

How to SLIC the VMware EFI

This guide steps through the process of adding a SLIC to the VMware EFI.

Needed: VMware EFI, three OEM SLP related modules (included with kit), appropriate SLIC.BINs, UEFITool 0.28.0 (included with kit), Hex Editor (WinHex in this guide – not included). The EFI should match the VMware version.

Note: The NE versions of UEFITool do not allow editing of firmware images, but version 0.28.0 does.

Adding a SLIC to a VMware EFI requires the addition of three OEM SLP related modules to the EFI. These modules are not native to the VMware EFI, but can be added. The included FFS module sets consist of:

4C494E55-5849-5342-4554-544552212121.ffs	SlpSupport	
996AA1E0-1E8C-4F36-B519-A170A206FC14.ffs	SLIC PubKey	c/w DELL PubKey
69009842-63F2-43DB-964B-EFAD1C39EC85.ffs	SLIC Marker	c/w DELL Marker (2.3/2.4/2.5/2.6/2.7 SLIC)

All the following steps apply to both EFI32/EFI64.

[Step 1 – Locate the OEM ID, Public Key, and Marker] All the data necessary for modding the EFI is in the SLIC.BIN. In this case we have the DELL[PE_SC3]2.4-2B4E6B10.BIN. We are interested in three sections. All SLIC.BINs are laid out this way. From top to bottom:

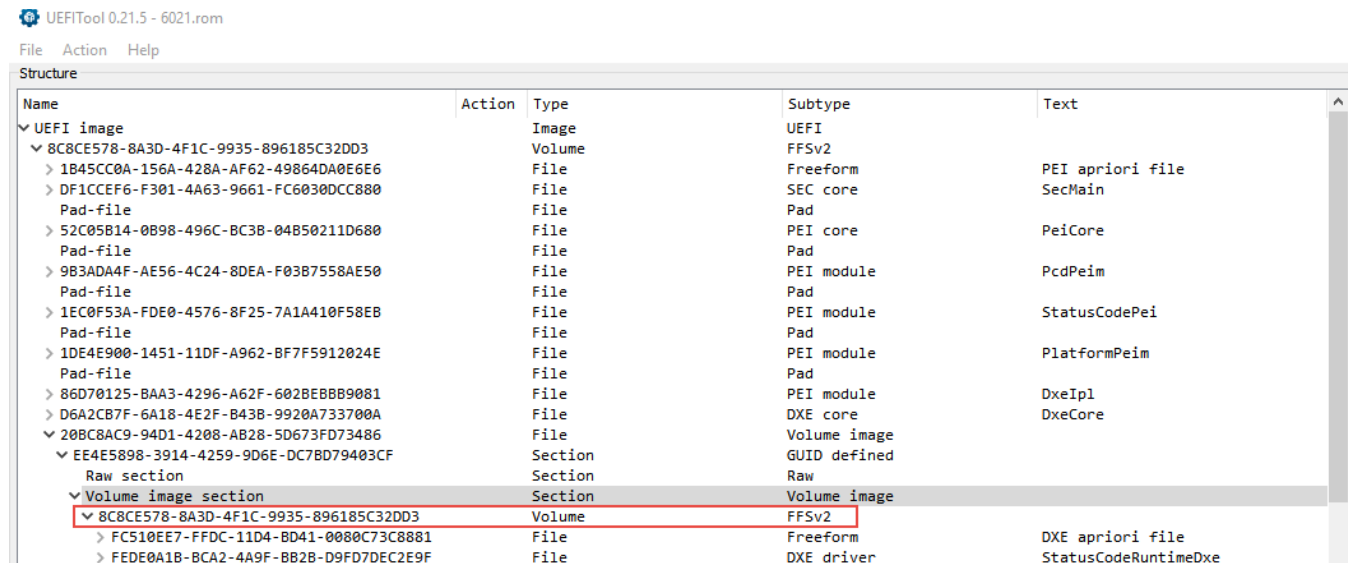
WinHex - [DELL[PE_SC3]2.4-2B4E6B10.BIN]																
File Edit Search Navigation View Tools Specialist Options Window Help																
DELL[PE_SC3]2.4-2B4E6B10...																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	53	4C	49	43	76	01	00	00	01	A6	44	45	4C	4C	20	20
00000010	50	45	5F	53	43	33	20	20	01	00	00	00	4D	53	46	54
00000020	01	00	00	00	00	00	00	00	9C	00	00	00	06	02	00	00
00000030	00	24	00	00	52	53	41	31	00	04	00	00	01	00	01	00
00000040	7F	F6	C1	05	BE	5C	57	63	A5	8A	68	F3	6E	8F	06	FA
00000050	AF	B4	9F	68	82	23	EC	50	40	5A	73	7F	EC	E4	07	CB
00000060	DC	25	1A	9C	E3	E3	66	11	E0	A5	98	06	C5	80	0A	FA
00000070	42	93	86	98	E7	D5	1B	D4	D7	3A	A4	0B	EE	E2	7D	BE
00000080	5F	5B	15	0C	AB	D0	21	DE	BF	E9	B5	6E	A4	57	B9	8C
00000090	0C	D2	BA	3A	69	30	76	94	71	A2	64	D7	4C	D8	85	BF
000000A0	DF	A5	6A	C8	DC	45	D5	4D	8C	B8	8C	05	2F	FC	2E	23
000000B0	C4	29	C5	6F	3F	29	6C	6D	57	79	0E	B6	75	ED	21	95
000000C0	01	00	00	00	B6	00	00	00	00	00	02	00	44	45	4C	4C
000000D0	20	20	50	45	5F	53	43	33	20	20	57	49	4E	44	4F	57
000000E0	53	20	04	00	02	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	0C	38	B7	C3	1B	3C	6E	85	C6	6A
00000100	64	A2	08	13	B7	24	93	1B	B8	66	C4	0C	B9	45	33	91
00000110	1C	9E	94	63	B1	1F	7E	52	31	E6	E2	D0	DC	99	DD	B7
00000120	0D	5B	7B	A1	1C	2C	62	EB	65	35	C2	DB	BC	29	39	63
00000130	8E	14	58	CB	63	B4	D7	7F	3A	12	63	7E	CA	FE	B4	03
00000140	B0	CF	49	21	AD	DA	D5	CF	3E	C0	57	6F	2B	A7	55	1F
00000150	01	CB	73	20	6D	19	26	DB	9A	6B	AE	03	1A	9D	C9	8D
00000160	A3	9F	71	49	39	B2	FA	07	3B	01	47	28	43	C5	D8	C2
00000170	4C	8C	AC	7F	BA	F8										

SLICv ;DELL
PE_SC3 MSFT
|æ
\$ RSA1
öÄ %\WcYŠhón ú
~Yh,#iP@Zs iä È
Ü% æääf à¥~ÄE ú
B~tçÖ Ö×:« iä)%
_[«D!Pçéun«W«E
Ö°:i0v~qcd«LØ...ç
B¥jÈÜEÖME,Ç /ü.#
Ä)Äo?)lmWy Qui!•
q - DELL
PE_SC3 WINDOW
S
8-Ä <n...Ej
de -\$" ,fÄ ^E3'
ž~c± ~RlæâDÜ~Y~
[i; ,bëe5ÄÜ*)9c
Ž XËc~× : c~Êp~
°İ!-ÜÖİ>ÄWo+ŞU
Ës m &Üškø É
£YqI9~ú ; G(CÄØÄ
LÇ~ °ø

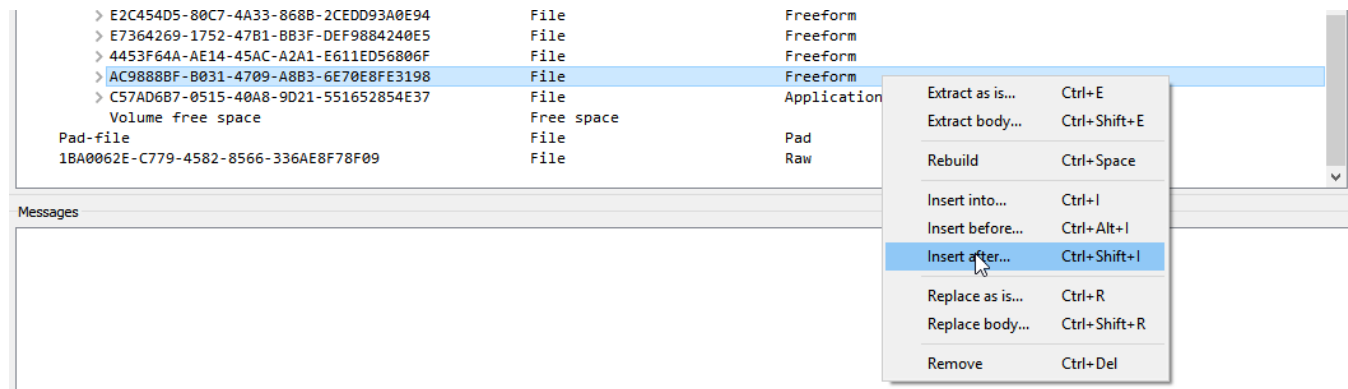
1. OEM ID (OEMID & OEM Table ID)
2. SLIC Public Key (PubKey)
3. SLIC Windows Marker

Important: Get all the data from the same SLIC.BIN.

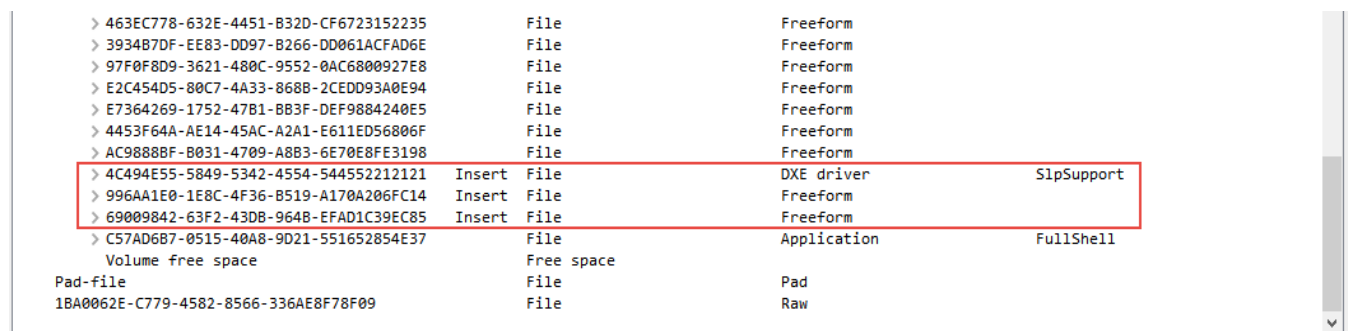
[Step 2 – Insert SLP modules into the EFI] Open the unmodified EFI in UEFITool. Expand 8C8CE578-8A3D-4F1C-9935-896185C32DD3. All OEM SLP operations take place here. We can start with any FFS module set, but in this case, for illustrative purposes, the Dell 2.3 SLIC FFS set is used. **Tip: if you start with the Dell 2.7.ffs set the EFI will be completely modded by completing steps 2 & 3.**



Scroll down to the very bottom. The three modules must be inserted before the final module C57AD6B7-0515-40A8-9D21-551652854E37 (FullShell). You can use *Insert after* AC9888BF-B031-4709-A8B3-6E70E8FE3198. Insert them one after the other.



It will look like this:

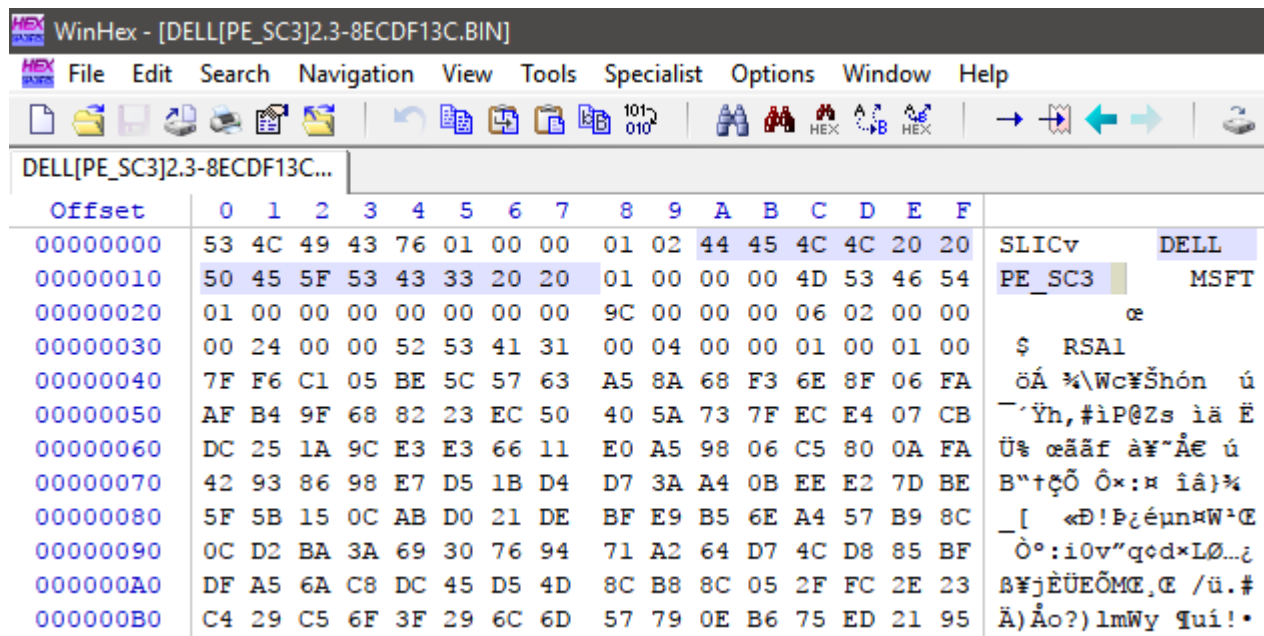


You can *File – Save image file* at this point and UEFITool will process the changes, or you can go to the next step and save/process later.

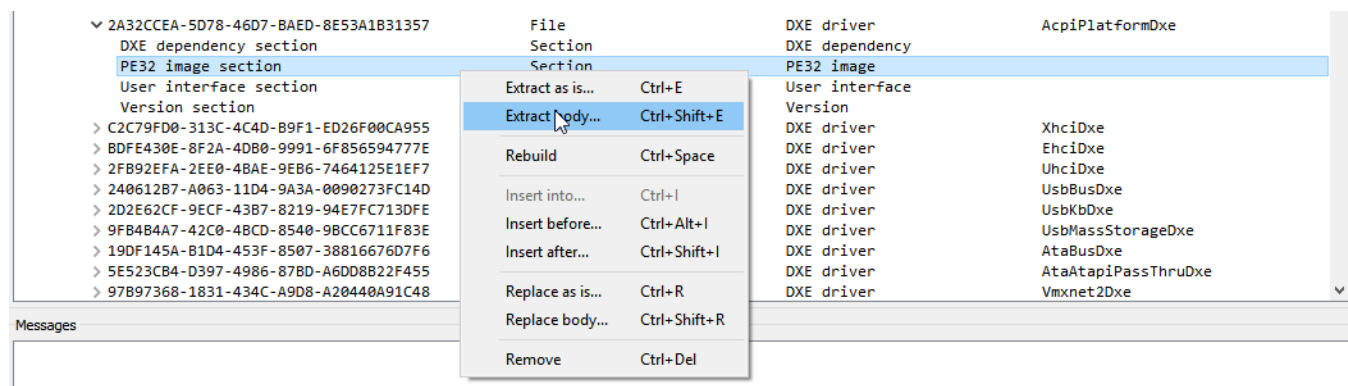
At this point the EFI has the necessary modules for OEM SLP activation. The SLP Marker and Public Key are DELL 2.3. Next, edit the OEM ID from INTEL to DELL.

Next: Edit the OEM ID

[Step 3 - Edit the OEM ID] First, to find the OEM ID open the SLIC.BIN in WinHex. Again, the OEM ID can be found in the SLIC Table starting from offset 10. It's exactly 14 bytes.



Next, In UEFITool edit the OEM ID in 2A32CCEA-5D78-46D7-BAED-8E53A1B31357. Extract the body of the *PE32 image* section.



Open the extracted body in WinHex. Search for 440BX and replace the Intel ID with the Dell ID.

00003720	4E 49 43 2E 20 55 6E 61 62 6C 65 20 74 6F 20 50	NIC. Unable to P
00003730	75 62 6C 69 73 68 20 54 61 62 6C 65 73 3A 20 25	ublish Tables: %
00003740	72 2E 0A 00 00 00 00 00 00 00 00 00 00 00 00	r.
00003750	00 59 4E 59 58 58 58 58 58 00 59 58 58 58 58	YNYXXXXX YXXXXX
00003760	58 58 00 5F 53 31 5F 00 5F 53 34 5F 00 00 00 00	XX _S1_ _S4_
00003770	00 00 00 00 00 00 00 00 49 4E 54 45 4C 20 34 34	INTEL 44
00003780	30 42 58 20 20 20 00 56 4D 57 41 52 45 00 00 00	OBX VMWARE
00003790	79 D3 F0 66 F3 B4 74 40 AC 43 0D 33 18 B7 8C DB	yÓðfó't@-C 3 ·œÛ
000037A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000037B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000037C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

It will look like this.

00003710	41 63 70 69 50 6C 61 74 66 6F 72 6D 3A 20 50 41	AcpiPlatform: PA
00003720	4E 49 43 2E 20 55 6E 61 62 6C 65 20 74 6F 20 50	NIC. Unable to P
00003730	75 62 6C 69 73 68 20 54 61 62 6C 65 73 3A 20 25	ublish Tables: %
00003740	72 2E 0A 00 00 00 00 00 00 00 00 00 00 00 00	r.
00003750	00 59 4E 59 58 58 58 58 58 00 59 58 58 58 58	YNYXXXXX YXXXXX
00003760	58 58 00 5F 53 31 5F 00 5F 53 34 5F 00 00 00 00	XX _S1_ _S4_
00003770	00 00 00 00 00 00 00 00 44 45 4C 4C 20 20 50 45	DELL PE
00003780	5F 53 43 33 20 20 00 56 4D 57 41 52 45 00 00 00	_SC3 VMWARE
00003790	79 D3 F0 66 F3 B4 74 40 AC 43 0D 33 18 B7 8C DB	yÓðfó't@-C 3 ·œÛ
000037A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000037B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000037C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Save and reintegrate with UEFITool using *Replace body*.

UEFITool 0.21.5 - 6021.rtm
File Action Help
Structure

Name	Action	Type	Subtype	Text
> 202A2B0E-9A31-4812-B291-8747DF152439		File	DXE driver	Ps2MouseDxe
> 0ABD8284-6DA3-4616-971A-83A5148067BA		File	DXE driver	IsaFloppyDxe
> B3762FA2-54D6-4EBC-84DE-4CFA9340FCB3		File	DXE driver	AcpiAMLDxe
> F9229745-981C-4E07-9FC6-789545CB8818		File	DXE driver	AcpiSupportDxe
> 327328E6-BD0C-478C-AF05-E9AD5DF922F6		File	Freeform	
▼ 2A32CCEA-5D78-46D7-BAED-8E53A1B31357		File	DXE driver	AcpiPlatformDxe
DXE dependency section		Section	DXE dependency	
PE32 image section		Section	PE32 image	
User interface section		Section		
User section		Section		
> C2C79FD0-313C-4C4D-89F1-ED26F00CA955		File		XhciDxe
> BDFE430E-8F2A-4DB0-9991-6F856594777E		File		EhciDxe
> 2FB92EFA-2EE0-4BAE-9EB6-7464125E1EF7		File		UchiDxe
> 240612B7-A063-11D4-9A3A-0090273FC14D		File		UsbBusDxe
> 2D2E62CF-9ECF-43B7-8219-94E7FC713DFE		File		UsbKbDxe
> 9FB484A7-42C0-48CD-8540-9BCC6711F83E		File		UsbMassStorageDxe
> 19DF145A-B1D4-453F-8507-38816676D7F6		File		AtaBusDxe
> 5E523CB4-D397-4986-87BD-A6D08B22F455		File		AtaAtapiPassThruDxe
> 97B97368-1831-434C-A9D8-A20440A91C48		File		Vmxnet2Dxe
> 982DD8E9-2B79-485F-9AC3-FA67B508C913		File		Vmxnet3Dxe
> 7E983BCE-5C99-4BE0-83D0-210E8FDD03C0		File		VlanceDxe
> 12842ABE-72DA-4B17-A24C-356EC688B915		File		E1000Dxe
> C45FC489-64E6-4EB9-BA3E-50278A9FB5D8		File		E1000EDxe

Extract as is... Ctrl+E
Extract body... Ctrl+Shift+E
Rebuild Ctrl+Space
Insert into... Ctrl+I
Insert before... Ctrl+Alt+I
Insert after... Ctrl+Shift+I
Replace as is... Ctrl+R
Replace body... Ctrl+Shift+R
Remove Ctrl+Del

It will look like this after the operation.

> 202A2B0E-9A31-4812-B291-8747DF152439	File	DXE driver	Ps2MouseDxe
> 0ABD8284-6DA3-4616-971A-83A5148067BA	File	DXE driver	IsaFloppyDxe
> B3762FA2-54D6-4EBC-84DE-4CFA9340FCB3	File	DXE driver	AcpiAMLDxe
> F9229745-981C-4E07-9FC6-789545C88818	File	DXE driver	AcpiSupportDxe
> 327328E6-BD0C-478C-AF05-E9AD5DF922F6	File	Freeform	
▼ 2A32CCEA-5D78-46D7-BAED-8E53A1B31357	Rebuild	File	DXE driver
DXE dependency section		Section	DXE dependency
PE32 image section	Remove	Section	PE32 image
PE32 image section	Replace	Section	PE32 image
User interface section		Section	User interface
Version section		Section	Version
> C2C79FD0-313C-4C4D-B9F1-ED26F00CA955	File	DXE driver	XhciDxe
> BDDE430E-8F2A-4DB0-9991-6F856594777E	File	DXE driver	EhciDxe
> 2FB92EFA-2EE0-4BAE-9EB6-7464125E1EF7	File	DXE driver	UhciDxe
> 240612B7-A063-11D4-9A3A-0090273FC14D	File	DXE driver	UsbBusDxe

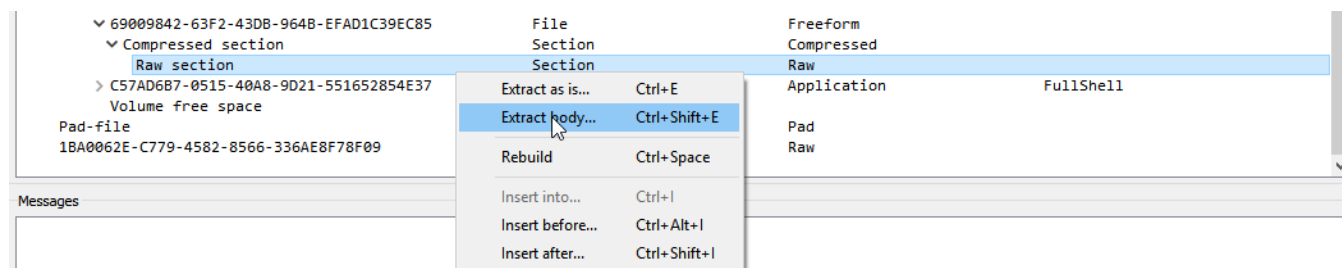
Now *File – Save image file* and save it, for example, as 6021_23SLIC.rom. UEFITool will process the changes and save the file. It's a good idea to re-open the file to check the changes.

That's it. The EFI is fully modded with the DELL 2.3 SLIC.

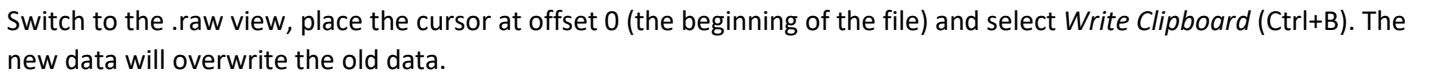
Next: Upgrade to DELL 2.4 (2.5/2.6/2.7) SLIC

[Step 4 – Upgrade to DELL 2.4 (2.5/2.6/2.7) SLIC] It's not difficult to upgrade from DELL 2.3 to DELL 2.4 because the OEM ID and the SLP Pubkey are the same. Just copy the 2.4 DELL SLP Marker into the EFI SLP Marker module.

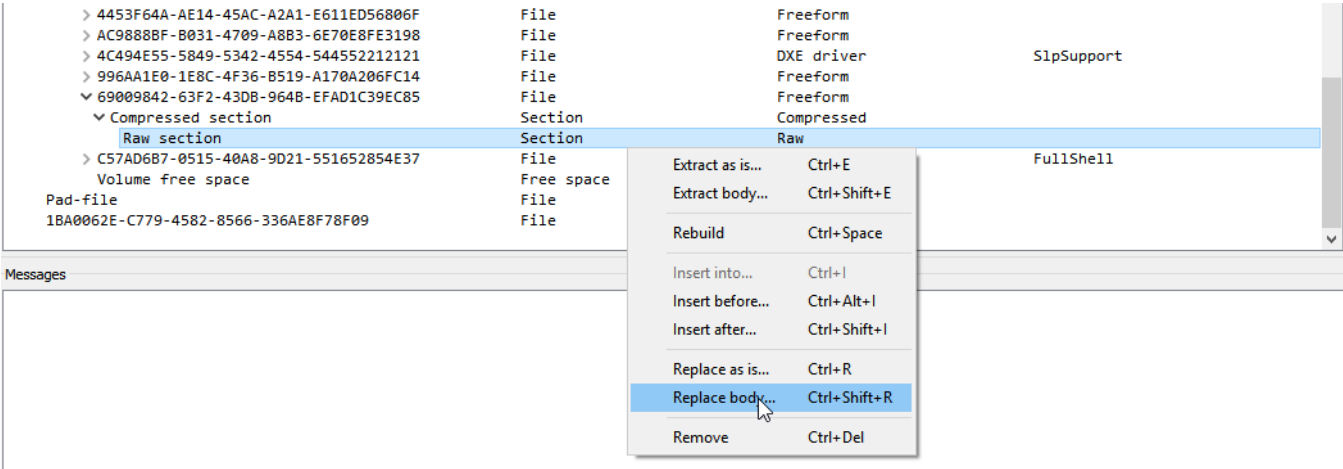
To do this, open the DELL 2.3 EFI in UEFITool and extract the *raw section* of module 69009842-63F2-43DB-964B-EFAD1C39EC85. Save it as a .raw file, for example, as 6900_body.raw.



Open both DELL[PE_SC3]2.4-2B4E6B10.bin/DELL[PE_SC3]2.5-20712DFB.BIN and 6900_body.raw in WinHex. In the SLIC Table the SLP Marker starts with 01 00 00 00 B6 (offset C0) and runs to the bottom of the file and is exactly 182 bytes. Highlight and *Copy Block* (Ctrl+C).



In UEFITool use *Replace body* to integrate the modded 6900_body.raw into 69009842-63F2-43DB-964B-EFAD1C39EC85. You don't need to rename it.



Finally, in UEFITool, select *File – Save image file* and that's it. Give it a name like 6021_24SLIC.rom. UEFITOOL will process the changes. The EFI now has the DELL[PE_SC3]2.4-2B4E6B10 SLIC.

It's a good idea to reopen the EFI to check the changes.

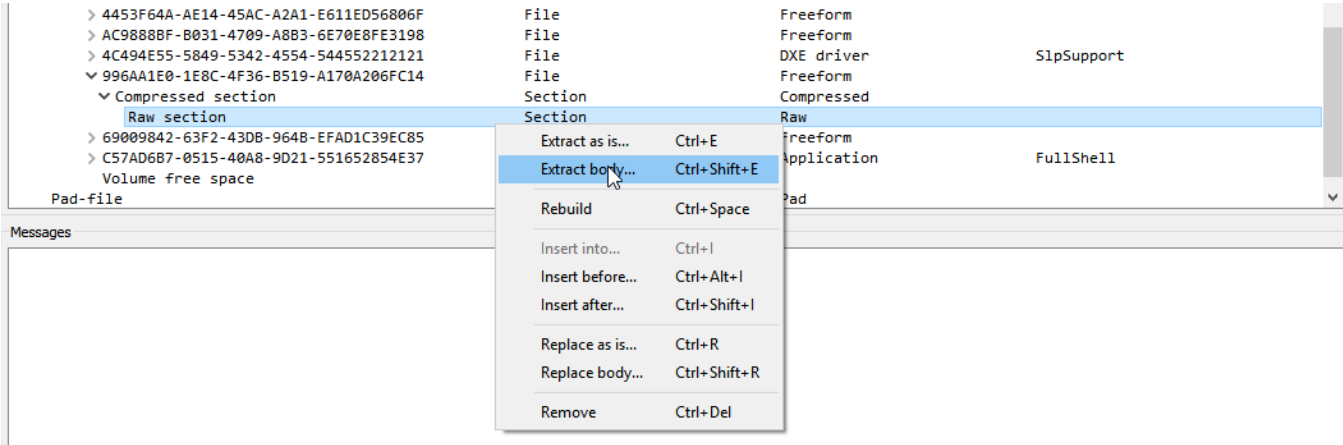
Next: Mod with entirely different SLIC.

[Step 5 – Mod with an entirely different SLIC] Assuming that the EFI has the additional 3 modules, but you want to use a completely different SLIC, for example, Asus 2.1, you will need to change the:

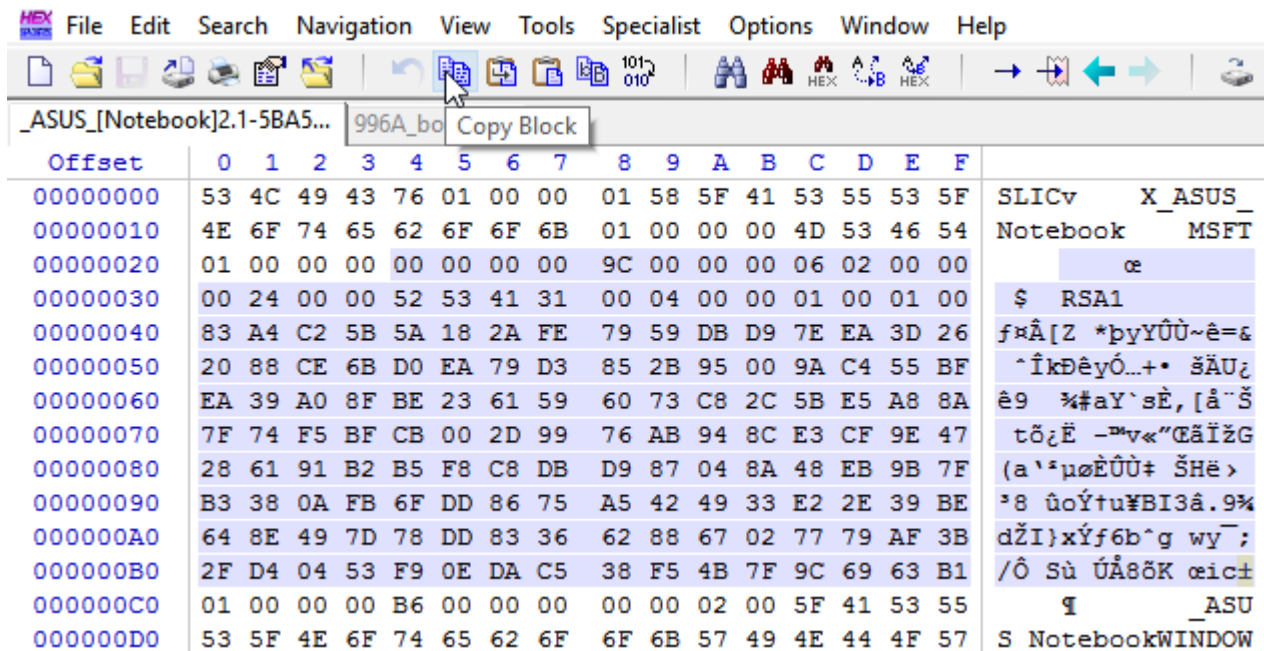
- OEM ID as described in [Step 3]
- SLP Marker as described in [Step 4]
- SLP Pubkey as described below

It's important that the SLP Marker, SLP Pubkey, and OEM ID match. All can be copied from the same SLIC Table. In the EFI the SLP Pubkey is in module 996AA1E0-1E8C-4F36-B519-A170A206FC14. It can be edited using the same steps as described in Section 3.

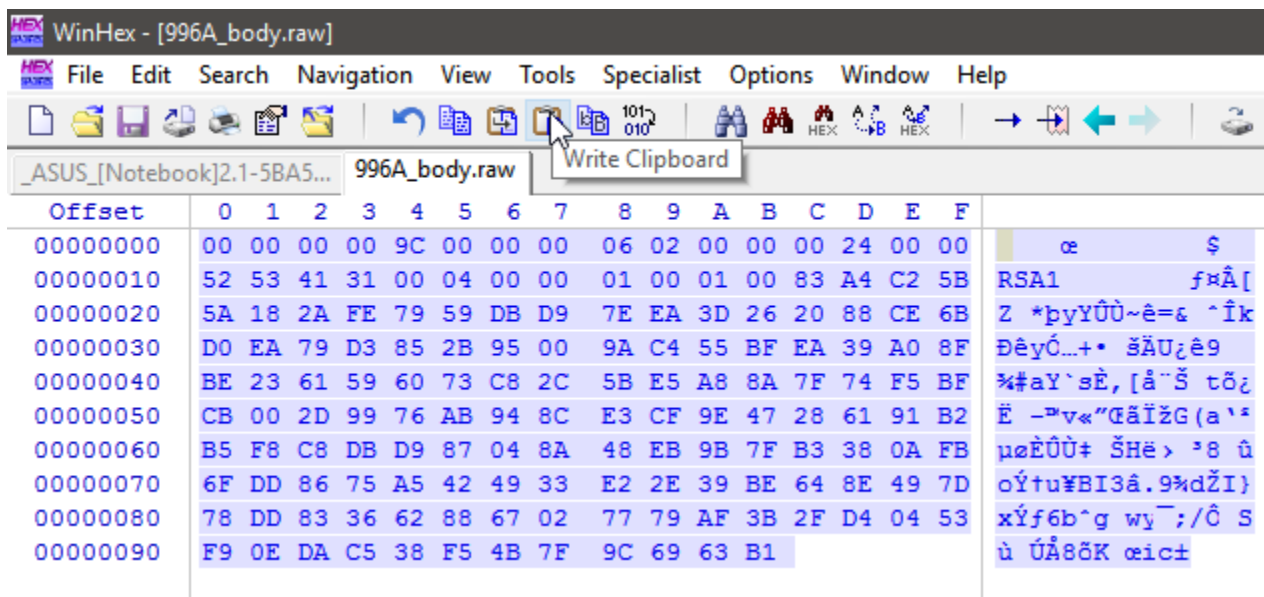
Extract 996A_body.raw from 996AA1E0-1E8C-4F36-B519-A170A206FC14.



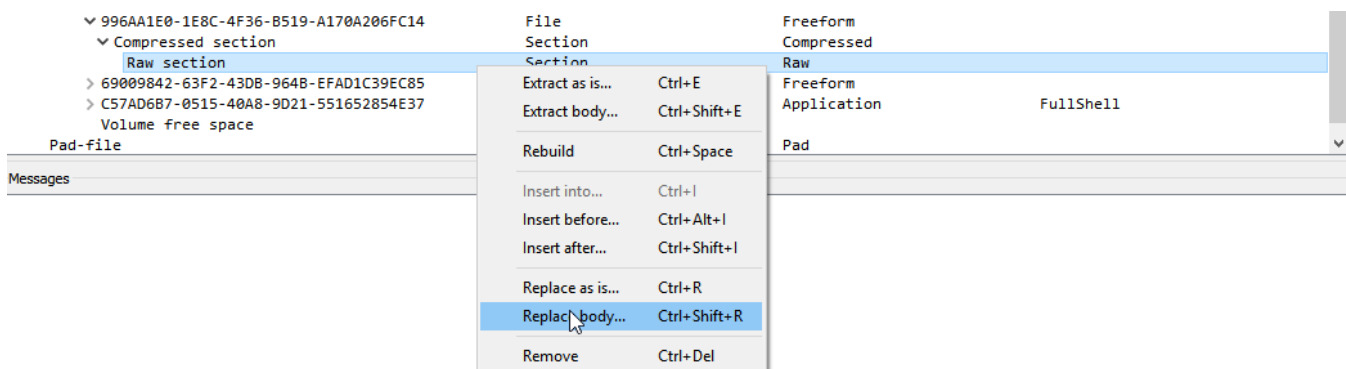
The SLP Pubkey starts with 00 00 00 00 9C (offset 24) in the SLIC table and is exactly 156 bytes. *Copy Block* (Ctrl+C).



Write Clipboard (Ctrl+B) at offset 0.

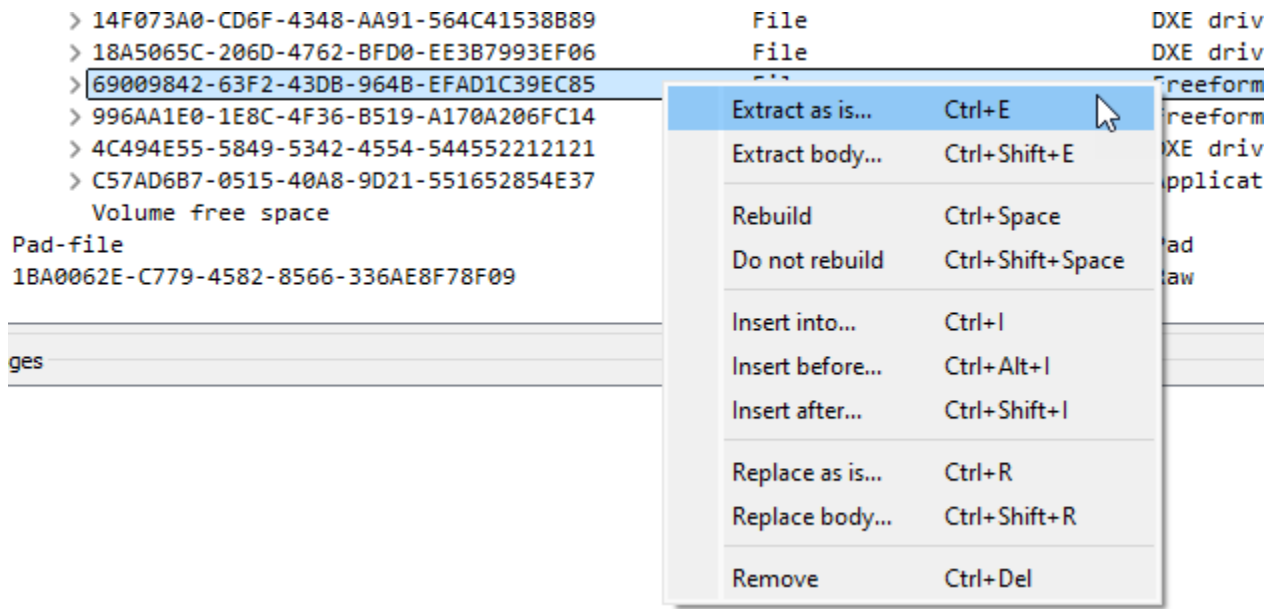


Save and reintegrate into 996AA1E0-1E8C-4F36-B519-A170A206FC14.



Then *File – Save image file*. That's it. The EFI is modded with the _ASUS_[Notebook]2.1-5BA55846 SLIC.

Tip: If you save your modded modules as .ffs files you can easily mod new VMware EFI versions by inserting the three modules and editing the OEM ID. To save, select the module and use 'Extract as is...', and save as .ffs.



996AA1E0-1E8C-4F36-B519-A170A206FC14.ffs
 69009842-63F2-43DB-964B-EFAD1C39EC85.ffs
 4C494E55-5849-5342-4554-544552212121.ffs

SLP PubKey – as modded
 SLP Marker – as modded
 SlpSupport – common to all modded EFIs

pantagruel@My Digital Life Forums

<https://forums.mydigitallife.net>

Credit to cuiplay of bbs.kafan.cn for this approach to modding the VMware EFI.