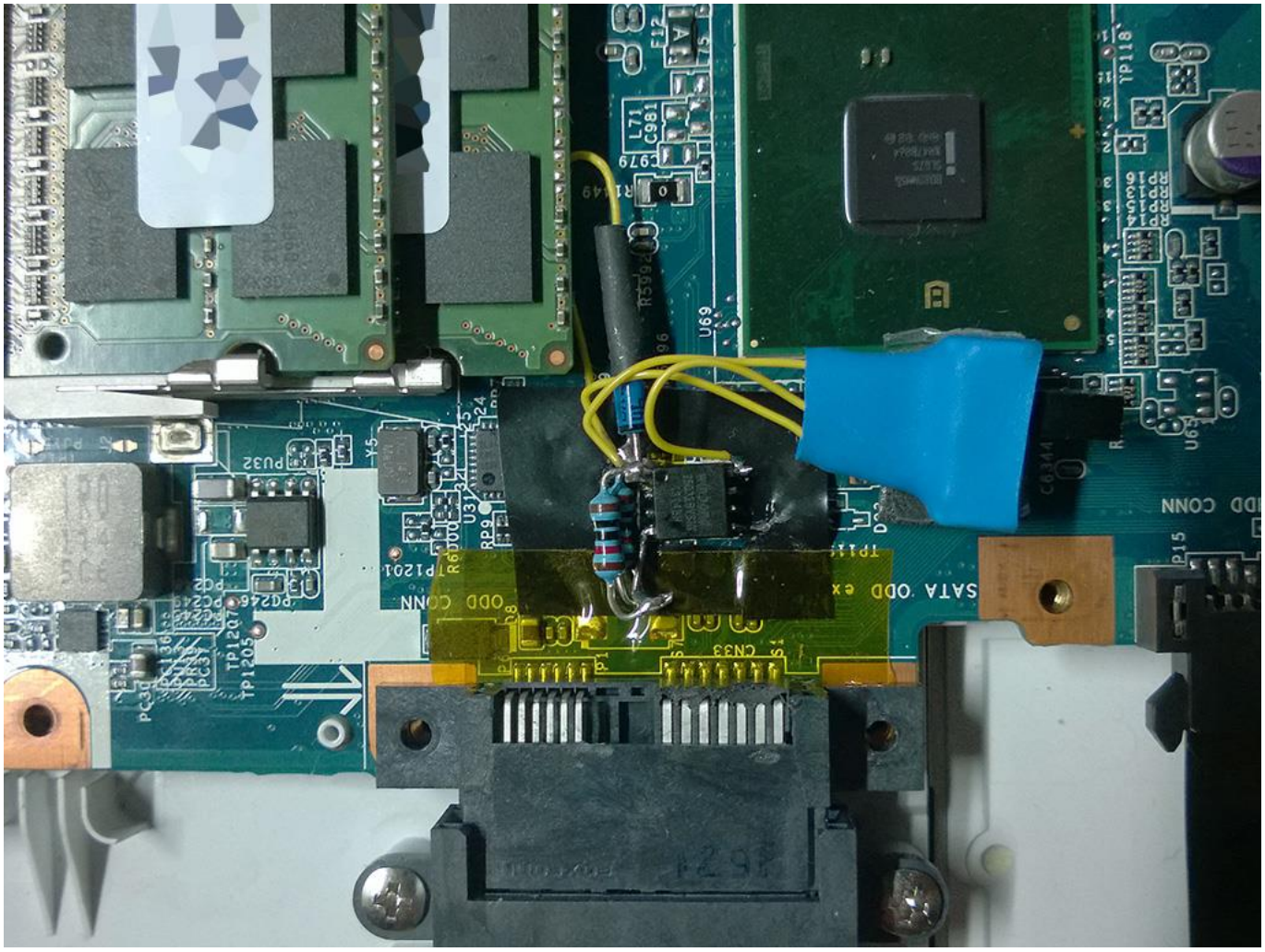


The last thing: UEFI Boot.

Unfortunately it was pretty impossible to enable it, because it was permanently removed from the BIOS. Maybe it can be added via modules, but I don't know where to grab and how to enable it.
As I said, after a month of research and tests I've just made these changes:
– Dual-BIOS solution. Good for brick-free tests.
– Updated Intel VBIOS from v2009 to v2120 (Without results, because it's disabled)
– Updated Intel ME Firmware from v6.0.31.1208 to v6.1.20.1059
– Updated i5 480M CPU Microcodes from revision 02 (2010) to revision 04 (2013) (also updated microcodes for some other CPUs)
– Updated Marvell 88E8059 O-ROM from v6.65.1.1 (alpha) to v6.68.1.3
– Unlocked advanced BIOS submenus and options (but they're not visible, don't know why)
– Increased ATI VBIOS frequencies from 450/790MHz (0.95V) to 550/800MHz (1.00V)
– New bootlogo B-) (Oh, yeah! I've just improved the old one!)

About the Dual-BIOS mod: here is the schematic according to the flash memory datasheet: *The SPI Chip Select (/CS) pin enables and disables device operation. When /CS is high the device is deselected and the Serial Data Output (DO) pin is at high impedance. When deselected, the devices power consumption will be at standby levels unless an internal erase, program or status register cycle is in progress. When /CS is brought low the device will be selected, power consumption will increase to active levels and instructions can be written to and data read from the device. After power-up, /CS must transition from high to low before a new instruction will be accepted.*





READ THE DISCLAIMER AT THE END OF THIS ARTICLE FIRST!!!
To mod/reflash your BIOS you do not need the Dual-BIOS mod. Dual-BIOS mod is only for hardcore users :-)
Here are the ME firmware, VBIOS and O-ROM used for this mod:
Original+Modded VBIOSes/Modules/ME Firmware

And here there are the already modded Aptio ROM images for both VAIO models (Only AMI Aptio Image, 2nd part. If you want to also update the ME firmware you will have to make a full SPI dump and replace it via hex-editor by yourself). Remember that YOU MUST compare with your laptop original ME firmware and check if there are some bits to sets via Intel FIT, otherwise your machine could work badly or not work at all.
AMI BIOS/Firmware Update Utility 32/64bit (Directly from AMI website)
R1170Y8 Modded BIOS v0.4
R0300Y8 Modded BIOS v0.3* (WARNING: NOT fully tested on real hardware! I can't verify if it works correctly!)
* Due to missing original Intel HD script file I was not able to update the Intel VGA O-ROM module. If anyone own the "ilm_1930.bsf" script file (Ironlake Mobile v1930) please contact me on Twitter.

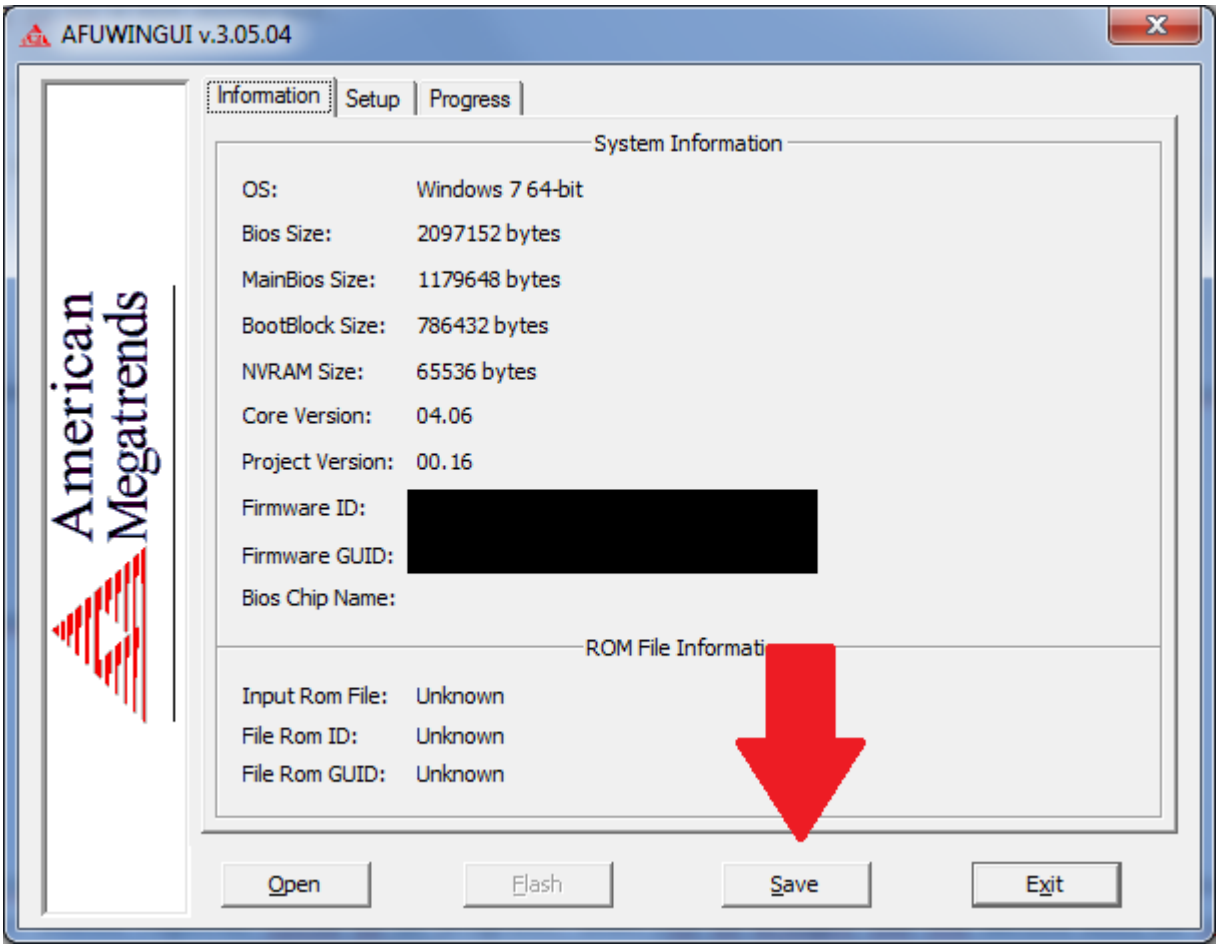
Note: I can't public software like AMIBCP, MMTool, Intel BMP and Intel FIT, because of copyright. Try search them on Google! :P

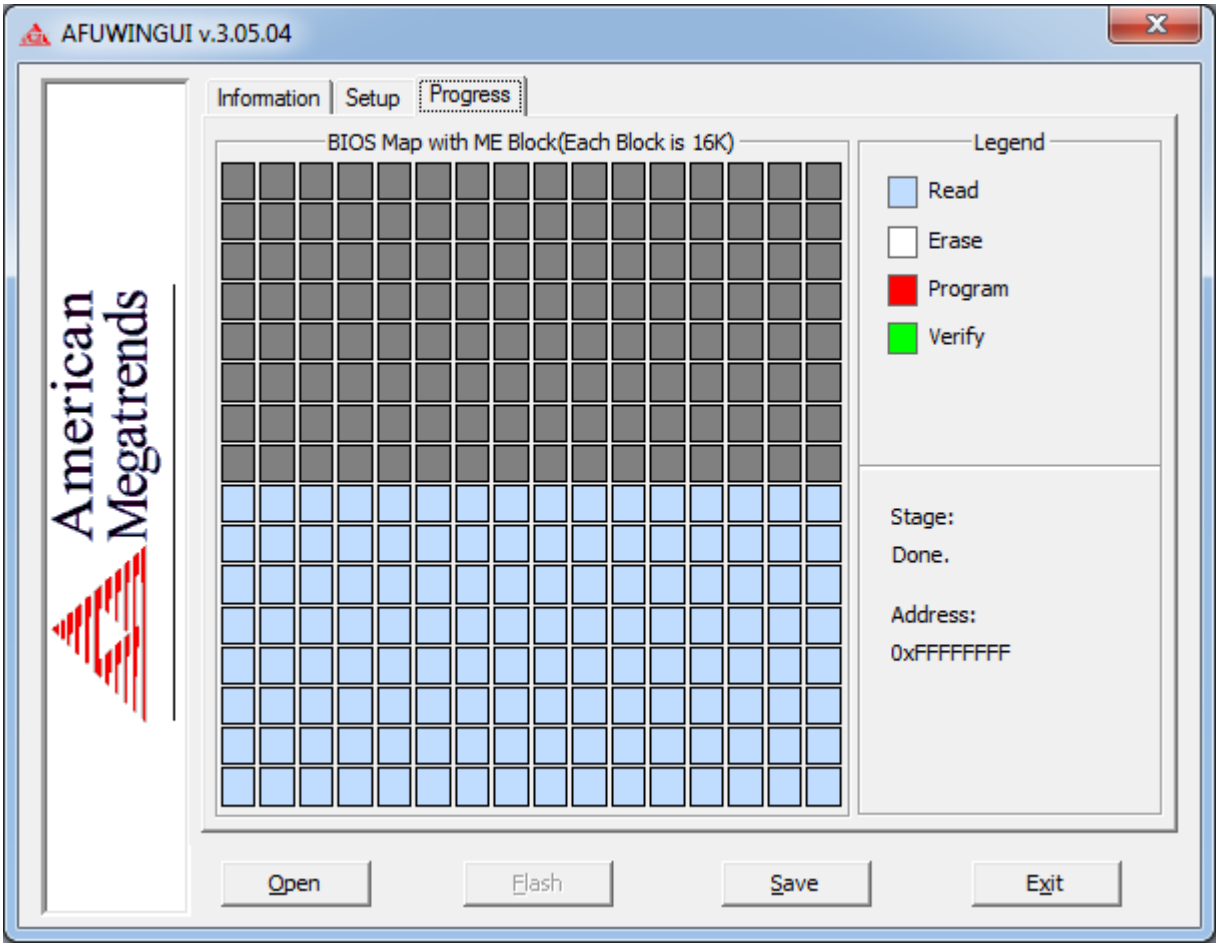
How to flash:

IMPORTANT: Before flash, check which BIOS version you have. To check this: shutdown your laptop, power it on and press immediately and repeatedly “F2” button on keyboard, you’ll enter in the BIOS menu. Read “BIOS Version” and check if it’s “R1170Y8” OR “R0300Y8”. If your BIOS IS NOT named as one of these two DON’T GO FORWARD! DO NOT FLASH ANYTHING!!!

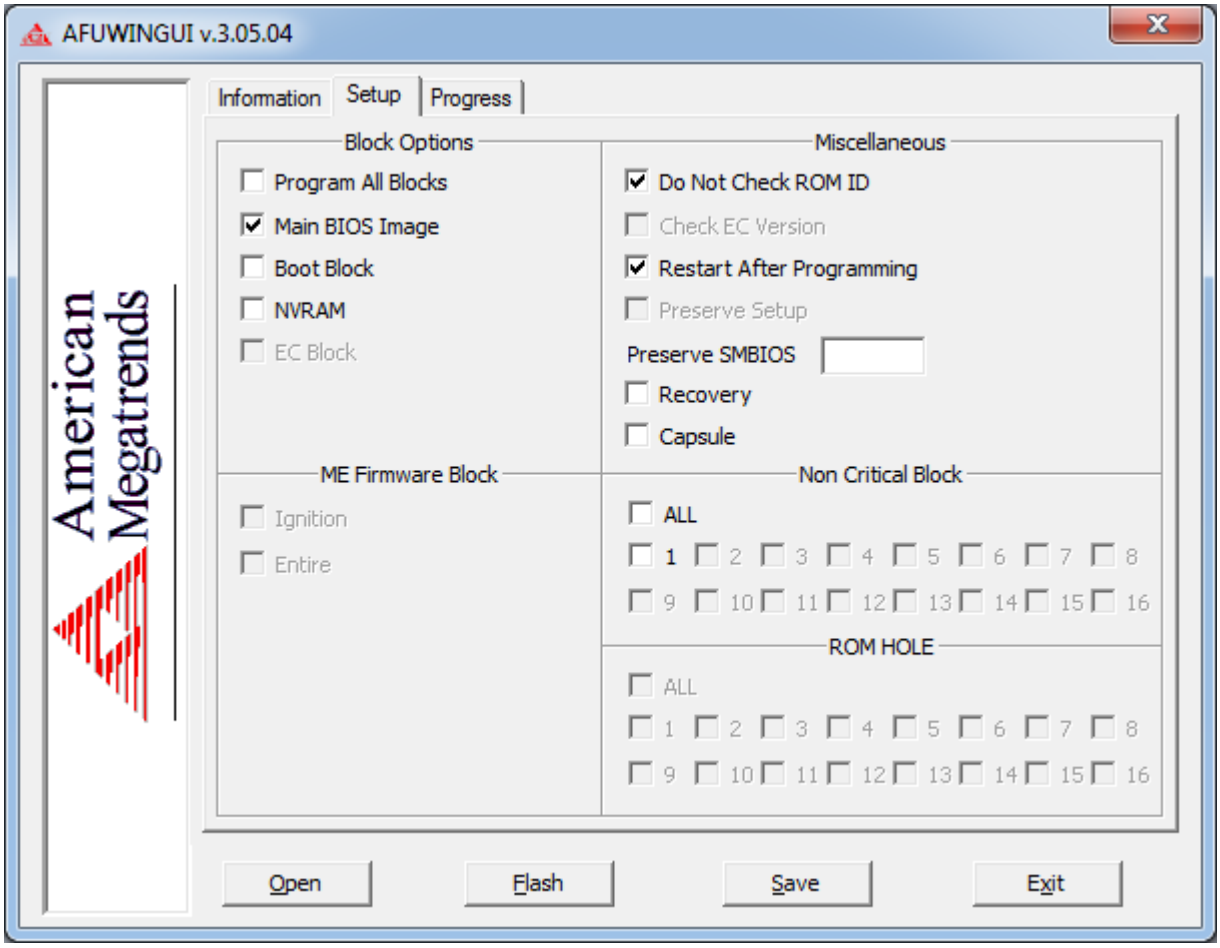
To prevent any problem close all programs, and also disable the antivirus. Some programs can interfere with the BIOS flash and in result you can BRICK your machine!

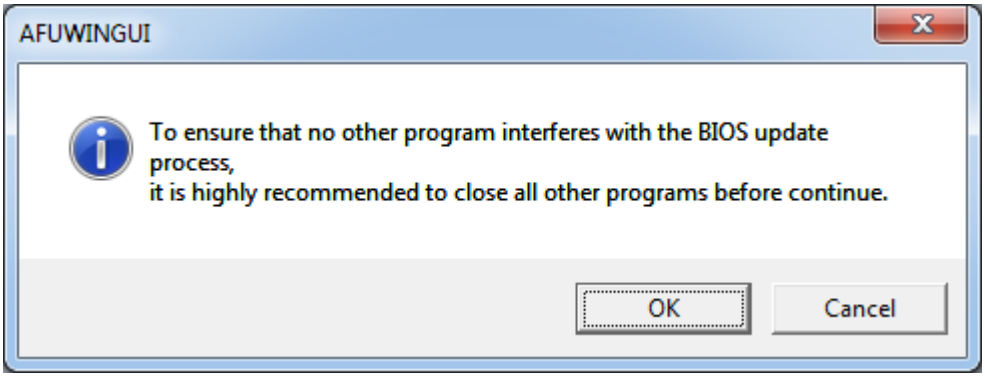
Note: You’ll hear the fan spinning to the maximum speed and in some operation (read or write) your mouse and keyboard will be temporarily disabled, this is normal.
Open AfuWin (select 32 or 64bit, depends on your OS), and first make a backup of your current ROM by clicking on the “Save” button. Write a name for your BIOS (eg. my_bios_ok.rom), if you want, and save in a known location to easily retrieve it if you need to. Be sure to make multiple copies of this backup (on external drive like USB pendrives, etc).

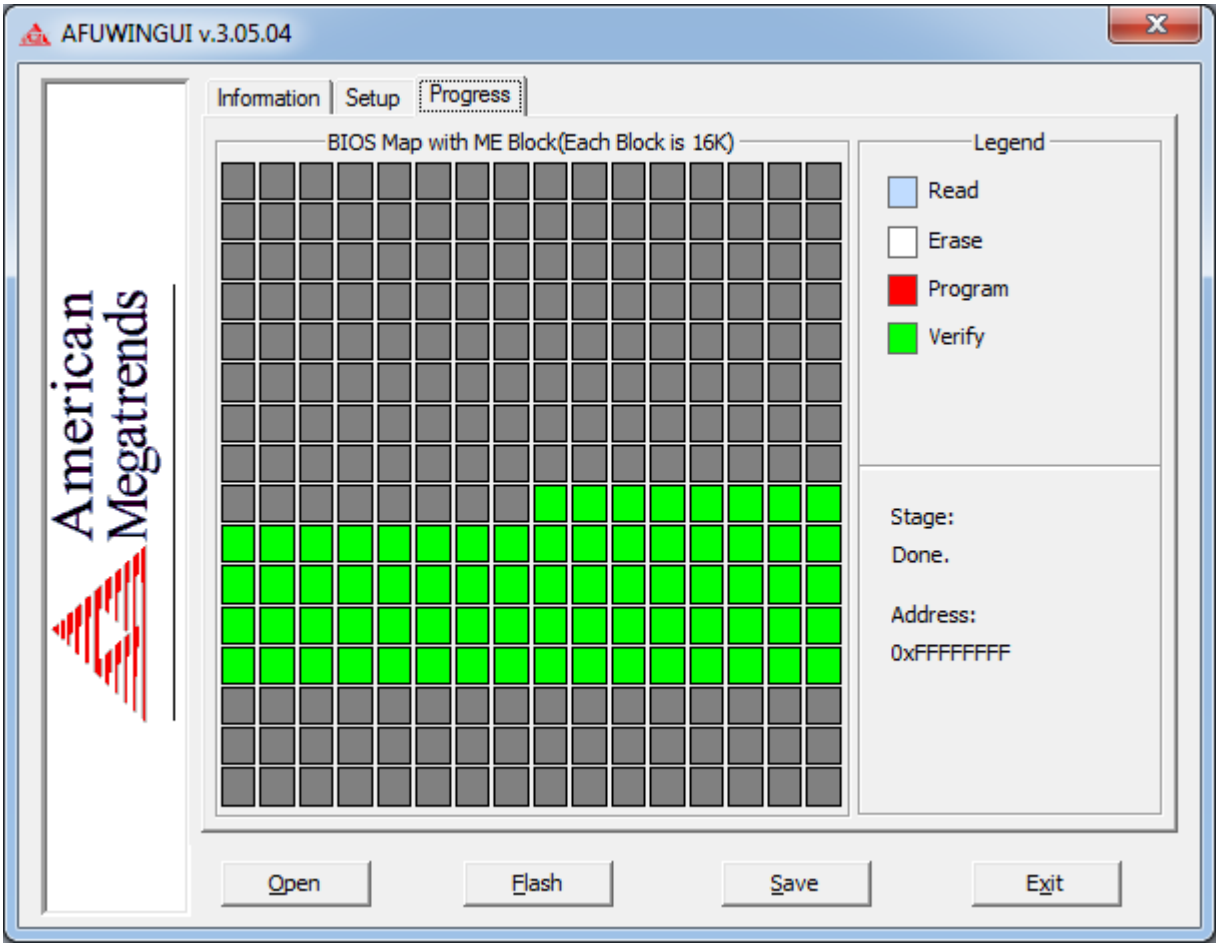




Then click on “Open” button and select the ROM with the name as your BIOS version. DO NOT SELECT THE WRONG FILE, YOU COULD BRICK! Then check “Do Not Check ROM ID” and “Restart After Programming” and press Flash. Click on “Ok” when AfuWin asks if you want to continue and wait until the flash is done.







Your PC will reboot and you should see a new logo! Press immediately F2 to enter BIOS options, go to “Exit” and select “Load Default Values” and then “Shutdown”. Power on your laptop and check if all is working good! If you have any trouble you can reflash the backup ROM you made before.

UPDATE x1:
Guys at Guru3D have found a workaround to fix ATI video playback problems on newest drivers! There are two files, made by Sony, that are not shipped with newest drivers anymore so drivers cannot recognize the VGA at all. Just put this two files in System32 and SysWOW64 (in case you have a 64bit OS) and reboot. That’s all! Works Windows 7, 8.x and 10 (for now)!
You can download the two files here.

WARNING, I’LL NOT ASSUME ANY RESPONSIBILITY ABOUT THIS ARTICLE AND FILES/SOFTWARE LINKED, PUBLICIZED AND MENTIONED HERE! BIOS MODDING IS REALLY DANGEROUS AND COULD BRICK OR DAMAGE YOUR MACHINE! BE SURE TO KNOW WHAT ARE YOU DOING AND POSSIBLY HAVE AN SPI DUMP OF YOUR FULL BIOS!!!