

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	data																		note
type: 25 SPI FLASH 💌	🥝 edit ı	node			fil	e su	տ շվ	ode:	003	303D	730H	7		c	hip	sum	code: 00303D730	F	たけ引脚図
firm: WINBOND	ADDR	0	1 2	з	4	5	6	7	8	9	Α	В	С	D	E	F	ASCII		
chip: W25022	00000000	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF			
cmp: <u>₩26032</u>	00000010	5A /	A5 F0	OF	02	00	04	02	06	02	10	10	20	00	00	00	Z		
capa: 32Mbits/4Mbytes	00000020	1B (00 30	09	00	00	00	00	00	00	00	00	FF	FF	FF	FF	0		
_ operation	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	OF	00	00		_	
Auto (F9)	00000050	FF	OF OC	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF			
	00000060	00	00 OE	0A	00	00	0D	0C	18	01	08	08	FF	FF	FF	FF			芯片位 置
0	00000070	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF			CHEE
Erase(F4)	00000080	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF			
0	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			•
Write(F6)	000000B0	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		_	
	00000000	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		_	
	00000000	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		_	24/- 1
C Verify(F8)	000000E0	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		_	a 25 s
	000000F0	FF	FF FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		_	
Read(F7)	00000100	82	56 20	08	OF	00	00	00	00	00	00	00	00	00	00	00	.V	_	
Nead (I'')	00000110	00	EO CE	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		
Blank (F3)	00000130	00	00 00	00	00	00	00	00	00	00	00	00	18	03	00	00		-	
	1:13:47 d	evice	conne	cted															
	1:13:50 o	pen su	icceed																
Test (F5)																			
Bulk Mode(F2)																			
	1																		
open succeed		f	ile:	C:\		AMIA	PTI	ON VA	ATO	MOD	va	io 1	ina	l vł	ios	oris	v. rom b:	rower	GZUn [№]
		1		10.1			1,				_ • a		- -	• L	200	_ ~ ~ + 6			

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).

		0 1 10 0 1	C1	A (1)	E 4 6	0.0.1	
🗁 Main	Handle	Control Group Structures	Show	Access/Use	Failsate	Optimal	
	(02F4)	PEG Port Configuration					
Advanced	(02F7)	PEGO	Yes	USER			
Advanced	(02FA)	PEG1	Yes	USER			
PCI Subsystem Settings	(02FC)	Always Enable PEG	Yes	USER	Disabled	Disabled	
ACPI Settings	(02FE)	Force X1	Yes	Default	Disabled	Disabled	
CPU Configuration	(02F2)	ASPM	Yes	Default	Enabled	Enabled	
Power & Performance	(0302)	Automatic ASPM	Yes	USER	Manual	Auto	
ME Configuration	(030F)	Extended Synch	Yes	Default	Disabled	Disabled	
	(0304)	ASPM LOs	Yes	Default	Both Root a	Both Root and Endpoint Ports	
+ Themal Configuration	(030D)	ASPM L1	Yes	Default	Enabled	Enabled	
Port 80h	(0309)	ASPM L0s Aggressiveness	Yes	Default	Ultra-aggres	Ultra-aggressive	
USB Configuration	(0341)	MCH Turbo	Yes	Default	Enabled	Enabled	
🗄 💼 Serial Port Console Redirection	(0345)	MCH Limit	Yes	Default	Enabled	Disabled	
Network Stack	(0347)	MCH Power Limit Value	Yes	Default	200	511	
North Bridge Configuration							
Clarksfield_Lynnfield MRC/Q							
🕀 🧰 Aubumdale_Havendale							
Aubumdale_Havendale MRC							
Arrandale Clarkdale							
Arrandale, Clarkdale MBC/Q							
Common North Bridge Control							
PEG Port Configuration							
⊡⊡ South Bridge Configuration							
💼 Security							
🛅 Boot							
Exit							

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.

Load Image Insert Replace Delete Extract CPU Patch RomHole Save Image Module file Browse Browse Browse Browse Save Image as Vol. Index 03:02-02 Insert FFS Options Insert FFS Options Insert As is Insert As is Insert As is Insert As Insert As Insert As Insert As Insert Insert As Insert As Insert As Insert As Insert Insert<		l Aptio-	R1170Y8.ROM			_ 						
Save Image Module file Browse Save Image as Vol. Index 03:02:02 Insert FFS Options Insert FFS Options Create Report Link Present Insert As is Insert Insert Close Vendor ID Device ID Insert As is Insert Volume Index FileName Source size GUID 00 00 0000FFB8 CEF5B3A3:476D:497F:9FDC:E981. 01 00 0000FFB8 CEF5B3A3:476D:497F:9FDC:E981. 02 00 0000FFB8 CEF5B9A3:476D:497F:9FDC:E981. 02 00 0000FFB8 CEF5B9A3:476D:497F:9FDC:E981. 02 01 S3Resume 000012418 17089572:377F:44E:78F4E:804FF 03:02:02 02 0000CE93 AE717C2F:1A42:4F2B:8861:78879 03:02:02 03:02:02 00 FileSystem 00001721 33:02:78C:1F09:47E:F8B2:5814F 03:02:02 03 CORE_DXE 0000B0CE1 CE552C4A:383A:41EB:A848E 03:02:02 04 Runtime 0000B0CE5 SAE3E37E:44E:41AE:3	Load Image Insert Replace Delete Extract CPU Patch RomHole											
Vol. Index 03:02:02 Save Image as Vol. Index 03:02:02 Create Report For Option ROM only Insert FFS Options Close Vendor ID Device ID Insert As is Volume Index FileName Source size GUID 00 00 0000FF88 CEF5B3A3:476D-497F-9FDCE981 01 00 0000FF88 CEF5B3A3:476D-497F-9FDCE981 02 01 S3Resume 0000153A EFD652CC-0E99-40F0-96C0-E080C 02 01 S3Resume 00001721 93002F82-1772-44EF-8744EF-8744EF-894F4.809FF 03:02:02 01 S3Resume 00001721 93002F82-1F09-47EF-88B2-5814F 03:02:02 02 00000CE93 AE717C2F-1A42-4F2B-8861-78B79 03:02:02 01 00001721 93002F82-1F09-47EF-8B82-5814F 03:02:02 02 00000CE93 AE717C2F-1A42-4F2B-864-4312-0DCC 03:02:02 02 00000CE5 5AE 5F37E-4EAE-414E-824/03545E 03:02:02 04 Runtime 00000000B1 CE59C4A-383A-41EB-86E-4438 <td colspan="8">Save Image Module file Browse</td>	Save Image Module file Browse											
Save Image as For Option ROM only Insert FFS Options Create Report Link Present Insert As is Close Vendor ID Device ID Insert As is Volume Index FileName Source size GUID 00 00 0000FFB8 CEF5B9A3.476D.497F.9FDC-E981. 01 00 0000FFB8 CEF5B9A3.476D.497F.9FDC-E981. 02 01 S3Resume 0000159A EFD652C2.0E99.40F0.96C0-E080C 02 01 S3Resume 00001721 93022F8C.1F09.47EF.8F4E.805F.78879 03:02:02 00 FileSystem 00001C94 13AC6DD0.73D0.11D4.8068.00A4 03:02:02 00 FileSystem 00000CE9 DAC28117.85FB.430A.41EB.48EE.4498 03:02:02 03 CORE SAE2537E.4EAE.41AE.824095455 03:02:02 04 Runtime 000001C94 13AC6DD0.73D0.11D4.806AACC.731C 03:02:02 04 Runtime 000000CE5 SAE357E.4EAE.41AE.824095455 03:02:02 05 PeiBus 000001C1 80E66E0A-CCD1.43FA.47B1.205E <td></td> <td>-3-</td> <td>Vol Index 02.02.02</td> <td></td> <td></td> <td></td>		-3-	Vol Index 02.02.02									
Create Report Insert FFS Options Close Link Present Insert As is Volume Index FileName Source size GUID 00 00 00000FFB8 CEF5B3A3-476D-497F-9FDC-E981- 01 00 00000FFB8 CEF5B3A3-476D-497F-9FDC-E981- 02 00 000015B8 CEF5B3A3-476D-497F-9FDC-E981- 02 00 00012418 17088572-377F-44EF-8F4E-809FFF 02 01 S3Resume 0000159A EFD652CC-0E99-40P0-96C-E08CC 02 02 00000CE93 AE717C2F-1A42-4F2B-8861-78879 0302-02 0302-02 00 FileSystem 00001721 93022F8C-1F09-47EF-BB82-5814F 0302-02 01 000000CC9 DAC28117-85F8-4964-A312-0DCC 0302-02 02 000000CC5 545377E-4EAE-41AE-8240-35456 0302-02 04 Runtime 000000000000000000000000000000000000	Save Imag	e as	Vol. Index [U3:U2-U2									
Close Link Present Insert As is Volume Index FileName Device ID Insert Compressed 00 00 0000FFB8 CEF5B9A3.476D-497F-9FDC-E981. 01 00 0000FFB8 CEF5B9A3.476D-497F-9FDC-E981. 02 00 000012418 17088572-377F-44EF-8F4E-809FF 02 00 000159A EFD652CC-0E99-40F0-96C0-E980. 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E980. 02 02 0000CE93 AE717C2F-1A42-4F28-8861-78879 03.02-02 01 S3Resume 00001721 93022F8C-1F09-47EF-8B82-5814F 03.02-02 01 00000CE93 AE717C2F-1A42-4F28-8861-78879 000000CB9 03.02-02 01 00000CB9 DACCED17-B5B-4964-A312-00CC 000000CB9 03.02-02 02 000000CB9 DACCED17-B8B-4964-A312-00CC 0302-02 03.02-02 04 Runtime 000000C5 5AE3F37E-44EA-41AE-8240-35455 03.02-02 05 PciBus 0000077D5 E03ABADF-E536-4488-83A0-877F	Create Re	eport	For Optio	n ROM only	- Insert FFS Options							
Close Vendor ID Device ID C Insert Compressed Insert Volume Index FileName Source size GUID GUID 00000FF88 CEF5B3A3-476D-497F-9FDC-E9814 01 00 000 0000FF88 CEF5B3A3-476D-497F-9FDC-E9814 02000FF88 CEF5B3A3-476D-497F-9FDC-E9814 02 00 0000153A EFD652CC-0E99-40FD-96C0-E080C 020000C193 AE717C2F-1A42-4F28-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 000000C89 DAC28117-85F8-4964-A312-0DCC 000000C89 DAC28117-85F8-4964-A312-0DCC 0000000C89 DAC28117-85F8-4964-A312-0DCC 03:02-02 02 0000000010C1 80E650A-4CD1-43FA-A781-205495 03:02-02 04 Runtime 000080011 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 000010C1 80E660A-CD1-43FA-A781-205495 03:02-02 07 CpuDxe 000010C1 80E660A-CD1-43FA-A781-205495 03:02-02 07 CpuDxe 000010C1 80E660A-CD1-43FA-A781-205495 03:02-02 08 MicrocodeUpdate 0000010C1<			Link	Present	Insert As is							
Volume Index FileName Source size GUID 00 00 0000FF88 CEF5B9A3-476D-497F-9FDC-E981- 01 00 0000FF88 CEF5B9A3-476D-497F-9FDC-E981- 02 00 0000FF88 CEF5B9A3-476D-497F-9FDC-E981- 02 00 00012418 17088572-377F-44EF-8F4E-809FFF 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 00 000012418 17088572-377F-44EF-8F4E-809FFF 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 Signesume 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 00001C34 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 000000C89 DAC28117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 0000000000000000000 Signes-4438 03:02-02 04 Runtime 000000000000001 SIGE59C4A-383A-41E8-48498 03:02-02 06 PciRootBridge 000010C1 80E66E0A	Close		Vendor ID	Device ID	C Insert Compressed	Insert						
Volume Index FileName Source size GUID 00 00 0000FFB8 CEF5B9A3.476D-497F-9FDC-E981. 01 00 0000FFB8 CEF5B9A3.476D-497F-9FDC-E981. 02 00 00012418 17088572-377F-44EF-8F4E-809FFf 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E0800 02 02 02 000DCE93 AE717C2F-1A42-4F2B-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-B8B2-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-806B-00A4 03:02-02 02 00000CB9 DAC2B117-85FB-4964-A312-0DCC 03:02-02 02 00000CB9 DAC2B117-85FB-4964-A312-0DCC 03:02-02 04 Runtime 00000CB9 DAC2B117-85FB-4964-A312-0DCC 03:02-02 04 Runtime 000000CB9 DAC2B117-85FB-4964-A312-0DCC 03:02-02 05 PciBus 00000A119 3C1DE39F-0207-408A-AACC-731C 03:02-02 05 PciBus 000010C1 80E66E0A-CCD1												
Volume Index FileName Source size GUID 00 00 0000FFB8 CEF5B3A3-476D-497F-9FDC-E981- 01 00 0000FFB8 CEF5B3A3-476D-497F-9FDC-E981- 02 00 000012418 17089572-377F-44EF-8F4E-809FFf 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 02 0000DCE93 AE717C2F-1A42-4F28-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-B8B2-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 00000CB9 DAC28117-85F8-4964-A312-0DCC 03:02-02 03 CORE_DXE 00000CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 000000CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 00000000000000011 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 05 PciBus 0000171 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 06 PciRootBridge												
00 00 0000FFB8 CEF5B9A3-476D-497F-9FDC-E981- 01 00 0000FFB8 CEF5B9A3-476D-497F-9FDC-E981- 02 00 00012418 17088572-377F-44EF-8F4E-809FFf 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 00 0000DCE93 AE717C2F-1A42-4F28-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 00000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 02 00000CCS 5AE3F37E-4EAE-41AE-8240-35485 03:02-02 02 00000CCS 5AE3F37E-4EAE-41AE-8240-35485 03:02-02 02 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 02 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 03 CDRE_DXE 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 000000CDS 5AE3F37E-4EAE-41AE-8240-35485 03:02-02 03:02-02 04 Runtime 00000000CDS 5AE3F3	Volume	Index	FileName	Source size	GUID	·						
01 00 0000FFB8 CEF5B9A3-476D-497F-9FDC-E981- 02 00 00012418 17088572-377F-44EF-8F4E-809FFf 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 02 000DCE93 AE717C2F-1A42-4F2B-8861-78B79 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 00000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 02 00000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 03 CORE_DXE 00000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 00000B0E1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 000001C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 06 PciRootBridge 00001C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 0000077D5 E03ABADF-E536-4E88-B3A0-B7FF 03:02-02 08 Microcode	00	00		0000FFB8	CEF5B9A3-476D-497F	-9FDC-E98143						
02 00 00012418 17088572-377F-44EF-8F4E-809FFf 02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 000DCE93 AE717C2F-1A42-4F28-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 00000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 02 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 03 CORE_DXE 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 000000CB9 DAC2B117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 000000000000000000000000000000000000	01	00		0000FFB8	CEF5B9A3-476D-497F	-9FDC-E98143						
02 01 S3Resume 0000159A EFD652CC-0E99-40F0-96C0-E08C0 02 02 000DCE93 AE717C2F-1A42-4F28-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-8B82-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 00000C89 DAC2B117-85F8-4964-A312-0DCC 03:02-02 02 000000C89 DAC2B117-85F8-4964-A312-0DCC 03:02-02 03 CORE_DXE 000000C89 DAC2B117-85F8-4964-A312-0DCC 03:02-02 04 Runtime 000000000 SAE3F37E-4EAE-41AE-8240-35468 03:02-02 04 Runtime 000000000 SAE3F37E-4EAE-41AE-8240-35468 03:02-02 04 Runtime 00000000 SAE3F37E-4EAE-41AE-8240-35468 03:02-02 05 PciBus 00000000 SAE3F37E-4EAE-41AE-8240-35468 03:02-02 05 PciBus 00000000 SAE3F37E-4EAE-41AE-8240-35468 03:02-02 06 PciRootBridge 00001001 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02	02	00		00012418	17088572-377F-44EF-	8F4E-B09FFF4						
02 02 000DCE93 AE717C2F-1A42-4F2B-8861-78879 03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-BBB2-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-8068-00A4 03:02-02 02 00000CB9 DAC2B117-B5FB-4964-A312-0DCC 03:02-02 03 CORE_DXE 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 00000B0E1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 00000A119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 00001C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 0000077D5 E03ABADF-E536-4E88-B3A0-B7FF 03:02-02 08 MicrocodeUpdate 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 09 NBDXE 000011BD 85DE8B02-38A2-44DD-B149-7D96 03:02-02 0A MchDxePlatformPolicy 0000011BD 85DE8B02-38A2-44DD-B149-7D9	02	01	S3Resume	0000159A	EFD652CC-0E99-40F0)-96C0-E08C08						
03:02-02 00 FileSystem 00001721 93022F8C-1F09-47EF-BBB2-5814F 03:02-02 01 00001C94 13AC6DD0-73D0-11D4-B06B-00A4 03:02-02 02 00000CB9 DAC2B117-B5FB-4964-A312-0DCC 03:02-02 03 CORE_DXE 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 05 PciBus 00000A119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 0000077D5 E03ABADF-E536-4E88-B3A0-B7FF 03:02-02 08 MicrocodeUpdate 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 09 NBDXE 000011BD 85DEB802-38A2-44DD-B149-7D96 03:02-02 0A MchDxePlatformPolicy 000011BD 85DE8B02-38A2-44DD-B149-7D96 03:02-02 0B lioWrapper 000001459	02	02		000DCE93	AE717C2F-1A42-4F2B	-8861-78B79C						
03:02-02 01 00001C94 13AC6DD0-73D0-11D4-B06B-00A4 03:02-02 02 00000CB9 DAC2B117-B5FB-4964-A312-0DCC 03:02-02 03 CORE_DXE 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 0000B0C1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 00000L11 S0E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 06 PciRootBridge 000010C1 S0E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 0000077D5 E03ABADF-E536-4E88-B3A0-B7FF 03:02-02 08 MicrocodeUpdate 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 09 NBDXE 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 0000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 000001869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0C VtdWrapper 000000B69	03:02-02	00	FileSystem	00001721	93022F8C-1F09-47EF	BBB2-5814FFE						
03:02-02 02 00000CB9 DAC2B117-B5FB-4964-A312-0DCC 03:02-02 03 CDRE_DXE 0000B0CC5 5AE3F37E-4EAE-41AE-8240-35465 03:02-02 04 Runtime 0000B0E1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 00000L119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-877F 03:02-02 08 MicrocodeUpdate 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 09 NBDXE 000011BD 85DEBB02-3BA2-44DD-B149-7D96 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEBB02-3BA2-44DD-B149-7D96 03:02-02 0B IioWrapper 0000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 000000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00000109 E0EC8EC9-8193-4351-A488-36A65	03:02-02	01		00001C94	13AC6DD0-73D0-11D	4-B06B-00AA0						
03:02-02 03 CDRE_DXE 000B0CC5 5AE3F37E-4EAE-41AE-8240-35456 03:02-02 04 Runtime 0000B0E1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 0000L119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-877F 03:02-02 08 MicrocodeUpdate 00001FD5 E4ECD082-E277-4F28-BEC8-E4D7 03:02-02 09 NBDXE 000011BD 85DEB802-38A2-44DD-B149-7D96 03:02-02 08 lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001099 E0EC8EC9-8193-4351-A488-36A68	03:02-02	02		00000CB9	DAC2B117-B5FB-4964	4-A312-0DCC7						
03:02-02 04 Runtime 000080E1 CBC59C4A-383A-41EB-A8EE-4498 03:02-02 05 PciBus 0000A119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-B77F 03:02-02 08 MicrocodeUpdate 000045E1 F3331DE6-4A55-44E4-B767-7453F 03:02-02 09 NBDXE 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 0A MchDxePlatformPolicy 000011BD 85DE8B02-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 0000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001109 E0ECBEC9-B193-4351-A488-36A65	03:02-02	03	CORE_DXE	00080005	5AE3F37E-4EAE-41AE	E-8240-35465B						
03:02-02 05 PciBus 0000A119 3C1DE39F-D207-408A-AACC-731C 03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-B77F 03:02-02 08 MicrocodeUpdate 000045E1 F3331DE6-4A55-44E4-B767-7453F 03:02-02 09 NBDXE 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001109 E0ECBEC9-B193-4351-A488-36A65	03:02-02	04	Runtime	0000B0E1	CBC59C4A-383A-41EE	8-A8EE-4498AI						
03:02-02 06 PciRootBridge 000010C1 80E66E0A-CCD1-43FA-A7B1-2D5E 03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-B77F 03:02-02 08 MicrocodeUpdate 000045E1 F3331DE6-4A55-44E4-B767-7453F 03:02-02 09 NBDXE 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001109 E0ECBEC9-B193-4351-A488-36A65	03:02-02	05	PciBus	0000A119	3C1DE39F-D207-4084	A-AACC-731CFI						
03:02-02 07 CpuDxe 000077D5 E03ABADF-E536-4E88-B3A0-B77F 03:02-02 08 MicrocodeUpdate 000045E1 F3331DE6-4A55-44E4-B767-7453F 03:02-02 09 NBDXE 00001FD5 E4ECD082-E277-4F28-BECB-E4D7 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001109 E0ECBEC9-B193-4351-A488-36A65	03:02-02	06	PciRootBridge	000010C1	80E66E0A-CCD1-43F/	A-A7B1-2D5EE						
03:02-02 08 MicrocodeUpdate 000045E1 F3331DE6-4A55-44E4-B767-7453F 03:02-02 09 NBDXE 00001FD5 E4ECD0B2-E277-4F28-BECB-E4D3 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEBB02-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001109 E0ECBEC9-B193-4351-A488-36A65	03:02-02	07	CpuDxe	000077D5	E03ABADF-E536-4E8	8-B3A0-B77F7{						
03:02-02 09 NBDXE 00001FD5 E4ECD082-E277-4F28-BEC8-E4D3 03:02-02 0A MchDxePlatformPolicy 000011BD 85DEB802-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A438BD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001099 E0EC8EC9-8193-4351-A488-36A65	03:02-02	08	MicrocodeUpdate	000045E1	F3331DE6-4A55-44E4	-B767-7453F7/						
03:02-02 0A MchDxePlatformPolicy 000011BD 85DEBB02-3BA2-44DD-B149-7D96 03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigStrc 00001099 E0ECBEC9-B193-4351-A488-36A65	03:02-02	09	NBDXE	00001FD5	E4ECD0B2-E277-4F2E	B-BECB-E4D75						
03:02-02 0B lioWrapper 000014F9 75A3EC38-A333-42B0-9A15-EDED 03:02-02 0C VtdWrapper 00000869 D1A438BD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigStrc 00001099 E0ECREC9-8193-4351-A488-36A65	03:02-02	0A	MchDxePlatformPolicy	000011BD	85DEBB02-3BA2-44D	D-B149-7D966						
03:02-02 0C VtdWrapper 00000869 D1A43BBD-A946-4AF0-9931-90AF/ 03:02-02 0D SaveMemoryConfigSrc 00001099 E0FCREC9-B193-4351-A488-36665	03:02-02	OB	lioWrapper	000014F9	75A3EC38-A333-42B0	-9A15-EDED8						
03:02-02_0DSaveMemoryConfigStc00001099E0ECBEC9-B193-4351-A488-36A65	03:02-02	0C	VtdWrapper	00000B69	D1A43BBD-A946-4AF	0-9931-90AFA						
	03:02-02	ND	SaveMemoryConfigSrc	00001099	E0ECBEC9-B193-4351	1-A488-36A655						
						•						

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!!!



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-k Ω ±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.

🔚 FirmwareUltimo_VAIO.xml - Flash Image Tool								
<u>File Build H</u> elp								
🗋 😅 🛃 🚨 Intel® 5 Series Chipset 💌	Intel® HM55 - Mobile 🔹							
🖃 🗁 Flash Image	Parameter	Value	Help Text	*				
🖃 🚖 Configuration	ODM ID used by Intel® Upgrade Service	0x0000000	ID generated by or registered with Intel® Upgrade Service web servers i					
- 🗀 ME	System Integrator ID used by Intel® Upg	0x0000000	ID generated by or registered with Intel® Upgrade Service web servers i					
Power Packages	Reserved ID used by Intel® Upgrade Serv	0x0000000	Reserved ID may be used for a Reseller ID or other Intel® Upgrade Servic					
Features Supported								
Manageability Application	MEBx Password Policy	0	0 = Over network password change allowed only if it is default. 1 = Ove	E				
Intel® Anti-Theft (AT-p) Techno	Provisioning Time Period	0	Set Remote Configuration Provisioning Time Period. Valid values are 0					
Setup and Configuration	Remote Configuration Enabled	false	false = Disable, true = Enable,					
	PKI DNS Suffix		Set PKI DNS Suffix in dotted string format.					
	Remote PC Assist Technology Enabler ID	0000000-0000-0000-0000-000000000000	Unique numeric ID of the party which enabled the service in manufactu					
	Remote PC Assist Technology Enabler N	0.01	Description of the party which enabled the service in manufacturing. M					
	Remote PC Assist Technology Hw Button	0x01	0x01 = Chassis Intrusion. 0x02 = RCS Trigger.					
	Hash 0 Active	false	false = Not Active true = Active					
	Hash 0 Friendly Name		Enter Hash Name. Maximum of 32 characters.					
	Hash 0 Stream		Enter raw hash string or certificate file.					
	Hash 1 Active	false	false = Not Active true = Active					
	Hash 1 Friendly Name		Enter Hash Name. Maximum of 32 characters.					
	Hash 1 Stream		Enter raw hash string or certificate file.					
	Hach 2 Active	falce	false - Not Active true - Active					
	Hash 2 Friendly Name	Taise	Enter Hash Name Maximum of 32 characters					
	Hash 2 Stream		Enter raw hash string or certificate file.					
	Hash 3 Active	false	false = Not Active true = Active					
	Hash 3 Friendly Name		Enter Hash Name. Maximum of 32 characters.					
	Hash 3 Stream		Enter raw hash string or certificate file.					
Flash Image Configuration	Hash 4 Active	false	false = Not Active true = Active					
Coniguration	Hash 4 Friendly Name		Enter Hash Name. Maximum of 32 characters.					
	Hash 4 Stream		Enter raw hash string or certificate file.	*				
Flash Image\Configuration\Setup and Configuration	ation		NUM					

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.

🖪 He	🗓 Hex Workshop - C:\Users\Jacksoft\Desktop\AMIAPTIO\VAIO_MOD_vaio_final_vbios_orig.rom																		
<u>F</u> ile	Edit Disk Option	ns <u>T</u> o	ools	Plug-I	ns <u>W</u>	<u>(</u> indow	<u>H</u> el	р											
2	I 🗟 🔂 🔂	* 4	A 🖪	8	s 4	26	A	1 🐴	8 🏭	۵۵ 🖉	۵ 📃			- 📳	۲ ۵	"℃	16	🗠 📖	
11 11 🏊		d . da	En3	h-II	234 Б	a 186	122	ACCIL		-	ЪB	Laa a	. IN	NN		<u></u>			
8		V 3	5 UT		₩ 8	■ [3]	Legacy	ASCII											
	C\Users\Jacks	oft\De	sktop\			AIO N		vaio fi	inal vb	ios or	ia.rom	,							\mathbf{x}
Data		0	1	2	3	4	5	6	7	8	<u>a</u>	7)	P	C	D	F	F	0123456789ABCDEE	
≤	0.0.0.0.0.0.0.0.0.0	0	-	4		-		00		0		-	5	0.0	0.0	E 0.0		0123430705ABCDEF	
sual	00000FB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		Â
izer	00000FC0	0.0	00	00	00	00	00	00	00	00	00	00	00	0.0	00	00	00		
	00000FE0	0.0	00	0.0	00	0.0	0.0	0.0	0.0	00	0.0	00	00	0.0	0.0	0.0	0.0		
	00000FF0	00	00	00	00	0.0	00	00	00	00	00	00	00	0.0	00	00	00		
	00001000	20	20	80	0 F	40	00	00	10	00	0.0	00	0.0	0.0	0.0	00	0.0	(d	
	00001010	24	46	50	54	07	00	00	00	20	10	30	ΕO	07	00	64	00	\$FPT0d.	
	00001020	20	00	00	00	07	FC	FF	FF	00	00	00	00	00	00	00	00		
	00001030	46	4 F	56	44	4B	52	49	44	00	04	00	00	00	1C	00	00	FOVDKRID	
	00001040	01	00	00	00	01	00	00	00	00	00	00	00	83	07	00	00		
	00001050	45	46	46	53	4 F	53	49	44	00	20	00	00	00	00	03	00	EFFSOSID	
	00001060	40	0B	00	00	60	27	00	00	00	00	00	00	84	27	00	00	@ ` ' '	
	00001070	4E	56	4B	52	4B	52	49	44	00	00	00	00	00	00	01	00	NVKRKRID	
	00001080	40	0B	00	00	60	27	00	00	00	00	00	00	82	28	00	00	@`'(
	00001090	4E	56	54	44	54	44	49	44	00	00	00	00	00	20	00	00	NVTDTDID	
	000010A0	40	0B	00	00	60	27	00	00	00	00	00	00	82	28	00	00	@`'(
	00001080	4 E	56	56	45	F.F.	E.E.	E.E.	E.E.	00	00	00	00	00	00	00	00	NVVE	
	00001000	101	00	00	00	U L	00			00	20	00	00	82	21	00	00	/	
	00001000	40	00	00	00	01	00	00	00	00	20	0.0	00	80	27	00	00	FIPK	
	000010E0	4 F	46	54	50	<u>ਜ</u>	ਹ ਹ ਸ ਸ	ਹ ਹ ਸ ਸ	ਹ ਹ ਸ ਸ	00	20	00 0D	00	00 ਸਾਸ	, 2 च च	ਹ ਹ ਸ ਸ	ਹ ਹ ਸ ਸ	NETD	
	00001100	01	0.0	00	00	01	0.0	0.0	0.0	0.0	00	0.0	0.0	80	2.7	0.0	0.0		
	00001110	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		
	00001120	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		
	00001130	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		
	00001140	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		
	00001150	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF		
	00001160	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		
	00001170	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$		
	00001180	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF		Ŧ

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).

	v.3.05.04		×
	Information Setup	Progress	,
		System Information	
	OS:	Windows 7 64-bit	
	Bios Size:	2097152 bytes	
	MainBios Size:	1179648 bytes	
gal	BootBlock Size:	786432 bytes	
G C	NVRAM Size:	65536 bytes	
at e	Core Version:	04.06	
l č ž	Project Version:	00.16	
l ₹₹	Firmware ID:		
	Firmware GUID:		
	Bios Chip Name:		
191 J		ROM File Information	
1	Input Rom File:	Unknown	
	File Rom ID:	Unknown	
	File Rom GUID:	Unknown	
	<u>O</u> pen	Elash <u>S</u> ave E <u>x</u> it	



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.

AFUWINGUI	v.3.05.04	— ×-
American Megatrends	Information Setup Progress Block Options Program All Blocks Main BIOS Image Boot Block NVRAM EC Block ME Firmware Block Ignition Entire	Miscellaneous ✓ Do Not Check ROM ID ○ Check EC Version ✓ Restart After Programming Preserve Setup Preserve SMBIOS ○ Recovery ○ Capsule Non Critical Block 1 2 9 10 11 12 12 3 4 5 6 7 8 9 10 11 12 13 14 15 15 16 ROM HOLE ALL 1 2 3 4 5 6 7 8 9 10 11 12 12 13 14 15
	<u>O</u> pen <u>F</u> lash	<u>S</u> ave E <u>x</u> it





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!!!