## How to guide: Add a SLP 2.0 SLIC and SLP 1.0 string to Virtual PC 2007

Tools used:

- ResourceHacker <u>http://angusj.com/resourcehacker/</u>
- AMI MMTool v2.22.1 Beta
- Hex Editor (for example WinHex, like i used in this guide)

What else do you need:

- Microsoft Virtual PC 2007
   <u>http://www.microsoft.com/downloads/details.aspx?FamilyId=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en</u>
- Valid XP oembios file set (ASUS in this guide case) <u>http://www.oembios.net</u> 'f000','c000','3fff','ASUS\_FLASH'
- Valid Vista SLP 2.0 SLIC table (In this guide i use the ASUS slic)
- First thing we have to do is to extract the BIOS file from the Virtual PC 2007 executable.
   Open "Virtual PC.exe" with the ResourceHacker, Select "BIOS" from the treeview on the left side, right click with your mouse and choose "Save [BIOS] resources..."

Resource Hacker - C:\Temp\Virtu	al PC.exe
<u>File Edit View Action H</u> elp	
En BIOS	
i i i i i i i i i i i i i i i i i i i	
⊕	
⊡ 13502	
🖶 💼 DLL	
ELOPPYFORMAT	
EGISTRY	
🗄 🖳 Cursor	
🗄 🛄 Bitmap	
I ⊡ Icon	
I ⊕ in Menu	
🕂 🛄 Dialog	

Four files are extracted to the directory you specified to save the resources to, eg: \*.rc, Data\_1.bin, Data\_3.bin and Data\_3.bin. We only need "Data\_1.bin" so you can delete the others.

Name	Date modified	Туре	Size
bios.rc	30-12-2007 13:53	RC File	1 KB
Data_1.bin	30-12-2007 13:53	BIN File	256 KB
Data_2.bin	30-12-2007 13:53	BIN File	48 KB
🕥 Data_3.bin	30-12-2007 13:53	BIN File	45 KB
🔀 ResHacker.exe	24-3-2002 19:23	Application	861 KB
ResHacker.ini	30-12-2007 13:50	Configuration Sett	1 KB
崎 Virtual PC.exe	18-2-2007 8:29	Application	4.374 KB

Rename Data\_1.bin, In this guide i renamed it to BIOS.ROM.

2. Start MMTool, open the BIOS.ROM you just extracted and click the "Power MMTool" button. Click the Extract tab, select the 1B module and extract.

MN 🕅	/Tool v2.22.1 - C:\Temp\BIOS	.ROM				
La	ave ROM Module file:	e Delete Extra	act			Browse
Sav	e ROM as Module ID: Close Offset Segment	1B	Extract Module C As is in th In uncom	e ROM file pressed form		
м	MTool Lite		Extra	ct		
ID	Name	RomLoc	Source size	Size in Rom	%%	RunLoc
08 04 0C 18 19 18 21 06	Bootblock - Runtime interface Setup Client ROMID OEM Logo Display Manager Font Module Single Link Arch BIOS Multi Language DMI	F000:98B8 F000:5ECC F000:5EB0 F000:4DE0 F000:378C F000:31DC D000:ACD4 D000:8BC0 D000:88A8	071C(01820) 602E(24622) 0008(00008) ADBA(44474) 3EBD(16061) 1304(04868) 342AA(213674) 4905(18693) 067C(01660)	071C(01820) 39D8(14808) 0008(00008) 10BC(04284) 1640(05696) 059C(01436) 184F4(99572) 2100(08448) 0304(00772)	0.00 39.86 0.00 90.37 64.54 70.50 <b>53.40</b> 54.81 53.49	Dynamic Dynamic Dynamic Dynamic Dynamic Dynamic 0004:5553 Dynamic
Free S	Space: 188A0(100512)					

Ok we will start by adding the SLP 2.0 Slic table.
 Start your Hex Editor, open the 1B.ROM file you just extracted and saved using MMTool.
 Find the following text string: AMIBIOS 0800
 Ok, once you have found it you will see it is located at offset: 137FD

WinHex - [1B.ROM]			12							-				-	-			0.00710			X
Eile Edit Search	h <u>P</u> osition	<u>V</u> iew <u>T</u> ools	Spec <u>i</u> a	list <u>O</u>	ption	s <u>W</u>	/indo	w	<u>H</u> elp											-	Ξ×
🗅 🚔 🗟 🎒 🖆	🏂 🛛 🖻	a 👪 🗈 🗤	<i>ĝ</i> ĝ	HEX (	на На на	. <b>#</b>		-	-	<b>\</b>	⇒	6	<u>s</u> 5	6 <	ni) 🛅	<b>a</b> 🖌		₫ ◀	) 🗖 🖩		<i></i>
1B.ROM																					
1B ROM		Offset	0	1 2	3	4	5	6	7	8	9	A	В	С	D	E	F				*
C:\Temp		000137A0	00	00 00	00	00	00	00	00	00	00	00	00	00	00	00	00				
Dia sino i	200 KD	000137B0	00	00 00	00 0	00	00	00	00	00	00	00	00	00	00	00	00				
Pile size:	13.674 bytes	000137C0 000137D0	00	00 00 00 00	00	00	00	00	00	00	00	00	00	00	00	00	00		· · · · · · · ·	· · ·	
Default Edit Mede		000137E0	00	00 00	00 0	00	00	00	00	00	00	00	00	00	00	00	00				
State:	original	000137F0 00013800	00 42	00 00 49 41	) 00 7 53	00 20	00 30	00 38	00 30	00 30	00 30	00 32	00 00	00 00	41 30	4D 32	49 2F	BIOS 0		MI 02/	
Undo level:	0	00013810	32	32 2H	30	36	28	43	29	32	30	30	31	20	41	6D	65	22/06(	C)2001 /	Ame	
Undo reverses:	n/a	00013820	72	69 63	61	6E	20	4D	65	67	61	74	72	65	6E	64	73	rican	Megatre	nds	
C	20 12 2007	00013830	2C	20 49	9 6E	63	2E	20	41	6C	6C	20	52	69	67	68	74	, Inc.	All Rig	ght	-
Page 500 of 1336		Offset:		137F	D				= 4	IS BI	ock:							n/a Size	e:		n/a

This AMIBIOS 0800 string is quite unique as it is always remapped to 000FF400h memory address in your running bios.

Knowing this we can add the SLP 2.0 Slic table here, and make it so it will also be remapped to a fixed address in your bios memory.

Start the Calculator, Choose Scientific view, now take the offset we found the AMIBIOS 0800 string minus 200h, eg: 137FD – 200 = 135FD

By doing this we now know for sure the Slic address will be remapped to 000FF200h memory adrress (000FF400h – 200h = 000FF200h )

Now open the ASUS Slic in the Hex Editor, Select all (Ctrl+a) -> Click Edit -> Copy Block -> Hex Values and write it (Edit -> Clipboard Data -> Write) in the 1B.ROM at offset 135FD found above.

000135F0	00	00	00	00	00	00	00	00	00	00	00	00	00	53	4C	49	
00013600	43	76	01	00	00	01	4B	5F	41	53	55	53	5F	4E	6F	74	CvK_ASUS_Not
00013610	65	62	6F	6F	6B	24	06	00	11	4D	53	46	54	97	00	00	ebook\$MSFT[
00013620	00	00	00	00	00	9C	00	00	00	06	02	00	00	00	24	00	
00013630	00	52	53	41	31	00	04	00	00	01	00	01	00	6F	92	9D	.RSA1o1.
00013640	DC	B3	79	EE	27	26	08	F8	DC	5B	D8	5F	4B	21	34	AB	ܳyî'&.øÜ[Ø_K!4«
00013650	60	EC	90	C7	C2	D5	60	D5	F5	D9	82	F9	2E	BE	E8	43	`ì.ÇÅÕ`ÕõÙ∎ù.¾èC
00013660	38	D5	C2	5B	9E	25	B8	93	CD	15	B8	1B	C3	30	7D	AD	8ÕÅ[∎%,∎Í.,.Ã0}-
00013670	55	69	79	BD	1Å	7E	44	C8	BC	59	5A	17	BE	81	AD	EF	Uiy½.~DȼYZ.¾.−ï
00013680	EE	96	21	37	CC	84	42	62	C6	14	05	09	21	69	7A	E1	î∎!7Î∎BbÆ!izá
00013690	8C	44	CE	D6	C8	18	78	78	86	2B	30	63	Δ6	E5	64	B7	JÎÖÈ.xx +0c¦åd∘
000136A0	D2	14	5E	2B	44	BE	33	12	6B	6B	A3	BD	9E	85	BB	BE	Ò.^+D¾3.kk£½∎⇒»¾
000136B0	6C	E1	B1	33	C2	$D\mathbb{A}$	91	80	-F3	44	B4	CA	9F	01	00	00	lá±3ÅÚ′∎óD′Ê∎
000136C0	00	B6	00	00	00	00	00	02	00	5F	41	53	55	53	5F	4E	.¶ASUS_N
000136D0	6F	74	65	62	6F	6F	6B	57	49	4E	44	4F	57	53	20	00	otebookWINDOWS .
000136E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000136F0	00	00	00	24	B0	89	CF	B1	-F3	1D	B8	7A	80	35	CB	CD	\$*∎ϱó.,z∎5ËÍ
00013700	4 A	C8	2F	84	CE	99	Α0	4F	- 38	76	B0	04	F9	6F	05	33	]È∕∥Î∥ 08v°.ùo.3
00013710	C7	EC	Α8	58	Α6	D7	B7	3F	5B	82	B1	EE	2B	Α7	81	52	Çî‴X¦×+?[∎±î+S.R
00013720	F3	45	13	CE	EE	D5	57	37	FE	75	5F	SC	62	C4	53	DA	óE.ÎîÕ₩7þu_∖bÄSÚ
00013730	86	F1	34	FA	ED	91	86	73	9E	D2	65	FD	8A	ЗD	86	94	ñ4úí′ s Òeý =
00013740	2F	2A	65	18	SC	D9	E5	7C	15	1E	F2	08	C5	85	C4	8F	/*e.∖Ùå ò.Å∎Ä.
00013750	0B	FA	Δ5	C3	Α9	B0	F1	B2	E7	6A	46	$\mathbf{FB}$	18	01	5D	4C	.ú¥Ã©°ñ²çjFû]L
00013760	36	33	DE	$\mathbf{FB}$	E7	1D	E8	15	C2	85	9F	8A	Α9	32	68	1F	63Þûç.è.Å∎∎©2h.
00013770	B4	BC	A8	00	00	00	00	00	00	00	00	00	00	00	00	00	1411
00013780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

In the Hex Editor search string: "RSDT" (Should be found at offset 2882C)

Raise the RSDT table length by counting +4h to it, eg: take the HEX value right after the RSDT string, in this case 28 + 4 = 2C

## Replace "A M I OEMRSDT" with "\_ASUS\_Notebook"

From the R character of RSDT string count 40 bytes up and insert 000FF200h in reverse order, eg: 00F20F00

.,."∎Ø∎À∎Èë±RSDT	54	44	53	52	B1	EB	C8	8C	CO	8E	D8	8E	Α8	00	B8	08	00028820
ASUS_Note	65	74	6F	4E	5F	53	55	53	41	5F	00	01	00	00	00	2C	00028830
book"MSFT	00	00	00	97	54	46	53	4D	02	00	06	22	6B	6F	6F	62	00028840
<mark>.ò.</mark>	00	00	00	00	00	00	00	00	00	0F	F2	00	00	00	00	00	00028850

Repeat above action for the XSDT table, raise the XSDT table length with +8h (2C = 8 = 34) Replace "A M I OEMRSDT" with "\_ASUS\_Notebook"

And last count 44 bytes (40+4 as it's 4 bytes longer now) up to the X character of the XSDT string.

00028920	00	00	00	00	00	00	00	00	00	00	00	00	58	53	44	54	XSDT
00028930	34	00	00	00	01	00	5F	41	53	55	53	5F	4E	6F	74	65	4ASUS_Note
00028940	62	6F	6F	6B	22	06	00	02	4D	53	46	54	97	00	00	00	book"MSFT
00028950	00	00	00	00	00	00	00	00	00	F2	0F	00	00	00	00	00	òò

## 4. Adding the SLP 1.0 String

NOTE: SLP 1.0 requirements can be achieved for about 90% of the OEM partners by simply adding the desired SLP 1.0 string to your computers DMI table. There are exception to this, for example the 'ASUS\_FLASH' string should be located im memory prior to the DMI table.

What is 'f000','c000','3fff','ASUS\_FLASH' ?

- F000,C000 -> Start Address (0x000FC000) of the SLP Address
- 3FFF -> Address range in bytes (in hex)
- ASUS\_FLASH -> SLP 1.0 String which must be placed in the address range

To determine where the slp 1.0 string should be located run HWDirect on a Virtual PC installed OS, Select "Memory Dump" in program left side treeview.

Type: 000FC000 as Physical address, 3FFF as Length, Click "Dump" button.

Find a string you can find back in the 1B.ROM module, scroll a bit down in the HWDirect dump and you will find a IBM COMPATIBLE... string

🗖 Memory Dump	
Physical Address (Hex) Size (Bytes in Hex) 000FC000 3FFF Dump Write Memory Dump	Clear
000FDFC0       FF       FF	A  8IB E IBM MARK IONAL ACHIN .44 
⊙ ASCII Mode ◯ HEX Mode ◯ Case s	ensitive

In 1B.ROM still open in the Hex Editor find string: IBM, make sure you at the exact same location as shown above, Now you can insert the ASUS\_FLASH string.

Make sure, you don't overwrite anything that might corrupt the Virtual PC BIOS, normally empty space "00 00 00 00 00 00" can be used without risk, in this example i wrote the string at offset : 123FD (Not exactly empty block here, but that doesn't matter in this case)

000123F0	00	00	00	00	00	00	00	00	00	00	00	00	00	41	53	55	
00012400	53	5F	46	4C	41	53	48	D4	38	00	00	49	42	4D	20	43	S_FLASHÔ8IBM C
00012410	4F	4D	50	41	54	49	42	4C	45	20	49	42	4D	20	49	53	OMPATIBLE IBM IS

5. Save changes to 1b.ROM, Swith back to MMTool In the replace Tab replace 1B Module with our new one, save the BIOS.ROM file.

In Resource Hacker, replace BIOS -> 13500 -> 1033 File with our new bios file, and save the new Virtual PC.exe

x

## 6. Done!

You can now use ASUS Vista OEM Certifcate to pre-activate Vista on this Virtual PC, futhermore you also can use ASUS XP oembios files to pre-activate XP OEM media on this Virtual PC