Monday, June 10, 2013

466 comments:

drakonn June 11, 2013 at 3:54 AM

Very good tutorial donovan but I can not get me to work ... my knowledge about this are null and not come out the same as you and. I can not find the tabs in the IDA ... It may be because I have a different version of InsydeH20 (3.7).
I've been hours trying it and nothing.
If one day you have time and are interested, you do me a favor modifying my bios to have these advanced options :)
Good day.

Sorry for my english, google traductor!

Reply

Replies

donovan6000 June 11, 2013 at 1:27 PM

I can take a took at your bios. What's your computer's model?

drakonn June 11, 2013 at 2:39 PM

My notebook is a Lenovo g580 2189 with windows 8 64bits.
Link to my bios: http://download.lenovo.com/consumer/mobiles/5ecn96ww.exe
I would be very grateful and of course would contribute with a donation for you to take a few beers this summer!

donovan6000 June 11, 2013 at 3:16 PM

How many tabs are currently viewable in your setup utility? Just skimming though your bios reveals that there are potentially 9 tabs. I have run across a few bios that have duplicates of certain tabs for some reason. It also looks like it would be easy to replace the existing tabs with the hidden one, as I did with my Power tab in the tutorial. And do you know how to recover you laptop incase I mess up?

drakonn June 11, 2013 at 3:27 PM

I can see 5 tabs in my bios.
And no, i dont know how to recover my laptop in case of error.
Thank you :)

donovan6000 June 11, 2013 at 5:50 PM

Just created a tutorial about bios recovery. If you can get it working, then I'll send you a modified version of your bios to try. I don't want to accidentally brick your computer while trying to help you.

drakonn June 12, 2013 at 12:52 AM

This comment has been removed by the author.

drakonn June 12, 2013 at 3:45 AM

Wait.
I put the bios on usb or cd with many different names and different extensions in case but when I turn on the computer by pressing windows + b seeks nothing, just the screen stays black until those loose buttons below to continue booting normally .
I tried win + b, fn + b, fn + esc fn + r, ... and nothing.
Not searching for anything, either usb or cd ... But continue to try
I don't have a lot time because I am on exams. I'll tell you.

drakonn June 12, 2013 at 4:43 AM

Yesssss. Recovery bios worked!
Unplug ac and batery.
Insert usb or cd(cd before unplug ac).
Hold power button 10 seconds.
Plug ac adapter.
Press fn + b and press power button.
Fan spin on and automatically search bios in cd or usb and install.
After some minuts (5 because dont restart automatically) press power button 5 seconds to close pc.
Then press power button and laptop restarts nornmally

In my case no beep in any moment.
:)

drakonn June 12, 2013 at 1:50 PM

Good. I can enter the bios recovery ... but it seems that seeks nothing. If I have a CD set, it seems that it runs about 20 seconds and then stops reading, however if I have a usb or sd not even read them ... not search for files or anything. In all these media I have 28 copies of the bios with different names.

donovan6000 June 12, 2013 at 4:20 PM

Ok, that too bad. I haven't found many things online about Lenovo insyde recovery, so it might be different. We'll just be extra careful when modding your bios as to avoid bricking it. I would feel really bad if you bricked your computer because of me.

Try this one and let me know if there is anything different about your setup utility's tabs. All I did was replace one of the referenced tabs with a different one: www.mediafire.com/?vls5a9adth40njs

donovan6000 June 12, 2013 at 4:21 PM

Oh and let me know if insideflash.exe gives you an error. I didn't check you iscflash.dll for any anti-mod protection.

drakonn June 13, 2013 at 3:56 AM

When laptop restarts to install bios, say that firmware image invalid!
Thanks :)

donovan6000 June 13, 2013 at 1:41 PM

Would you mind uploading a picture of the error here www.tinypic.com/

So I can see it.

drakonn June 13, 2013 at 2:18 PM

http://tinypic.com/r/fvkx95/5

This is the error.

donovan6000 June 13, 2013 at 3:26 PM

People have confirmed that they we're able to bypass this error by flashing their modified bios with the recovery procedure. So we just have to get that working.

Here's a new modified bios rom that should have two new tabs unlocked: www.mediafire.com/download/zteb3hyo3uw8930/new.zip

The two file's in there are what I think the recovery rom will be named. So just put them on the root of a FAT32 usb and try to recover. I've also read that if the recovery finds the correct file it'll beep once.

Would you also mind making me a backup of your bios rom with flashit.exe. You can get it here:www.mediafire.com/?nz968aqc6tjoaq2

It can only be run in dos, so I also included Rufus, which can easily install dos onto a flashdrive and make it bootable. So after doing that, copy the flashit.exe file onto that dos flash drive and restart your computer to boot to it. Now run flashit.exe -G which will make a backup.

drakonn June 14, 2013 at 1:56 PM

If I try to make a backup with flashit... error :
http://tinypic.com/r/muwhuf/5
Now, try to flash the modified bios.
Thanks.

drakonn June 14, 2013 at 2:53 PM

Bios recovery works...read the usb but dont found bios files. In my usb i have 28 files with diferents names, including QIWG5.BIN and G5901.bin

drakonn June 14, 2013 at 3:04 PM

Here is a backup of my bios with universal bios backup toolkit.
https://www.dropbox.com/s/1sz2unmrqms2743/LENOVO-5ECN96WW%28V9.01%29.fd

donovan6000 June 14, 2013 at 4:07 PM

I'm kind of out of ideas. If we can't get it to flash the rom with the recovery procedure then we're out of options. It's too bad Lenovo never release any information about it.

Reply

OJ Williams June 13, 2013 at 8:55 AM

im having a bit of problems with mine... what version of andy's tool are u using? i dont have the decompress option and when i try to do it any way the cmd prompt step gives me an errror

Reply

Replies

drakonn June 13, 2013 at 10:29 AM

Here are the last version with decompress option! :
http://www.sendspace.com/file/xxd63k

OJ Williams June 13, 2013 at 10:59 AM

thx but im stil having abit of problems... is ther any way u can mod my hp dv4 2145dx bios plz? i need advanced options only...i gtg for 4 hours now but heres the link incase u agree.. thx alot even if u do or not http://ftp.hp.com/pub/softpaq/sp49501-50000/sp49543.exe

donovan6000 June 13, 2013 at 1:43 PM

Unless your willing to donate after I'm done, then I'm not going to do it for you. One of the goals of this blog is to more people involved in modding their own bios.

OJ Williams June 13, 2013 at 2:05 PM

ahh i understand.. i would donate but no credit card yet... any way yeah ill do it but in that tutorial some of the steps were kinda hard to follow and im using the ida pro demo and its telling me use 64 bit version to extract amd64? ive tried it on 64 bit and 32 bit oses and same thing... whats that about?

donovan6000 June 13, 2013 at 2:16 PM

Most the bios I've used have been 64bit, so you do need the 64bit version of IDA Pro to disassemble them. The demo doesn't have support for that though.

Here you go: www.mediafire.com/?fp9o9px7n54nwj3

Just run Insydeflash.exe or Insydeflsh64.exe to install it. Let me know if you get an error when you try to install it. I didn't check your iscflash.dll for mod protection.

OJ Williams June 13, 2013 at 3:04 PM

what exactly did u do to that file? are the stuff decompressed in it?
i havent installed it asyet

donovan6000 June 13, 2013 at 3:29 PM

I modified the setup utility to unlock the power and advanced tabs. Hopefully it'll work. If by the off chance that it bricks your computer, them follow the brick recovery procedure I posted.

donovan6000 June 13, 2013 at 3:31 PM

My bad, I only modified your to replace the diagnostics tab with the advanced tab. I got confused thinking of a different one I was working on.

OJ Williams June 13, 2013 at 3:40 PM

wow thx! ur the best! the power tab wasnt unlocked tho and my pc is booting up and operating like 10x slower but i still appreciate it! btw do u know how to increase dedicated memory for an ati radeon hd 4200 video card? i have over 2gbs video card and only 320mb dedicated for graphics n gaming which sux...and is there any way i can message u facebook,msn, something? i would like to learn more about this so i can help others also.. im a computer tech>>>programmer and graphic design/hacker but im only 18 so i have alot to learn and always wanting to learn more

donovan6000 June 13, 2013 at 9:10 PM

You can send me your email through my Contact page. I'll get a hold of you after that.

OJ Williams June 13, 2013 at 10:14 PM

done (y)

Reply

avinash bommina June 20, 2013 at 12:52 AM

how to have access to the BIOS rom

Reply

Replies

donovan6000 June 20, 2013 at 11:44 AM

Sometimes it's as easy as renaming the installer's extension from .exe to .zip. But sometimes this doesn't work, so you'll have to run the installer and find out where it extracts the rom to before installing.

Reply

avinash bommina June 20, 2013 at 1:13 AM

please send me the whole video of advanced tab

Reply

Replies

donovan6000 June 20, 2013 at 11:47 AM

I don't have any way of recording the advance tab right now. Sorry. If your curious about which options are there, you can browse through your setup utility module with a hex editor to see the strings of the settings. Be aware though that some of these settings are still hidden.

Reply

MARKO LUCIC June 20, 2013 at 3:17 PM

can you help me i tried to follow this tutorial and i get messed up with all the things that needs to be done is there by any chance that you could do this for me my laptop is a hp dv7 2105ez bios download link http://ftp.hp.com/pub/softpaq/sp50501-51000/sp50677.exe

Reply

Replies

donovan6000 June 20, 2013 at 10:11 PM

Sorry, but unless your willing to donate I wont do it for you. I want more people to be able to do it themselves. I'd recommend trying to change one of the current tabs with one of the hidden as this is easier than unlocking one. I know how hard it is to get started. When I began modding insyde bios, I spent my first 3 weeks starring at assembly code and bricking my computer lol. Perseverance pays off though. Good luck :)

MARKO LUCIC June 21, 2013 at 2:44 AM

if i could i would donate but i am i living in a shit country where is hard to get a job or a card for internet payment so i cant.thanx for a quick answer
P.s sorry for my bad english

Reply

Reply

Anonymous June 22, 2013 at 9:49 AM

I got to the part where it has If that python script didn't work for your BIOS, here's a second option that might work.

I don't know what the next step is cause i don't need that part. You don't make it clear what the next part is if you don't need that option.

Reply

Replies

donovan6000 June 22, 2013 at 11:06 AM

Sorry for the inconvenience. I've added a few asterisks to the beginning of the paragraph that assumes that you now know the location of the tabs. I hope that clears things up :)

Reply

Anonymous June 23, 2013 at 8:18 AM

Hi,
I can't see any conditional jumps as show here https://lh3.ggpht.com/-9CBBmPdF3i4/UbeUxK725YI/AAAAAAAAAXI/4j8LUdvw5s4/s1600/11.png.
I have no options with jz before them. Does that mean my bios doesn't have advanced options?

thanks.

Reply

Replies

donovan6000 June 23, 2013 at 12:29 PM

I try to keep these tutorials as generic as possible, but no two bios versions are implemented the same way. I've only seen a handful of them that have the hidden tab's initialization set up like mine. It doesn't mean that you don't have an advanced option, it just means that it is initialized a different way. Try changing one of the referenced tabs to on of the hidden ones like I did at the end with switching in the power tab.

Reply

Anonymous July 11, 2013 at 7:57 AM

If You can do it with ?

I tried to do it with j-bios but the items on the menu and did not appear
and try on your article did not have the opportunity because I do not have a computer windows

http://ftp.hp.com/pub/softpaq/sp47501-48000/sp47531.exe

http://rghost.ru/47354628
<< 3635F13.FD file from exe

Reply

Replies

donovan6000 July 11, 2013 at 12:24 PM

I only used j-bios in this tutorial to reveal the offsets of the tabs. I also posted an alternative way of locating them by searching for this byte sequence in the setup module, DF 42 4D B5 52 39 51. Also IDA Pro has a Windows, Mac, and Linux versions available, so there's no reason that not having Windows should be holding you back.

I'm not going to do the work for you unless your willing to donate. One of the goals of this blog is to get people more involved with doing this themselves. Good luck :)

Тёма :DDDD July 14, 2013 at 12:12 AM

I will try to do on your instruction
Yesterday I bought and put the windows, put all the software
but I have no any conditional jumps

http://rghost.ru/47410118/image.png
This means that the hidden items in my BIOS does not exist?

dump http://rghost.ru/47354628
I buy you a beer too :3

donovan6000 July 14, 2013 at 2:07 AM

Hey Tema :)

You still have hidden tabs in your bios, but they're not enabled by doing the same thing as I did in my tutorial. No two bios releases are implemented the same way. The easiest way for you to get to them is by replacing the existing tabs with the hidden ones. Here's a picture that describes the process if you want to do it yourself.

http://i42.tinypic.com/2cmsldk.png

Or I can do it for you.

Тёма :DDDD July 14, 2013 at 4:17 AM

it would be great
Now I'll try, but probably not something that has replaced and expanded menu does not appear

Тёма :DDDD July 14, 2013 at 9:33 AM

I translate !
18004C930 there is 48 8D 05 40 B8 04 00
18004E380 there is 40 8D 05 84 D2 04 00
18004DFC0 there is 4C 8D 05 B1 CE 04 00

donovan6000 July 14, 2013 at 12:13 PM

Thanks for calculating the offset's relative positions. Saves me a couple minutes :)

Try this. I replaced your system configuration, diagnostics, and security tabs with the debug, power, and advanced tabs.

http://www.mediafire.com/?12evf5h150whdb1

Тёма :DDDD July 14, 2013 at 11:26 PM

Thank you, it works, but I can not save settings.
you have no ready-made solutions?
I will try to open the settings on one taboo, then i can save it.

donovan6000 July 14, 2013 at 11:59 PM

I've heard about cases of that happening. I don't think anyone really knows why. What happens when you try to save your settings? Can you save the settings without changing any of them?

Тёма :DDDD July 15, 2013 at 12:33 AM

He just hangs and nothing can be done, even if the settings should not just keep changing them.
I have noticed that if I open only one tab is hidden (in hex editor) everything is kept setings .

donovan6000 July 15, 2013 at 1:09 PM

I'm having some trouble understanding what your saying. I wish I spoke french so we could communicate better.

So saving the settings works when you only enable one of the hidden tabs?

Reply

Felipe Furtado July 11, 2013 at 9:55 AM

Hi donovan, i'm having a really hard work trying to unlock the advanced tab in my bios, i lost almost 2 days trying to pull out this menu but i'm completly lost. (never used hex codes, IDA pro or phyton before)

Could you take a look at my files please?
I buy you a beer 8-)

Bios dump & RW: http://www1.datafilehost.com/d/0967c905

Acer's bios: http://global-download.acer.com/GDFiles/BIOS/BIOS/BIOS_Acer_2.15_A_A.zip?

acerid=635067212785876098&Step1=NOTEBOOK&Step2=ASPIRE&Step3=ASPIRE%20E1-571&OS=ALL&LC=pt&BC=ACER&SC=PA_3

Reply

Replies

donovan6000 July 11, 2013 at 1:36 PM

Lol 2 days is nothing. I spent 3 weeks just trying to get one of the tabs unlocked. Try this out and let me know if anything changed.

http://www.mediafire.com/?t4kufucgcu7dpwy

Also I'd recommend you get a way recover incase something goes bad? All I did was replace one of the existing tabs with a different one. I'd like to try out some other ways to unlock the tabs, but some of these other methods can result in a brick. So I'm only going to do really safe mods until you get a way to recover. Don't want to accidentally brick you laptop :)

Felipe Furtado July 11, 2013 at 4:39 PM

Hey, thank you for replying so fast

I tried to flash, the flash process was incredibly fast (it started and rebooted 2 seconds after).
When the computer turned on again, a message saying "InsydeH20 - invalid bios ... press any key to reset system..."

pressed enter and the default bios was back on.

Obs: the .fd file in this compilation is 6.603 kb, can this be the reason?

Thanks again

Felipe Furtado July 11, 2013 at 4:48 PM

if i use this Q5WV1X64.fd original file on the usb drive, i will be able to recovery in case of a brick with FN + ESC function correct?

donovan6000 July 11, 2013 at 5:50 PM

Turns out Acer implements a protection against flashing corrupt/modifies bios roms. Not sure about the Acer recovery procedure, but that sounds right. Also be aware that there's always a chance that something unrecoverable can occur when flashing bios, so it's entirely your choice if you want to continue.

Try this and let me know if you get the same results.

http://www.mediafire.com/?t4kufucgcu7dpwy

Felipe Furtado July 11, 2013 at 6:05 PM

the exact same result... :/ (kind of crapped my pant's when i hitted "OK") lol
don't want to bother you though... I just would like to access those settings to install mac os x. Can't boot the setup disk with these current bios settings...

donovan6000 July 11, 2013 at 6:50 PM

Thought so. Fortunately people have shown successful by flashing the modded bios with the recovery procedure. I had today off, so it's not a bother at all.

Now we just have to get to the point where we can recover, then we can continue modding from there. Try putting the bios rom in the most recent file I uploaded on a fat32 flash drive and boot while holding down FN+ESC. If the fan speeds up then that's a good indication that it's working. Your computer should restart on its own when it's done recovering.

Felipe Furtado July 11, 2013 at 8:09 PM

Did that, the laptop bipped 5 times then restarted.
The bios is working fine, but nothing changed, menu stills the same.

Any clue?

donovan6000 July 11, 2013 at 10:32 PM

How long did it take before it restarted? Can you dump your bios again and send it to me?

Felipe Furtado July 11, 2013 at 11:09 PM

interesting... the file size still the same after flashing....
here's the link (dumped with Universal Bios Backup)

http://www1.datafilehost.com/d/86fba10e

Felipe Furtado July 11, 2013 at 11:10 PM

took around 30 - 50 secs to restart

donovan6000 July 12, 2013 at 12:05 AM

Unfortunately the recover procedure didn't flash the modified bios. Try this recovery procedure with this rom.

http://www.mediafire.com/?44n2yafqednq9uy

1. Put it on a fat32 formatted flash drive. Shut down computer and unplug flash drive.
2. Unplug AC adapter and remove battery

3. Plug in usb
4. Hold down FN+ESC then plug in AC adapter. You can also put the battery back in.
5. While still holding the keys down, press the power button. It should flash the bios rom.

Hope that works. After if finishes, dump it again and send it to me. Thanks for trying out so many different things.

Felipe July 12, 2013 at 7:50 AM

Tried that but nothing happened.

I renamed the file to Q5WV1.FD, now it's flashing i think... but it's been like 30 min since it started, usb is blinking and there is hdd activity...

I don't know what the outcome is gonna be, but i google it and there is a guy saying that his hp took arrond 20 hours to complete the process lol

Now i just have to wait

Felipe Furtado July 12, 2013 at 8:06 AM

Update: I saw the flashes was doing the same blinking over and over again, so I turned off the computer, turned on again, and everything was back to normal as i was before...

lol, i'm lost

donovan6000 July 12, 2013 at 1:46 PM

Try doing it without any bios rom on the flash drive. I'm thinking it took 30 mins because it was trying to locate the correct file on the flash drive, but since it didn't exists it just waited forever. The same thing happens on my laptop.

Also just ran across a post on MDL by Serg008 where someone was having a similar problem to what we're facing. Try out the recovery with his instructions and this rom. Send me a bios dump afterwards even if it looks like it didn't work. Thanks.

http://www.mediafire.com/?44n2yafqednq9uy

http://forums.mydigitallife.info/threads/7033-Insyde-bios-mod-requests/page1317?p=715907&viewfull=1#post715907

Reply

Garrett July 26, 2013 at 2:05 PM

Hi Donovan, I have a couple of questions regarding the bios modding process that you have detailed here.

I am working on modding the bios of a new HP envy 15z-j000. The bios is f.08, H20, rev. 3.7. using phoenix mod tool 2.14 I was unable to open the bios that I had removed from the latest bios install package from hp. In order to circumvent this I dumped my efi bios via aida64. From there I was able to edit them via phoenixtool 2.14, use IDA, as well as a hex editor on them.

The point of my question is this: Will I be able to flash this dumped bios image after I have edited it? Will I have to recompile or rename it into something else, or will I have to wait until the developer of phoenixtool is able to support my bios?

My other question is in regard to the offsets and jumps in IDA. I have 22 offsets and am not encountering jumps in the same way that you have described. Is there any sort of thought or hint you could bestow that would get me on the right track.

Thanks for your help and your awesome site. It is much more well organized and has a lot more information than most of the bios modding forums that I have been searching on.

Reply

Replies

donovan6000 July 26, 2013 at 10:35 PM

Hey Garrett,

Unfortunately those bios are RSA signed, so your not going to have any luck with modding them. Even if you only change one byte, your laptop will be bricked after flashing the modification. Make sure you know how to recover beforehand if you want to see this for yourself.

You can flash decrypted bios, like the one you extracted with Aida64, by using Insyde's flasher. But this will be useless in the end because of the RSA protection I mentioned.

There is no sure-fire way to enable the advanced tab in every bios since no two bios revisions are the exact same. Even though I made it look easy, it should still take most people weeks of reverse engineering and testing just to accomplish this task.

Sorry I couldn't be of more help. I know I probably told you the exact opposite of what you were hoping for. I don't own a laptop with unmoddable RSA bios so I don't have much more insight than this. I'd like to buy one just to try to bypass the protection, but I don't have the money right now. Glad you enjoyed the site.

Reply

Anonymous August 8, 2013 at 11:34 AM

please can you mod my bios to unlock advanced menu
http://h10025.www1.hp.com/ewfrf/wc/previousVersions?softwareitem=ob-115746-1&cc=us&dlc=en&lc=en&os=4063&product=5090717&sw_lang=

Reply

Replies

donovan6000 August 8, 2013 at 12:24 PM

Unfortunately your bios are RSA signed, so any attempt to mod them will result in a brick. However you can still manually change all the settings in your setup utility even though you don't have access to them. There's a tutorial here on how to do that if you have access to an efi shell. And I'm currently working on a tutorial that goes over how to do it without a shell.

http://www.bios-mods.com/forum/Thread-HOWTO-access-you-BIOS-settings-through-EFI-shell?pid=56913#pid56913

Reply

Anonymous August 11, 2013 at 5:43 AM

My bios is RSA signed. So Please help me to unlock advanced menu with your tutorial please or please mod I want to increase my vram 64mb :'(
http://h10025.www1.hp.com/ewfrf/wc/previousVersions?softwareitem=ob-115746-1&cc=us&dlc=en&lc=en&os=4063&product=5090717&sw_lang=
Sorry my bad english I'm asian

Reply

Replies

donovan6000 August 11, 2013 at 4:55 PM

As I said in my previous comment, any attempt to mod RSA signed bios them will result in a brick. Feel free to follow this tutorial that goes over how to change the setup's settings via an efi shell. I'm also writing a tutorial on how to do it without access to an efi shell right now.

http://www.bios-mods.com/forum/Thread-HOWTO-access-you-BIOS-settings-through-EFI-shell?pid=56913#pid56913

Reply

Artziz Aziz August 22, 2013 at 7:51 PM

Hey donovan,
Would you unlocking my HP laptop Bios advanced menu and whitelist removal, i already tried but every time i open the Setup utility (ROM) with IDA Pro, there's no automatically detected processor, so im kinda confused.
this is my bios link : http://ftp.hp.com/pub/softpaq/sp52501-53000/sp52604.exe
i found that someone has already made it, here's the link : http://www.bios-mods.com/BIOS/Insyde/sp52604_142xOnly_Ulk_Menus_ByCamiloml.exe,
but unfortunately it wont save the bios changes, it's only get hang and all i can do is only press power button to turn of or pressed ctrl+alt+del for restart.

thank you very much indeed :D

Reply

Replies

donovan6000 August 22, 2013 at 10:21 PM

Make sure your opening the correct setup utility module. There will probably be 2 - 4 of them in the DUMP folder. The biggest one is what your going to want to disassemble.

Unfortunately I'm not going to do the work for you unless your willing to donate. The point of this blog is to get more people to do it themselves. I'm sure you'll be able to mod it on your own without me. Good luck!

Reply

Germano José August 24, 2013 at 4:27 PM

Hi Donovan6000, I´m trying to open this file but I see RSA security.

Could you unlock advanced tabs from this ROM

http://www.dell.com/support/drivers/us/en/04/DriverDetails?driverId=F3GDC&fileId=3103841226

It´s from Inspiron 15R SE 7520

I can buy you a beer.

Please could you help?

Reply

Replies

donovan6000 August 24, 2013 at 10:54 PM

Not sure why you think it's RSA signed. So far HP is the only computer manufacture that has signed their bios with an RSA key, and I doubt that Dell will ever start doing that.

So your bios has 9 tabs in total:
1. Advanced 0x8BCC0
2. Power 0x89830
3. Main 0x89300
4. Security 0x87310
5. Boot 0x86170
6. Exit 0x954C0
7. Wireless 0x85E40
8. Advanced 0x850E0
9. Main 0x95220

It's not unusual to see multiple tabs with the same name as your Main and Advanced tabs are here. Unfortunately there's no obvious way that any of these tabs are being hidden, so the best I can do is swap the existing tabs for the hidden ones. If your fine

with that then tell me what tab you want to give up and which one you want to swap in.

For more details about each individual tab, here's a document with all the setting under each one. Curtsy of Falseclock's perl script.

http://www.mediafire.com/?tl37zxuqo1oivqb

Reply

Zeemanv2 August 27, 2013 at 8:25 AM

Hey Donovan ive read ur tutorial for unlocking tabs its a gr8 tutorial . Bt i want to change my boot logo/splashscreen coz i got a laptop from my college (Hp Pavilion G4 1303AU) and they burned their image on the chip. So everytime i boot i have to face that creepy logo.Is it possible if yes then how to do that?

Detailed info of system----------

OS Name Microsoft Windows 7 Ultimate
Version 6.1.7600 Build 7600
Other OS Description Not Available
OS Manufacturer Microsoft Corporation
System Name AIMAN-PC
System Manufacturer Hewlett-Packard
System Model HP Pavilion g4 Notebook PC
System Type X86-based PC
Processor AMD A4-3330MX APU with Radeon(tm) HD Graphics, 2200 Mhz, 2 Core(s), 2 Logical Processor(s)
BIOS Version/Date Insyde F.6A, 13-05-2013
SMBIOS Version 2.7
Windows Directory C:\Windows
System Directory C:\Windows\system32
Boot Device \Device\HarddiskVolume1
Locale India
Hardware Abstraction Layer Version = "6.1.7600.16385"
User Name Aiman-PC\Aiman
Time Zone India Standard Time
Installed Physical Memory (RAM) 2.00 GB
Total Physical Memory 1.48 GB
Available Physical Memory 795 MB
Total Virtual Memory 2.96 GB
Available Virtual Memory 2.01 GB
Page File Space 1.48 GB
Page File C:\pagefile.sys

Detailed info of mobo----------

Manufacturer Hewlett-Packard
Model 3564
Version 069113000020461000061010O
Chipset Vendor AMD
Chipset Model ID1705
Chipset Revision 00
Southbridge Vendor AMD
Southbridge Model ID780E
Southbridge Revision 11

BIOS
Brand Insyde
Rev 3.5
Version F.6A
Date 05/13/2013
PCI Data
1. PCI Available
2. PCI Available

Ive read in a post where a guy with similar bios replaced the logo (he had lenovo).Link is-- "http://www.deezthomas.com/9-tutorials/20-tutorial-change-bios-splash-on-lenovo-b460e-tn-govt-laptop.html?showall=&limitstart="

Im was a total noob at bios related stuff bt after going through several dozen forums and googling thousands of pages, now i can say i started to understand a bit. What ive done is taken backup of my bios with universal bios backup and try to edit with ezh20 bios editer. I found the logo which is displayed at boot bt since mine is hp so .bin files are necessary. After editing it gives only one .bin file bt after extracting fresh bios from hp it has 3 .bin files while in lenovo there's only one replace that n u r good to go. So i dont know which file to replace? So this method wont work for me right? Then i found ur blog , i guess im super lucky coz i havent found a blog/post related with insyde bios modding yet n trust me ive literally gone through if not thousand then several hundred pages (not slept properly for about 12 days, yeah really). Btw i see u r using insyde flash tool i.e. flashing from windows which as far as i done my research, not safe coz if anything goes wrong then ur mobo is done. So plz i request u to mod my bios and plz make it uefi compatible (flashable via hp efi utility). Here's the link-- "http://www.mediafire.com/download/vwqq0k2gj3j2q04/Installed_Bios.zip"

Ive given this to a guy @mdl forums bt he couldnt make efi flashable bios. Ive attached everything u need in zip file so plz mod with requested image and sorry for this extremely long post. I found this blog so im super excited bt super exhausted too coz of researching. So i told u everything i know and asked u everything i wanna know. TIA

Reply

▾ Replies

donovan6000 August 27, 2013 at 1:16 PM

Lol you still sound like a total noob with this stuff XD

I'll try to clear some stuff up for you. Bios updates often will have multiple roms in them so that they can support multiple types of systems. That's why your installer has 3 different roms. Only one of them is actually flashes into the bios region of your bios chip though.

I would never recommend you use the universal bios backup toolkit. The author even says that he can't ensure that the backups it creates are correct for every system. There are much better methods available of making bios backups.

Insyde's Windows flash tool is just as safe as any other method. If it weren't, then HP wouldn't use it in their bios updates. The bios

recovery procedure for HP computers is not located in the bios region of the chip, and this is the only region getting overwritten when installing a bios update. So even if it does mess up, you can most likely still recover. I've flashed my bios over 100 times and have not had a single problem. Just so you know there is always some risk involved when flashing any kind of chip. We can't predict their behavior under certain conditions.

No one is currently capable of making it so you can flash a bios rom via HP's efi utility. It requires knowing HP's private RSA key in order to create the signature necessary for the flasher to accept the rom.

Hope that clears up all your misassumptions. Now here's the solution to your problem. Just run the official bios update from HP and it will overwrite the logo with the original HP one. You might have to edit the platform.ini included in the bios update incase it doesn't overwrite the logo by default. Like this:

[ForceFlash]
ALL=0
BB_PEI=0
CPU_Microcode=0
Variable=0
DXE=0
EC=0
Password=0
OEM_NVS=0
Logo=0 <--- Change this to Logo=1
Type#09=0
Type#08=0

Zeemanv2 August 28, 2013 at 1:10 PM

"You still sound like a total noob with this stuff XD" Lel (Laughing extremely loud) im not noob its just that im over cautious n to brick my new laptop for a logo isnt worth it.

Yup u r right about value of logo in platform.ini its set to "0". After changing its value to "1" did i have to recompile it to flash or just run insydeflash installer? I assume changing value to "1" will bring stock hp logo right? What if i have to use a custom logo? Btw i flashed an updated bios available from hp. I thought it will change logo bt it didnt changed it. Altering the value will certainly change it, are u sure coz i didnt have a recovery usb stick to recover if things get messy thats why im not trying everything until its safe.

You said "No one is currently capable of making it so you can flash a bios rom via HP's efi utility. It requires knowing HP's private RSA key in order to create the signature necessary for the flasher to accept the rom." Well im not an expert in any way n relatively new to bios related stuff bt i know a thing or two. You can make bios file flashable via efi by using Andy's Phoenix Tool. You need .bin and .sig file to flash bios. Using Andy's tool u can make these files n put it under Hp tools partition under hp/bios/new. Then u can flash via efi utility at bootup. Dont ask me how to do this coz a guy made me those files n for hp systems, the files have to named acc. to system board id no. to flash correctly. Is this what u were referring to? If not then pardon me.

donovan6000 August 28, 2013 at 2:50 PM

It's alright, I was overcautious too when I started. I've probably bricked my computer over 40 times since then XD

Yep, all you need to do is change the 0 to a 1. Then just launch InsydeFlash.exe and it should update the logo. I personally set my platform.ini to force flash all regions. If you want to create you own logo then I wrote a tutorial on that here:

http://donovan6000.blogspot.com/2013/06/insyde-bios-modding-splash-screen-logo.html

So Andy's tool decrypts the bios rom with HP's public RSA key. This also produces the signature file which is used by HP to verify the bios rom when flashed via efi. That .sig file is unique and will not verify any other roms expect the one it was made for. So any modifications to the bios will require a new .sig in order to flash it via efi. Unfortunately we can only generate the .sig when the bios is previously encrypted by HP or if we know HP's private RSA key. You should look up some YouTube videos on RSA encryption as they do a very good job of explaining it.

Zeemanv2 August 30, 2013 at 7:53 AM

Oops!! Tried to teach u something which i even dont know properly. LMFAO

Nope changing the value of logo to 1 under heading force flash didnt replace logo. What i did was downloaded a fresh bios from hp, extracted the bios installer by winrar. Edited n saved the platform.ini . Run insydeflash.exe which was in the same folder as other files. Informed u so that u know n if i made a mistake in any step, let me know.

Can u suggest anything else besides-"http://donovan6000.blogspot.com/2013/06/insyde-bios-modding-splash-screen-logo.html". Coz finding one file among that heap would be pain in the a**.

Btw now ive created recovery usb stick. Throw anything at me now.

donovan6000 August 30, 2013 at 1:11 PM

Not sure why it's not changing the logo then. The next option would be to try modifying the logo in your complete bios dump and flashing it back. You can use Intel's flash programming tool to read/write the whole bios region to achieve this task.

Lol you sound lazy. My splash screen logo tutorial goes over a few ways of easily isolating which module contains the logo. You can use Ezh20 to accomplish the same results though. I didn't mention that tool in my tutorial because it only works on older Insyde bios and I want my tutorials to be as generic as possible.

Zeemanv2 August 31, 2013 at 1:10 AM

Lol u r funny. I may sound lazy bt if i want something i work my a** off. I searched for JFIF, BM, n PCX thru xsearch. It gave me about 33 results. I changed extension of each to .jpg then .bmp then .png bt it showed me nothing. 33 for each format= 99. If i was lazy i wouldnt have done it n simply be depended on u bt atleast i tried.

As for ezh20 tool it shows same logo at bootup bt i didnt patch any other image coz i dont know which bin file to replace in bios folder.

Zeemanv2 August 31, 2013 at 6:28 AM

Do u know "LatinMcG" ? He's a gr8 guy. Listen all my prob's n answer to all my stupid Q's.

He gave me two bios files- one to flash via efi, which we know it cant be flashed coz hp's prv8 rsa key n all. Second one to replace bin file in original bios folder then flash via insydeflash. I thought it would flash but it gave a error- "Bios image is corrupted or does not contain the correct digital signature. The Bios will not be updated."

You have ubuntu , so plz will u look into my current bios dump folder n if u can change the logo i will more than grateful. THANKS IN ADVANCE.

Link-"http://www.mediafire.com/download/52kwbszvede4ujs/DUMP.rar"

donovan6000 August 31, 2013 at 10:47 AM

I don't personally know LatinMcG, but I know he's very well known in the bios modding communities. I can't believe you have two great bios modders helping you for something as simple as changing a splash screen logo XD

That "bios image is corrupt error" has to do with InsydeFlash.exe verifying the rom before flashing it. I wrote a tutorial on ho to bypass it here:

http://donovan6000.blogspot.com/2013/06/insyde-bios-modding-getting-started.html

And here's the info on your logos. They're all jpegs.
HP Logo: 37946B52-EC4B-46AF-AB83-76DBBE1E13C4.ROM
Red Logo (lol): F882368D-2013-0124-3E20-5D836C57DCD3.ROM
White Logo: D72B868D-46E6-41D1-8220-5D836C57DCD3.ROM

Zeemanv2 August 31, 2013 at 12:27 PM

"I can't believe you have two great bios modders helping you for something as simple as changing a splash screen logo XD." Well what can i say? I guess im super lucky to be helped by not one bt two of this field's greatest. Im truly humbled.

U said in ur logo changing post to change the extension of files to jpeg so that u can view the logo n edit it right? Then explain this-I changed extension of the above .rom files to .jpeg but they still cant be opened/accessed. What's ur say in this?

If they cant be opened how am i supposed to edit them?

You n LatinMcg-two gr8's are helping me, im really honoured but whatever u guys are doing, u r expert in that n doing it for 3 or more years whereas its not been 3 weeks i got this laptop. So wrap around my head to whatever u say is quite difficult for me but im trying to get as much possible to get into my head n im quite happy with my progress coz ive never touched bios related stuff not even tried to update my computer's bios n look where am i in just about 1-1.5 weeks, i flashed my bios 3 times already n ready to flash more whether it will make or brick my computer.

So i request u to bear with me a lil more.

P.s. I know u have a blog to look after but if u can come to mdl forums i will be greatly honoured. Then i wont have to post at two places n u both can know current status n help me together.xD

donovan6000 August 31, 2013 at 9:51 PM

Recently Andy's tool was updated and he changed the format of the files in the dump folder. The first few bytes have to be removed so that the image file can be recognized. Then these bytes have to be added back so Andy's tool can repack all the changes. I'm going to start working on a program soon that can assist in this.

Lol 3 years? I've only been doing this for 9 months now, but a bulk of my discoveries happened in the first 3 months.

I have no problem continuing to help you. You have a great sense of humour which makes helping you kind of enjoyable. Ok, we can keep this in you MDL post from now on. So for anyone else reading these comments, this discussion is being continued in this thread:

http://forums.mydigitallife.info/threads/47165-Please-help-me-out

Reply

Claudio Sánchez September 3, 2013 at 10:16 AM

Hello. I have followed this tutorial until the point where I should open the isolated setup utility module with IDA Pro...

A software I don't have at all, and cannot find. I found 6.1 but it seems NOT to open the file properly, so I cannot use the function to get the 'referenced' function at all.

I managed, however, to unhide several options as you tell in the other tutorial.

Reply

Replies

donovan6000 September 3, 2013 at 10:55 AM

Andy changed the output of the dump files in his newest version of his tool. You have to manually remove the first few bytes, so that the first bytes are 0x4D 0x5A, then IDA pro will recognize it. Make sure you add the removed bytes back after your done modifying that module.

fiddlesticks October 24, 2013 at 12:11 PM

Could you update your tutorial(s) to include this?

Thank you!

donovan6000 October 24, 2013 at 2:21 PM

I'm planning in updating my tutorials after I get done creating a program that can assist in this procedure. I have a linux version of my program done, and I'm slowly porting it over to windows before releasing it. If you happen to know any window GUI programming and would like to help, then that'd be awesome.

fiddlesticks October 29, 2013 at 10:23 AM

I would help if I could. Let me know if you need any webdev help though haha.

Reply

Claudio Sánchez September 4, 2013 at 11:03 AM

OK. Now I have it. But I cannot find the conditional jumps you say. I found where the tab headers are, and located the functions that call them, but found no conditional jumps whatsoever.

But I can see a lot of extra text that I cannot see in the BIOS setup, including strings in different languages.

Reply

Replies

donovan6000 September 4, 2013 at 12:02 PM

All of my tutorials that you've managed to complete already were very simple and easy. They gave step-by-step instructions of exactly what to do. This one isn't nearly as nice.

No two bios versions hide the hidden tabs in the exact same way. Because of this I was unable to keep this tutorial as generic as some of the others. So your going to have to do a lot of the reverse engineering yourself in order to understand how it chooses which tabs to display.

Those groups of strings are how the bios can be localized between different countries. That's how my EFI IFR Dumper asks which language to choose by finding the available string packages first. If you want to know where everything located, my EFI IFR Dumper also shows the offsets of all these string packages and all the offsets of form sets (tabs).

Claudio Sánchez September 4, 2013 at 2:03 PM

Thanks. This seems to be my fishing point. Because I'm not a programmer I cannot do that reverse engineering. I don't know what do what thing. I managed to update de microcodes, and unhide some settings by changing the default value of some variables. But I know nothing about machine language.

Maybe if you want, I can send you the module and you could take a peek.

donovan6000 September 4, 2013 at 8:39 PM

You should be proud of yourself. You managed to make it farther than most people :)

Unfortunately I don't take requests unless your willing to donate. One of the purposes of these tutorials is to get more people involved by having them do it themselves. It's taken me more than half a year to to get this far, and I know it can be quite intimidating when you get started. Good luck!

Claudio Sánchez September 5, 2013 at 3:14 AM

Thanks. I will keep an eye on your "coming soon" utility that properly rips off the VGA BIOS to overclock it.

Reply

marwen September 13, 2013 at 9:38 AM

hallo donavan!! is there any possible way to change temperature throttling on acer aspire v3 571G (GT730M) witouhtmodding the bios????? you said that you will create a programme to change settings manual??? so is there any news????? also i tried to use your EFI dumper but an error msg comme up it said "Error: Form set not found
Appuyez sur une touche pour continuer" so is there any solution??????

Reply

Replies

donovan6000 September 13, 2013 at 9:57 AM

There might be a way to do it without modding it your able to find which offset in your setup's efi variable contains the value that controls the throttling temperature.

I never said I was creating a program to change settings manually. Your getting that confused with the program that I am making that separates the header and data information for the efi modules.

However I did create a tutorial on how to change settings manually here. Be aware that it might not work for you because your bios might be encrypted.
http://donovan6000.blogspot.com/2013/08/insyde-bios-modding-manually-changing-settings.html

My EFI IFR Dumper is designed for EFI's internal form representation protocol. You bios probably uses UEFI's protocol, which my program currently doesn't support. There's plenty of documentation from Intel on it, so it shouldn't be too difficult for you to reverse engineer it yourself. Good luck!

Reply

marwen September 13, 2013 at 10:30 AM

oh sorry !!! so my bios is an insydeh20 bios rev 3.7 version 2.15 of the acer aspire v3 571G (730M) is encrypted??? for the protocol yes it use UEFI protocol so the methode to manual change setting using EFI shell will not work????? please if is there any way to manual adjust the GPU temperature and the fan speed let me know it beacause i didn't found any solution!!!!!!!!!!!!!!! and thkx

Reply

Replies

donovan6000 September 13, 2013 at 10:43 AM

I never said your bios is encrypted. I said your efi global variables might be encrypted.

Nowhere in my tutorial do I use an efi shell to change settings. I think your mistaking my work for Falseclock's. Although his tutorial will probably work with your bios.

If nothing works for you, then your going to have to experiment and determine how to change the settings yourself.

Reply

marwen September 13, 2013 at 10:50 AM

thank you dononvan6000 for helping me and sorry another time!!!!!!!! help it work with me because i am tiered with low set temp throttling from the acer !!! ican't even play a game more than 1min with this GPU 730M 4GB!!!!!!!!!!

Reply

Replies

donovan6000 September 13, 2013 at 11:57 AM

Unfortunately I'm not going to do the work for you. This blog is to try to get people more involved by allowing them to mod their own bios. Bios modding isn't an easy task and it can take several months to get the results you want. It took me nearly 3 weeks before I was able to unlock the advanced tab in my own bios. If your not willing to spend this amount of time, then I'd recommend you just buy a different computer.

Reply

k3resnk1 September 13, 2013 at 6:44 PM

Hello,
I'm having trouble following this tutorial. I have an Insyde BIOS R0142C5, when I get to the part where you open the SetupUtility module under IDA Pro: there is only one file with the correct GUID in the DUMP folder and when I open it in IDA, it only recognizes it as a binary file. I'm not sure if mine is encrypted or something ?

Reply

marwen September 22, 2013 at 2:44 PM

hallo donovan6000 again !!!!!! please need help i want to change bios settings without moding it!! i will use the EFI shell to do it!!!!!! but the probleme that i'm not able to have the log file wich containt the advanced setting of my bios!!!!!!!i use the code(perl at a console) but i have an error!! it said "
Use of uninitialized value in numeric lt (<) at uefidump.pl line 245.
Can't use an undefined value as an ARRAY reference at uefidump.pl line 69"
so the log file can't be generated?????????? so please help.....

Reply

Replies

donovan6000 September 22, 2013 at 8:44 PM

Not really sure why your asking for my help regarding Falseclock's perl script. I was not involved in its development in anyway, so I can't provide any troubleshooting support for it. Unfortunately Falseclock hasn't been involved in the bios community for several months, so your probably going to be waiting for a long time for anyone to help you. It's probably be easiest to just create your own program to dump the UEFI IFR into a human readable form.

Reply

marwen September 23, 2013 at 9:26 AM

tknx for answer!! but the probleme is that i don't know how to do it!!!! also tried to mod my bios , i extracted the setup utility module and do like what you do with ida but the probleme that i'm unable to identify the location of the tabs offset exactly so i decided to adjust the settings i want manualy using EFI shell but you know i'm not able to have the log file so i can't do anything.....

Reply

Replies

donovan6000 September 23, 2013 at 10:15 AM

Bios modding is not easy. It took me several months before I was able to get the results I wanted, so expect to spend at least this amount of time working on your own bios. I wrote these tutorials and created these programs to give people some ideas of how to actually get started. However, even with all of these additional resources, bios modding is still very challenging if you've never done anything like it before. There are no shortcuts for this kind of things, so don't expect this to be easy.

Reply

War10ck October 2, 2013 at 7:42 AM

hi Dononav.. really a nice tutorial over here.. i m having trouble with my bios modding as u described here... First i backed up my Bios using Universal Bios Backup Toolkit which gave me the *.rom of my bios.. i imported it into the Andy's Tool, structured it and got the DXE, decompressed it and found "SetupConfig instead of SetupConfiguration" but i still went on and found the "setuputility" :) .. now next when i imported the setuputility module into IDA PRO 6.1, the program(IDA PRO) said that the recognized format is a Binary File and i still went on further.. now the problem is i cannot see the graph as it is asking for entry point to analyse file which i don't know.. how to find that entry point or how to make IDA recognize the file type.... pls help...

Reply

Replies

donovan6000 October 2, 2013 at 11:58 AM

The latest version of Andy's tool changed the format of the files in the DUMP folder. They now have some extra data in their header that makes it so IDA Pro can;t automatically detect the file format. Remove the first few bytes in the module until the first two are 0x4D 0x5A. Then you can disassemble it in IDA Pro. Just make sure to add those bytes back after your done modifying the module so that Andy's tool can repack everything correctly. Good luck.

I'm slowly working on a program that can assist in this procedure. I already have a linux version done, but I want to port it over to windows before releasing it, If you happen to know any Windows GUI programming and would like to help, then that'd be awesome :)

Reply

War10ck October 3, 2013 at 1:34 AM

Thanks donovan.... srry donovan but i m not that skilled in GUI yet.. i m student of 3rd sem.. :)

Reply

Juan Manuel October 4, 2013 at 5:51 AM

hi donovan i want to unlock the bios of a HP Notebook G42461la to get the advance menu but i tried following your tutorial but its so diferent you can help me to unlock it pls this is the link of the bios:

http://ftp.hp.com/pub/softpaq/sp52501-53000/sp52604.exe

pls i need it to install fedora 19 ot hackintosh ;) thx

Reply

Replies

donovan6000 October 4, 2013 at 9:26 AM

Unless your willing to donate, then I'm not going to do the work for you. One of the goals of this blog is to get more people involved by giving the some references that will help them along the way. I'm sure you'll be able to do it yourself if you just put in the time and effort required. Good luck!

Reply

Anonymous October 4, 2013 at 7:27 AM

Does advanced tab give overvolt options?

Reply

Replies

donovan6000 October 4, 2013 at 9:24 AM

I've only seen one bios that actually had its CPU clock settings inside its bios options. That was for an HP mini 311. It's extremely rare for HP and Insyde to keep them in the bios, so don't expect for them to be there. If your bios uses EFI IFR protocol, then you can see all the options available in your bios by using my program here:

http://donovan6000.blogspot.com/2013/07/efi-ifr-dumper.html

Juan Manuel October 4, 2013 at 10:41 PM

how i can donate? where? i dont have a lot of time thats why im asking for your help pls

donovan6000 October 5, 2013 at 12:10 AM

There's a donation tab in the menu bar at the top of my blog. It's kind of hard to miss. Here's a direct link:

http://donovan6000.blogspot.com/p/donate.html

Donating should be a last resort though. Reverse engineering software is an extremely challenging task, but it's also very rewarding. It's well worth taking the time to learn how to do it. I would really much rather have you accomplish this task on your own through handwork and determination.

Reply

nearffxx October 4, 2013 at 9:48 AM

I have mooded the HP Palivion dv5-1144el BIOS by adding the debug and power tab.
So I'm gonna share if anyone need it.
http://www.megafileupload.com/en/file/457510/3602F21-SLIC-fd.html

Reply

Replies

donovan6000 October 4, 2013 at 9:58 AM

Nice job! Thanks for sharing it with everyone :)

Reply

Anonymous October 4, 2013 at 10:19 AM

I have a bios sp55299, it is different and when I edit it with IDA pro, it doesnt give me any portable executable. It just shows binary. Would appreciate any help. It would be better if you give me steps on a txt file or in this blog.

Regards Eesa

Reply

▼ Replies

donovan6000 October 4, 2013 at 10:35 AM

That's because the latest version of Andy's tool changed the format of the files in the DUMP folder. They have some extra data in the header that makes it so IDA Pro can automatically detect the file format. You have to remove the first few bytes until the first two are 0x4D 0x5A. They IDA Pro will detect the proper format. Just make sure you add those removed bytes back after you done editing the file so Andy's tool can repack the bios correctly.

I've made a program for Linux that can assist in this process. I'm waiting to port it over to windows before releasing it. If you happen to know any windows gui programming and would like to help, then that'd be awesome!

Reply

URCHMAN October 11, 2013 at 3:38 AM

Thanks very much for such a good tutorial, it took me weeks to search the internet to get a good tutorial like yours.
i tried your steps in editing my own BIOS but along the line i couldn't locate some options in my Andy's tool, maybe because of varying version.
Please i want you to help me to unhide my advance settings. Details of my Laptop is as follow
Manufacturer: TOSHIBA
-Model: Satelite ProC650
-Bios Type: INSYDE
-BIOS VERSION: 1.7
-BIOS SLIC: 2.1
-LINK TO BIOS: http://rt3.getdownload.net/downloadhelper/named/desktop_4031/6JIyqJ64/BcGNLKzj/bios-20120912135921.exe?dsid=xmjup.550e0b3b34266487fb7688a25d4a58f8

Thanks in Advance

Reply

▼ Replies

donovan6000 October 11, 2013 at 7:40 AM

What options couldn't you locate in Andy's tool?

And the newer versions of his program change the format of the files in the DUMP folder so that they have extra stuff in the header. This makes it so IDA Pro can't automatically detect the format. So you have to remove the first few bytes until the first 2 are 0x4D 0x5A. Then you can disassemble the modules. Just make sure you add those removed bytes back after editing the module so his program can repack the bios correctly.

URCHMAN October 11, 2013 at 8:26 AM

okay i will give it a try, but still help me in unhiding/unlocking ADVANCE TAB or any Hidden Options on my bios, you are a Pro am still learning, the work u did yourself is preferable than mine.
once again Thanks Man.

donovan6000 October 11, 2013 at 3:22 PM

The information in my tutorials show be enough to get you started. One of the purposes of my blog is to get more people involved by allow them to mod their own bios. I'm not going to do any of the work for you unless your willing to donate.

Reply

Unknown October 11, 2013 at 3:10 PM

This comment has been removed by the author.

Reply

Robert Candeletti October 11, 2013 at 3:13 PM

Every time I open the FE3542FE-C1D3-4EF8-657C-8048606FF670 file (happens to be the same for my BIOS) in IDA it tells me it can't detect the file type and will only load it as a binary file. I keep getting stuck here. Any suggestions or help would be appreciated. This is my first dive into this type of edit and with no experience in IDA and limited experience in hex I keep getting frustrated and lost.

My laptop is a HP Folio 13-1020us with the bios files located at http://h10025.www1.hp.com/ewfrf/wc/softwareDownloadIndex?softwareitem=ob-115580-1&cc=us&dlc=en&lc=en&os=4063&product=5218370&sw_lang=

I would like to be able to enable UEFI boot in the bios and the option is currently unavailable.

Again, thanks for any help and if there is anything I can do to repay you please let me know. I would not be against sending you some money for a 6 pack or the like via Paypal.

Reply

▼ Replies

donovan6000 October 11, 2013 at 3:19 PM

Lol I have to repeat this all the time. The newer versions of Andy's tool change the format of the files in the DUMP folder so that they have extra stuff in the header. This makes it so IDA Pro can't automatically detect the format. So you have to remove the first few bytes until the first 2 are 0x4D 0x5A. Then you can disassemble the modules. Just make sure you add those removed bytes back after editing the module so his program can repack the bios correctly.

I made a program for linux that can assist in this process. I'm want to port it over to windows before I release it though. If you happen to know any windows GUI programming and would like to help, then that'd be awesome.

Ans I always appreciate donations :) My donation page is here: http://donovan6000.blogspot.com/p/donate.html

Robert Candeletti October 11, 2013 at 5:51 PM

I'm kind of diving into all of this head first, so thanks for the nudge in the right direction. I'm actually doing all of this because I want to convert to a GPT partition scheme (and partially because I can) and HP of course blocked me from booting UEFI. I wish I was able to code much more then basic java and html. :-P I'm working on it though. Anyway, if you have linux tools that could help aid in this process I would be more then willing to test them for you. I run Debian on dual boot. The guide so far has been a huge help and I'm enjoying learning the background on what makes up my bios. If needed, my contact is robcandeletti at gmail if needed. Keep an eye out for a few bucks. :-D

donovan6000 October 11, 2013 at 6:17 PM

Don't sell yourself short. Java and html are pretty good to know. HP should just update all their bios to natively support UEFI. One of my goals when I first started modding my bios was to get UEFI booting to work...it ended in disappointment though...

Your bios might actually be currently unmoddable. HP computers started adding in a verification for the bios sometime in 2011. So we'd have to know HP's private RSA key inorder to resign the bios to reflect any changes. Since the first bios released for your computer was in 2011, then I cant be sure. It will result in a brick if you mod any part of it if it does have the verification.

Just to be on the safe side, I'd recommend you make sure you can recover before you even start trying to mod it. One of my tutorials goes over how to do this with a flash drive.

If you get that working, then we can start trying to unlock its hidden features. Here's the linux tool I was talking about. Just direct it to the DUMP folder and press unpack to separate the headers from the data. Then press pack to repack them. http://www.mediafire.com/download/o3h3secdbo3bt02/Module+Helper

I was also very curious about bios when I got started. Fortunately there's a ton of documentation from Intel on the UEFI standard protocol, so you can find out how everything works. I spent a few days reading about the internal forms representation protocol used to display things like the bios setup menu. Fortunately everything about UEFI is standardized so all the bios that use it have the same formats for everything.

donovan6000 October 11, 2013 at 6:20 PM

And thanks for the donation :)

It's definitely nice to be appreciated for the hundreds of hours I've put into learning and perfecting bios modding. I hope you enjoy the journey as much as I did.

Robert Candeletti October 11, 2013 at 7:01 PM

Everyone deserves to be appreciated for their hard work. I think I may have hit a brick wall myself, but I appreciate the help either way. Definitely got a better understanding of how things work. I was able to get the file loaded in IDA, but when searching the offsets I wasn't able to find any conditional jumps where needed. I think the menu is visible but the option isn't. Might have to try manually modifying the setting using the other tutorial.

Are there more conditional jumps I should be looking for other then jz? In the IFR DUMPER tool it shows the options I want, and they seem to be inside conditional statements there, but I'm losing something in the IDA side of things. Again, thanks for the help.

donovan6000 October 11, 2013 at 11:30 PM

Lol a brick wall already? I know IDA Pro can be very intimidating and boring at first. I hate staring at disassemble code since it takes a while for the bigger picture to actually set in. The flow chart view that IDA Pro produces really helps with this though since you can see physical links of where function calls and jumps go.

So this tutorial isn't as generic as I would like it to be, but this is only because no 2 bios revisions hide the tabs in the exact same way. There might be different offsets, different conditional jumps, or the tabs might just be hidden in an entirely different method.

As it turns out, yours are hidden with a different method. One of the most common ways it to only initialize the tabs who's string IDs for their title string don't match specified values. That'll make more sense when you look at this part of the disassembled code in IDA Pro. I actually have to update my EFI IFR Dumper slightly for you to recognize this though. I'm getting tired, so I'll release the update tomorrow.

Also your bios is one of the weirdest I've ever seen. It's produced in 2013 but uses old protocols. All currently made bios used UEFI's IFR protocol instead of EFI's. But since my EFI IFR Dumper works on yours, then it has to be using EFI's protocol. I take back what I said before; your bios is definitely moddable :)

donovan6000 October 12, 2013 at 11:16 AM

Just updated my EFI IFR Dumper to show the string IDs. So here's a picture of the code in your bios that skips initializing the tabs: http://i44.tinypic.com/xfn953.png

---

Reply

Anonymous October 13, 2013 at 10:21 PM

Hi there, can you please explain what the pci configuration options are. I just want to look at what it is before modding bios. Any help would be appreciated.

Reply

▼ Replies

donovan6000 October 14, 2013 at 10:06 AM

The options available are different for each bios revision, so I can't assume that yours has the exact same options available as mine. If your bios uses EFI's internal forms representation protocol, then you can use my EFI IFR Dumper to see all the options available

in your setup utility: http://donovan6000.blogspot.com/2013/07/efi-ifr-dumper.html

Reply

Tim Walls October 28, 2013 at 9:20 PM

Hi Donovan,

Wandering if there is any way to complete this without the IDA Disassembler as it looks like the "Free" non commercial version does not work. I was able to run your EFI IFR Dumper tool, but not sure if I can skip the IDA part of the tutorial.

Tim

Reply

▼ Replies

Tim Walls October 28, 2013 at 9:41 PM

For a bit more info, I receive the "Processor type z80 isn't included in the installed version".
When I try the latest demo version 6.4 I receive that it can only do certain types of files not including the one I am trying. I checked the first 2 bytes but doesn't look like they are 0x4D 0x5A.

Tim Walls October 28, 2013 at 10:39 PM

Ahh.... Got IDA finally trying to load the file by removed the bytes and changing the IDA config for ROM files.
But now when trying to load says use the 64Bit IDA for AMD64 files.
From my research I can't find a 64Bit Version.

If anyone is interested in modding for me the PC is an Acer TravelMate 8481G.
ROM can be found @ http://global-download.acer.com/GDFiles/BIOS/BIOS/BIOS_Acer_1.16_A_A.zip?acerid=634913096206824380&Step1=NOTEBOOK&Step2=TRAVELMATE&Step3=TRAVELMATE%208481G&OS=ALL&LC=en&BC=ACER&SC=AAP_10

Looking to enable Power menu and Advanced menu.

donovan6000 October 28, 2013 at 10:53 PM

Being able to disassemble the module is the most crucial step of this tutorial. Without this you can find the code in the module to modify to unlock the tabs. EFI IFR Dumper is only to assist you in finding the offsets of the form sets in the module's code. It is not an alternative to IDA Pro.

You can use any disassembler you want as long as it is capable of disassembling the format of the efi modules. My hackintosh native power management tutorial used objdump instead of IDA Pro, so check that out if your curious. I only used IDA Pro in most of these tutorials because it is the most visually advanced disassembler available. These tutorials would be much more difficult to understand if I didn't have IDA Pro's flowchart view to help support what I write.

The demo version of IDA Pro can't disassembler 64-bit binaries, so you won't be able to use it with your modules. I know the first two bytes aren't 0x4D 0x5A. The latest versions of Andy's tool changed the format of the files in the DUMP folder to give the some extra information in their header. You have to remove the first few bytes of the module you want to disassemble until the first two are 0x4D 0x5A. Then after your done editing the module, make sure you add those removed bytes back so that your bios can be repacked correctly. I made a program to assist in this procedure, but it's only for Linux. If you happen to know any windows GUI programming and would like to help, then that'd be awesome. I've asked over 20 people this and still haven't gotten any help lol.

Reply

Tim Walls October 30, 2013 at 4:47 AM

Hi Donovan, Thanks for the info. I will definately give another disassembler ago maybe objdump.
I went back through your posts and realised I read them wrong and confirmed what you have said about removing until the 2 bytes.
I have a little knowledge in VB.NET if that helps, I am assuming you just need something to open the file and remove everything up until those bytes, store it in a temp file. And then add it back when needed.

Reply

Jesse Anderson October 30, 2013 at 9:35 PM

Donovan,

This stuff is great. I've been doing development for quite some time, but I've never played at the assembly level. It's been fun reading through your tutorial and flipping through hex codes.

I have an HP dv7t-6c23cl with this lil bugger right here: http://ftp.hp.com/pub/softpaq/sp60501-61000/sp60717.exe

I was not able to find an area of the BIOS that referenced all of the tabs and had some form of jumps (JZ, JNZ, etc). I did see an area that looked a little more like Robert Candeletti's image you posted above. So maybe I will go and try manipulating that a bit. I assume you can just change the jump bytes the same way.

I also found a sub that referenced all of the tabs, but it was very linear code. It ran a different sub routine before each reference to a tab. I thought maybe that sub was somehow deciding if the tab should be shown or not so I poked around with that idea a bit.

I was able to successfully change the iscflash.dll to allow me to flash the update BIOS. I had to disarm two error messages one about the BIOS image being wrong and another about the BIOS not being a newer version. Once I got into DOS however, the UEFI environment told me the BIOS was corrupt. So it was either corrupt because my hunch was noobed, or I am also worried about something else you said (that I have seen in other forums as well) that the RSA encryption is impossible without the private key.

How would I go about finding out if it's even possible due to encryption, and if it is, am I on the right track so far? Andy's tool does produce an RSA.SIG. Does that spell doom?

Reply

▼ Replies

donovan6000 October 31, 2013 at 8:24 PM

Glad you like my blog. Also congratulations on getting this far. A lot of people that visit this site with the intention to mod their bios give up almost immediately when the realize what it takes to reverse engineer software. It's good to see someone else as interesting it in as I am :)

As I mention in this tutorial, no two bios revisions hide the tabs in the exact same way. There are several different ways that the compiler chooses to hide them, so don't assume that yours are hidden the same way that I describe in my tutorial. The function in Robert's screenshot is actual in every insyde bios I've ever disassembled. It's used for parsing through the form sets to start initializing them, so it's sometime common for the compiler to utilize the code there to hide some of the tabs.

Unfortunately your bios probably do implement a signature verification check on startup based on it telling you that the bios are corrupt. HP original used RSA signature verification only in the flasher utility, and this is the case for my bios. This is why modding iscflash.dll is necessary. However around sp60xxx the started incorporating the same check when the computer starts up. This has managed to prevent these kind of bios from being modded from about 2 years. Modding your bios will become a little bit harder since you'll have to locate and prevent the check(s) from occurring. No one has done this yet, so it could be challenging. I really hope you don't give up though. If you manage to develop a method to successfully mod, then it will make a lot of people very happy.

Jesse Anderson November 1, 2013 at 2:22 PM

I have some spare time this weekend. I am nowhere near as nimble as you are in this code, but I'll poke around a bit. Even a blind chicken gets a kernel of corn now and then.

Jesse Anderson November 11, 2013 at 1:50 PM

Donovan,

When you recover your bricked HP you use a USB drive with a volume labeled HP_TOOLS. This process works great, but I noticed you use a BIOS and RSA.SIG file produced by Andy's tool. Is there perhaps a way to exploit that to encrypt the modified BIOS with the public key and place it in the 'Current' folder?

donovan6000 November 11, 2013 at 2:17 PM

You'd have to know HP's private RSA key to encrypt the modded rom so that the recovery utility will flash it. You could always modify the recover utility to flash any rom to bypass this. However to launch a modded flash utility, you'd also have to modify CryptRSA.efi to launch files with invalid signatures. Unfortunately the bios wont launched a modded CryptRSA.efi unless the SHA-1 hash in the bios is updated to match the modded CryptRSA.efi's. So in the end, you have to be able to mod you bios to be able to launch a modded recovery utility that can flash modded roms.

Anyway, the RSA signature verification check happens on startup. So even if you were to flash a modded rom with the recovery method, it would still fail the signature check and result in a brick.

Jesse Anderson November 23, 2013 at 4:12 PM

So I thought I would downgrade my BIOS in hopes that a pre-sp60xxx BIOS wouldn't do the startup check - and hey, why not I already mod'd the installer to allow downgrades :D

I poked around in HpBiosUpdate.efi from the recovery util. I can see where it loads the signature file and writes the bios file. I'm tempted to short circuit the two. I am worried though that the memory locations won't be right when I do (i.e. what I think is the BIOS image is in the right spot address in memory).

Besides that, you mentioned something interesting about CryptRSA.efi. Is there also something in there to be worried about? Or do you think what I have found in HpBiosUpdate.efi has a chance of doing the trick?

Maybe I'm being a little too stubborn with this. ;-)

donovan6000 November 24, 2013 at 10:56 AM

First of all, the signature check happens on startup. Flashing your bios through different methods isn't going to remove this check. It'll happen as soon as your computer restarts after the flash because the code to preform the check is still in the bios. The bios rom contains a sha1 sum of the unmodified bios image and an RSA encrypted version of that same sha1 hash. These are what the startup check uses to verify the integrity of the bios.

The bios rom is encrypted when we get it from HP because InsydeFlash.exe decrypts is to verify it. So when it's done verifying it, then rom is now unencrypted and it flashes it. So the rom current stored in the bios chip is never encrypted.

You'd also have to modify CryptRSA.efi to not preform a signature check on HPBiosUpdate.efi so it'll load it even if it's modified. However to have the bios load a modified CryptRSA.efi, you'd have to update the sha1 hash for it in the bios rom.

Reply

Jia Wei Koh November 1, 2013 at 12:02 PM

Hi would love if you can help with my bios mod.. please do help me with this :)) I am looking for CPU/GPU Clock and volts , temperature , on board gpu enabling... and ram clock :)

https://www.dropbox.com/s/yquv1jkeh8t57gk/BIOS_WIN_V650.exe

Reply

▼ Replies

donovan6000 November 1, 2013 at 3:33 PM

Unless your willing to donate, then I;m not going to do any of the work for you. One of the goals of this blog is to teach people how to mod their own bos by giving them a reference on how it's done. You wont learn anything If you don't do it yourself

Jia Wei Koh November 3, 2013 at 8:27 PM

how much would i have to donate?

donovan6000 November 4, 2013 at 10:11 AM

What's your computer's model?

Also, almost every bios I've worked with doesn't contain settings to adjust CPU/GPU clocks and voltages or RAM clock. So even after your bios are modded, you'll most likely not have access to these.

Reply

T mac November 2, 2013 at 2:58 PM

Hi,

Could you have a look at my bios? Spent days trying to modify j-bios scripts as mine seems to be totally different to other InsydeH20 bios's out there! Happy to donate if you can help me out at all.

https://dl.dropboxusercontent.com/u/9950356/isflash.bin

Reply

Replies

donovan6000 November 2, 2013 at 10:50 PM

What's the model of your computer? Please provide an official link to its support page.

T mac November 3, 2013 at 2:38 AM

I cant link directly (site is full of javascript links) but its the W700 - http://www.acer.co.uk/ac/en/GB/content/drivers

donovan6000 November 3, 2013 at 12:16 PM

The Acer v2.xx bios haven't been modded yet because they'll produce an error on startup if the bios's code is changed. So for me to mod your bios, it'll probably take 10+ hours to discover a way to byass this issue. That's approximately a $130 donation. I'll mod your bios if your willing to do this, but I'd recommend you put that money toward buying a different laptop.

T mac November 3, 2013 at 1:05 PM

Ok, I really just wanted to disable the long duration power limit that Acer enforced (10 watts after ~20 seconds). I've just read through the EFI shell thread over at bios-mods and it looks like I should be able to modify the setting through the shell. If I can't get it to work I might come back and throw that $130 your way!

T mac November 10, 2013 at 6:07 AM

donovan6000, I don't suppose you know what the problem here might be.
So I've managed to change the bios settings using a custom grub shell and setup_var, I've literally changed every single setting that I think might effect throttling but my device still throttles to 10w after 28 seconds. It seems that although the setting changes are showing on tools (like intel extreme tuning) something else is overriding them. Do you think it is possible Acer have code elsewhere in the firmware that controls this throttle and is not accessible through the bios?

Reply

Robert Hinojales November 3, 2013 at 4:04 AM

can you unlock my bios advance settings
my laptop is Toshiba Satellite L745-S4110
Bios : Insyde
Bios Rev. 3.5
Bios version 2.60

Reply

Replies

donovan6000 November 3, 2013 at 12:10 PM

Unless your willing to donate, then I'm not going to do the work for you. One of the goals of this blog is to get more people involved by giving the some references that will help them along the way. I'm sure you'll be able to do it yourself if you just put in the time and effort required. Good luck!

Reply

Anonymous November 12, 2013 at 7:13 PM

sir,
Please unlock my bios for "Advanced Tab"
Model- HP Pavilion g6-1330se
BIOS url- http://h10025.www1.hp.com/ewfrf/wc/softwareCategory?os=4063&lc=en&cc=us&dlc=en&sw_lang=&product=5218311#N1582

Reply

Replies

donovan6000 November 12, 2013 at 7:29 PM

Unless your willing to donate, then I'm not going to do the work for you. One of the goals of this blog is to get more people involved by giving the some references that will help them along the way. I'm sure you'll be able to do it yourself if you just put in the time

and effort required. Good luck!

Reply

Anonymous November 19, 2013 at 12:27 AM

you said donate how much though to mod my bios its a hp g7 2275dx

Reply

Replies

donovan6000 November 19, 2013 at 7:22 AM

Donating should be a last resort option after you've spent months attempting to mod your bios without success. This blog is meant to educate, and you wont learn anything if your don't do anything yourself.

Reply

Fastmix November 19, 2013 at 2:13 PM

Hi Donovan,

Would you kindly mod this bios?

http://ftp.hp.com/pub/softpaq/sp50501-51000/sp50586.exe

Thanks

Reply

Replies

donovan6000 November 19, 2013 at 4:24 PM

Unless your willing to donate, then I'm not going to do the work for you. One of the goals of this blog is to get more people involved by giving the some references that will help them along the way. I'm sure you'll be able to do it yourself if you just put in the time and effort required. Good luck!

Reply

Anonymous November 19, 2013 at 6:33 PM

ok and that would be great if i didnt work 14 hours 6 days a week i dont really have the time. thank you anyway.

Reply

Anonymous November 19, 2013 at 6:36 PM

and besides andy tool told me i didnt have a insyde bios image eventhough i clearly downloaded it from hp and extracted it.

Reply

Fastmix November 20, 2013 at 11:25 AM

When I get to the IDA part what I see is different and confusing not really what you are showing, I think that is very difficult to follow....

Reply

Replies

donovan6000 November 20, 2013 at 6:20 PM

That's because your bios doesn't contain the exact same code as mine, so it should look different. Reverse engineering software isn't supposed to be easy. Don't assume that this is a generic guide that's a simple solution to unlock the tabs in all bios, because nothing like that will ever exist.

Reply

Anonymous November 20, 2013 at 3:40 PM

Hello. First, thanks for this tutorial. I searched through the web and this guide seemed like the only possibility to unlock hidden features in my bios. I have exactly the notebook provided in the link below. In your tutorial, you are unlocking hidden tabs in the bios, this notebook already has an advanced tab, but there are only two options to choose. What for do i have to search in IDA Pro, because i find some tabs but the things i want to unlock would be more like sub menus or something. How do i identify these?

http://www.sony.co.uk/support/en/product/SVT1313S1ES

Reply

Replies

donovan6000 November 20, 2013 at 6:23 PM

If your bios uses EFI's internal forms representation protocol then you can use my EFI IFR Dumper to extract the options into a human readable format. They can then be modified to make them visible in the tabs. I wrote a tutorial on it here:

http://donovan6000.blogspot.com/2013/07/insyde-bios-modding-hidden-settings.html

Anonymous November 21, 2013 at 8:25 AM

I tried to get your IFR Dumper to work with my Setup Utility (http://www.mediafire.com/download/b282s1g16btu6k5/FE3542FE-C1D3-4EF8-657C-8048606FF670_0_241.ROM)

It's really hard. I just want to know the pointers for the option to enable one of my SATA ports. Could you help?

donovan6000 November 21, 2013 at 10:52 AM

Your bios probably uses UEFI's IFR protocol instead of EFI's IFR protocol. As I said before, my EFI IFR Dumper only works on EFI's internal forms representation.

Also unless your willing to donate, then I'm not going to do any of the work for you. One of the goals of this blog is to get more people involved by giving the some references that will help them along the way. I'm sure you'll be able to do it yourself if you just put in the time and effort required. Good luck!

Reply

Anonymous November 21, 2013 at 1:04 PM

Thanks for the reply, the second post is not from me, i will follow the link you gave me and try to do it myself.
greetings vivian

Reply

mahesh eranga December 1, 2013 at 8:03 PM

how to mod hp 630 insyde h2O f.37 bios plz help me

Reply

▼ Replies

donovan6000 December 3, 2013 at 6:44 PM

Unless your willing to donate, then I'm not going to do any work for you. I made this blog to assist people in modding their own bios. I'm sure you'll be able to succeed if your juts put in the time and effort. Good luck!

Reply

Anonymous December 8, 2013 at 6:53 AM

please inform me that my bios is rsa signed or not
BIOS url- http://h10025.www1.hp.com/ewfrf/wc/softwareCategory?os=4063&lc=en&cc=us&dlc=en&sw_lang=&product=5218311#N1582

Reply

▼ Replies

donovan6000 December 9, 2013 at 3:07 PM

Unless your willing to donate, then I'm not going to do any of the work for you. This includes things like determining if your bios is RSA signed or not.

Reply

Anonymous December 10, 2013 at 6:07 AM

Hi, I've just read whole comments under this post and I don't know how to downgrade currently installed BIOS 2.14 to 2.04. I need one option which disappear on 2.14 and above DISABLE NVIDIA GRAPHIC CARD. I found this http://catchtito.blogspot.com/2013/05/how-to-update-to-2x-bios-from-1x-bios.html but my modified platform.ini is overwritten by InsydeFlash.exe. Could you give me some advice?

Reply

▼ Replies

Anonymous December 10, 2013 at 7:15 AM

This is the unofficial cracked version of InsydeFlash3.78.00, You can try this one to flash old bios version !
http://rapidgator.net/file/8853ed2dc164ef7d893457a8ede7557c/InsydeFlash3.78.00.rar.html
With regards . . .

Anonymous December 10, 2013 at 12:38 PM

Thanks for link but I have problem I can't downgrade BIOS there is info: this ec file is larger than rom part

Anonymous December 11, 2013 at 2:51 AM

I can't use this cracked version I've try everything. Maybe there is another way to downgrade from v2.14 to lower one?

Reply

BDMaster December 10, 2013 at 7:23 AM

I would You help me to unlock all features in bios for Acer Aspire 8930G and Acer Aspire 8951G to get complete owner to install Mac OSX Lion into (I hope unlocking bios it will be possible).
I found some things for 8930G, but few for 8951G, It's possible ? and I will donate $.50,00 for your help !
Let me know, so I will give the money by Paypal.

Reply

Replies

donovan6000 December 10, 2013 at 3:28 PM

Here's the v1.13 bios for the Acer 8951G. I unlocked the advanced and Power tabs.

http://www.mediafire.com/download/njn22zgaipl4qgq/Acer+1.13.zip

And here's the v1.20 bios for the Acer 8930G. I was only able to unlock the Advanced tab for this one. It wasn't blacklisting the Power tab in a usual way and I didn't want to brick your computer by trying something untested to unlock it. Hope you don't mind.

http://www.mediafire.com/download/77jb5n5euj9djco/Acer+1.20.zip

Just run InsydeFlash.exe to flash the modded bios roms.

BDMaster December 11, 2013 at 5:29 AM

I have got these ones above and have done some checks in binary mode, in past I tried to study about Insyde bios and I know that it's difficult for me ! But with your help may be I can understand much more !
I send your donation as I wrote You, so if do You want help me to understand Insyde bios I will be gratefull to You.
With regards.

http://www.bios-mods.com/forum/Thread-UNLOCKED-ACER-6935G
http://www.bios-mods.com/forum/Thread-UNLOCKED-Acer-5951G-6879
http://rapidgator.net/file/037313aa925163cca792a55c3fbcb94f/Acer_Aspire_8930G_VT_Slic21_7Menu_EIST.rar.html

BDMaster December 11, 2013 at 5:53 AM

PayPal Donation
Dettagli donazione
Numero di conferma:
74X965238T174700W
Importo donazione:
$50,00 USD
Totale:
$50,00 USD
Scopo:
Thanks
BDMaster

I have done as right ! If do You want write to me and let me know if You want help me to understand Insyde bios, cause I have tried as your examples, but I didn't find what you wrote in. (st r uct EFI _HI I _DATABASE_HEADER
{
ui nt 32_t Of f set ;
st r i ng I dent i f i er ;
ui nt 32_t St ar t St r i ngPackages;
ui nt 32_t St ar t For mSet s;
} ; $SBV + 80 EB 07 80 91 F5)
I looked in your efi-ifr-dumper text flle and found the offset (i looked in Hex manually) and followong your examole reversing I have to found my offset strings and forms in a row of extracted moule FE3542FE-C1D3-4EF8-657C-8048606FF670_0_163.ROM
DUMMY $ + 0xC674 Exit (0x2A0) first form , 0x10B94 eng first strings
Nothing !!!! why ???

BDMaster December 11, 2013 at 12:06 PM

Many Thans for your availability and courtesy in advance.

Reply

CHRISTIAN MINA CEVALLOS December 11, 2013 at 12:19 PM

Hi Donovan can you unlock the advanced and power tabs

Hp Envy m4-1015dx

Official Bios
http://ftp.hp.com/pub/softpaq/sp60001-60500/sp60462.exe

How much for the job...??? Thanks

Reply

Replies

CHRISTIAN MINA CEVALLOS December 11, 2013 at 12:22 PM

I will Donate you $40

donovan6000 December 11, 2013 at 2:02 PM

Based on how new your computer is, your bios probably incorporates HP's startup signature check which prevents the boot process from continuing if the bios has been modified. Since HP's private RSA key hasn't been leaked, we can't resign the bios to reflect any modifications, so any modifications will result in the rom failing the signature check. So your bios are probably unmoddable at the moment. Sorry for the disappointing news.

Reply

BDMaster December 11, 2013 at 2:29 PM

Hi Donovan, I would ask you if you can do the same work as 1.20 you gave me, on acer aspire 8930g 1.21 version.
I link to a VT and Slic version I had found on Marcan Blog time ago. An if it 'is possible give to me some explanations on it.
Many thanks.

http://rapidgator.net/file/858579189b2dd3411da61abb011ae9f6/Acer_Aspire_8930G_VT_Slic21.Marcan_Blog.rar.html

With regards

Reply

▼ Replies

donovan6000 December 11, 2013 at 3:20 PM

Thanks for the donation :)

So for v1.03 and v1.20, the tabs I unlocked were being blocked by a formset blacklist so that they would never be initialize. This is done by comparing the string ID for the form's name to a set of IDs that it doesn't allow. It's similar to this picture which I made for a different bios a few months ago: http://oi44.tinypic.com/xfn953.jpg

The EFI IFR Dumper doesn't search for the EFI IFR Database Header anymore to find out the starting offsets of the string packages and formsets. I realized that not all bios would contain this identifier, so I search directly for the op-codes that indicate the start of these components. I don't remember exactly what values it searches for, but the C++ code included with that software explains it very well.

The latest bios released for the 8930G is v1.20. You can see this on Acer's support website: http://us.acer.com/ac/en/US/content/drivers

Using bios versions that aren't directly released and supported by Acer can be dangerous and have unexpected results. I highly recommend you stick with V1.20. If you really want to use v1.21 then I can mod it. There's no place to directly download v1.21 from Acer, so I would have to mod Marcan's already modded version to accomplish this.

BDMaster December 11, 2013 at 3:28 PM

Bios 1.21

1) Bios 1.21 VT SLIC File: 1.21-clean_SLIC.fd
2) Bios 1.21 VT SLIC EIST File: KM2000FR.121-Acer-8930g-VTx-SLIC-EIST.fd

Module EIST

ORG: F7731B4C-58A2-4DF4-8980-5645D39ECE58_0_169.ROM Hex E8 - E8
MOD: F7731B4C-58A2-4DF4-8980-5645D39ECE58_0_169.ROM Hex F0 - F0

To add menu EIST needs filling as above:

Type Src Off Count Original Tag Off Count Modded
Replaced 293F 1 byte 0xE8 293F 1 byte 0xF0
Replaced 3D1B 1 byte 0xE8 3D1B 1 byte 0xF0

Bios 1.20

1) Bios 1.20 AA File: KM2X64.fd (BIOS_Acer_1.20_A_A)
2) Bios 1.20 AA MENU Unlock File: KM2X64.fd (Acer_6935G_Unlocked)

Module AA MENU Unlock

ORG: FE3542FE-C1D3-4EF8-657C-8048606FF670_0_163.ROM Hex 53
MOD: FE3542FE-C1D3-4EF8-657C-8048606FF670_0_163.ROM Hex FF

To add MENU Unlocked needs filling as above:

Type Src Off Count Original Tag Off Count Modded
Replaced 0611 1 byte 0x53 293F 1 byte 0xFF

These are my comparation for the files differences in Rom modules.
I saw differences between these ones and yours you used opcode (token) 90 only . . .
May be You explain to me much more, please . . .

donovan6000 December 11, 2013 at 10:22 PM

There are infinitely many ways to modify software to accomplish the exact same result. I use the 0x90 (no operation op-code) because it's my preferred way to cancelling out conditional jumps. After comparing the current form set's string ID to the blacklisted 0x53 value, it preforms a jump if zero command (jz). I cancel out this conditional jump by replacing it with no operations so it preforms nothing after comparing the values.

The string ID for your Advanced tab's name is 0x53. This is why he changed 0x53 to 0xFF. He assumed that none of your other form sets have the ID of 0xFF, so the blacklist wont have to reject any of them. Thus allowing the Advanced tab to be displayed.

For the EIST unlocking, he's changing the locked register from 0xE8 to 0xF0. The MSR register 0xE8 contains the bit that signifies if ESIT is locked or not. So by changing the register that has this lock bit set, the EIST remains adjustable.

BDMaster December 12, 2013 at 4:54 AM

Kizwan Guide to unlock EIST on Phoenix Bios :

Let me explain how to modify the First “bit 20 lock”:
- Replaced opcode bts (bit test & set) with btr (bit test & reset)
- Change this:
- 000028F0 480FBAE814 bts rax,0x14
- To this:
- 000028F0 480FBAF014 btr rax,0x14
- Remember, the file we will need to edit/modify is the one with the .ROM extensions
- For the First “bit 20 lock”, we will need to change the hexadecimal value at offset 000028F3 with 0xF0.
- Locate the offsets in F7731B4C-58A2-4DF4-8980-5645D39ECE58_3_606.ROM file, and substitute byte.

- Repeat the same procedure on the Second “bit 20 lock”. Change the hexadecimal values
- at offset 00003CD7 with 0xF0.

Modulo EIST for Acer Aspire 8930G :

ORG - F7731B4C-58A2-4DF4-8980-5645D39ECE58_0_169.ROM Hex E8 - E8
MOD - F7731B4C-58A2-4DF4-8980-5645D39ECE58_0_169.ROM Hex F0 - F0

Replaced 0000293F 0xE8 with 0xF0
Replaced 00003D1B 0xE8 with 0xF0

Kizwan :

Replaced 00028F0 0xE8 with 0xF0
Replaced 00003CD7 0xE8 with 0xF0

Set instructions
480FBAE814
480FBAF014

Are equals !

480FBAE814
480FBAF014

I think bts rax,0x14 change in btr rax,0x14 he changed opcode from BTS to BTR Bit set to Bit Reset !

Let me know . . . .
With regards

donovan6000 December 12, 2013 at 9:30 AM

Are you disassembling to code at all or just looking at the bytes that differ between the modules? It's going to be difficult for you to understand anything if your not disassembling the code.

Yes, he's setting the instruction to btr. My previous assumption in my last comment about the ESIT lock bit being located in the 0xE8 MSR register was incorrect.

Add comment

Load more...

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)