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

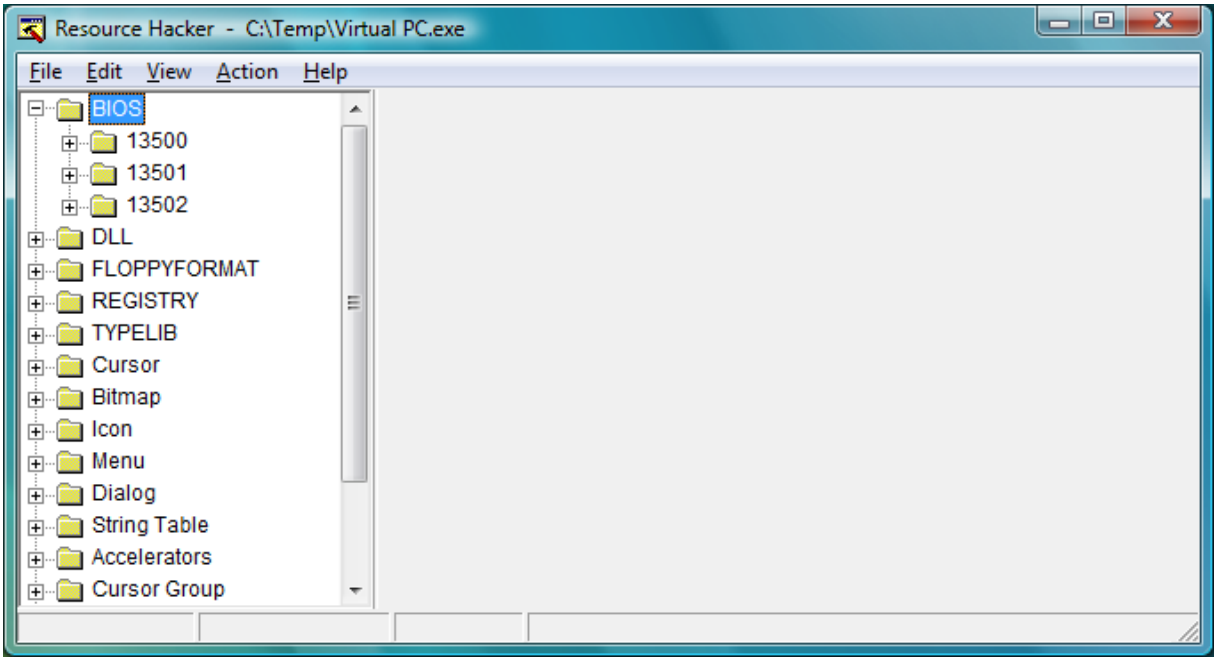
Tools used:

- ResourceHacker http://angusj.com/resourcehacker/
- 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
  http://www.microsoft.com/downloads/details.aspx?FamilyId=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en
- Valid XP oembios file set (ASUS in this guide case) http://www.oembios.net
  'f000','c000','3fff','ASUS_FLASH'
- Valid Vista SLP 2.0 SLIC table (In this guide i use the ASUS slic)

1. 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...”

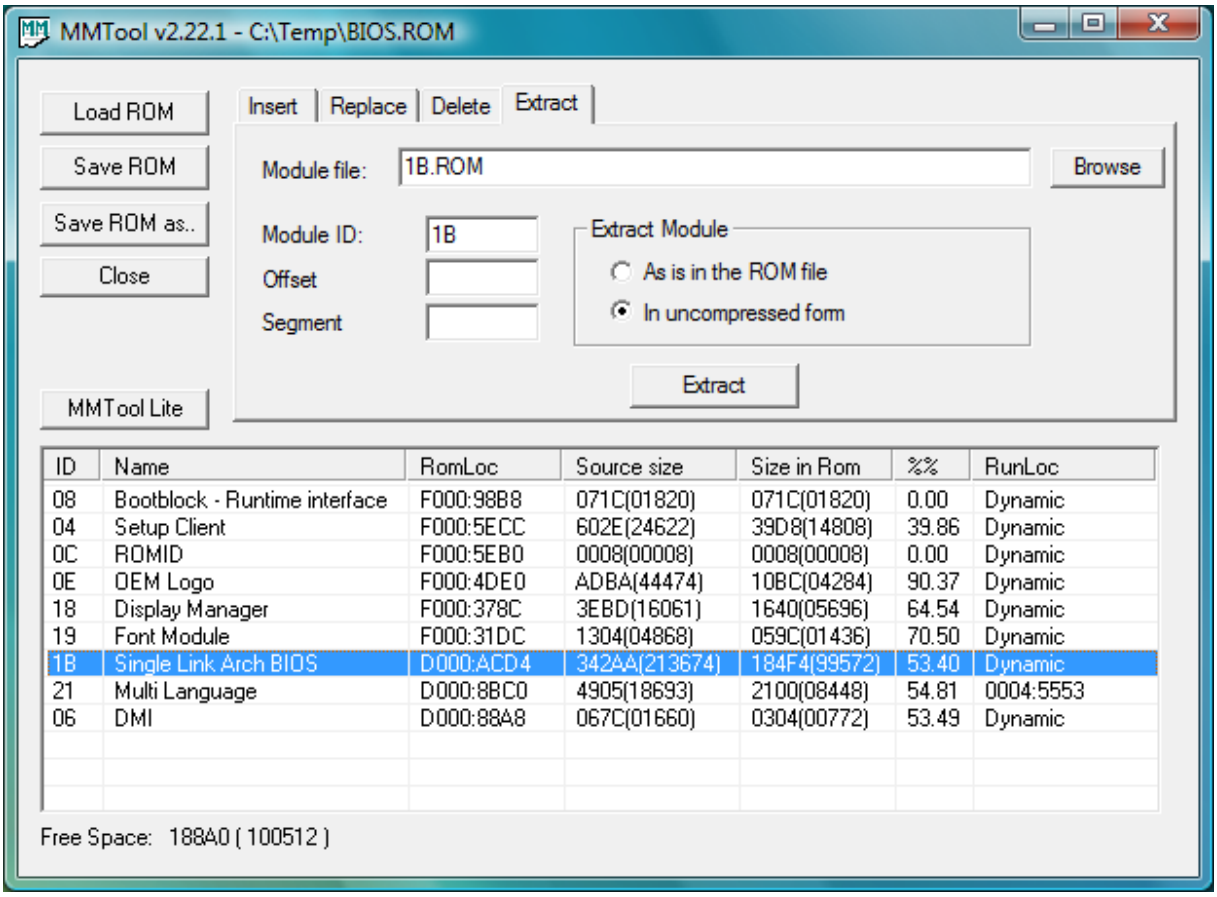


   Four files are extracted to the directory you specified to save the resources to, eg: *.rc, Data_1.bin, Data_3.bin and Data_3.bin. We only need “Data_1.bin” so you can delete the others.

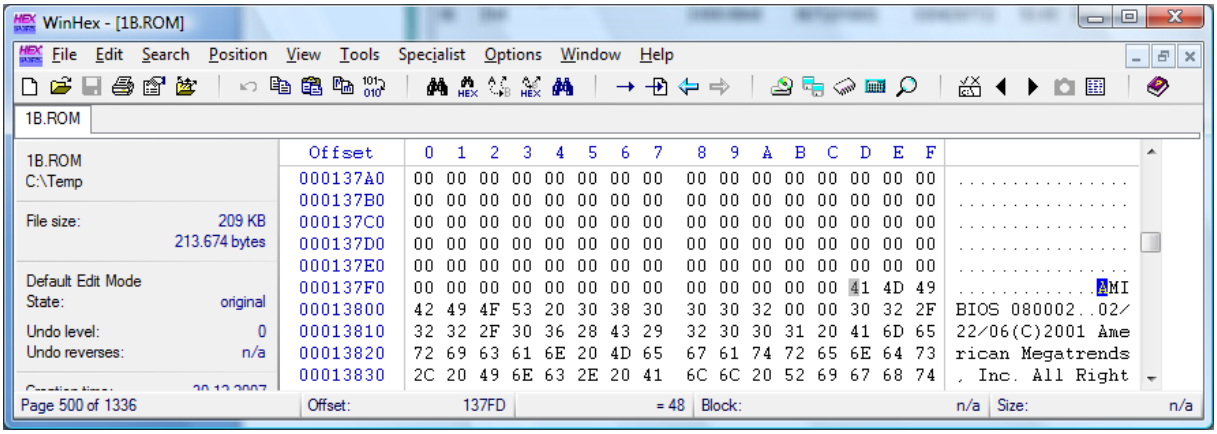
Name	Date modified	Type	Size
bios.rc	30-12-2007 13:53	RC File	1 KB
Data_1.bin	30-12-2007 13:53	BIN File	256 KB
Data_2.bin	30-12-2007 13:53	BIN File	48 KB
Data_3.bin	30-12-2007 13:53	BIN File	45 KB
ResHacker.exe	24-3-2002 19:23	Application	861 KB
ResHacker.ini	30-12-2007 13:50	Configuration Sett...	1 KB
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.



3. 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



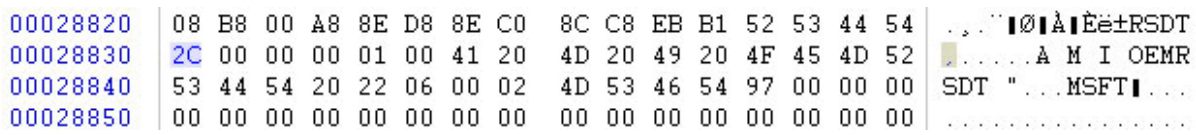
This AMIBIOS 0800 string is quite unique as it is always remapped to 000FF400h memory address in your running bios.
Knowing this we can add the SLP 2.0 Slic table here, and make it so it will also be remapped to a fixed address in your bios memory.
Start the Calculator, Choose Scientific view, now take 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.

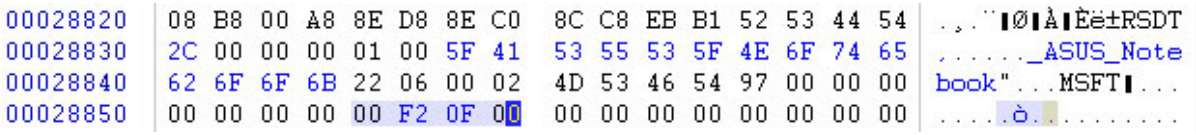
```
000135F0  00 00 00 00 00 00 00 00  00 00 00 00 00 53 4C 49  .............SLI
00013600  43 76 01 00 00 01 4B 5F  41 53 55 53 5F 4E 6F 74  Cv....K_ASUS_Not
00013610  65 62 6F 6F 6B 24 06 00  11 4D 53 46 54 97 00 00  ebook$...MSFT▮..
00013620  00 00 00 00 00 9C 00 00  00 06 02 00 00 00 24 00  .....▮........$.
00013630  00 52 53 41 31 00 04 00  00 01 00 01 00 6F 92 9D  .RSA1........o´.
00013640  DC B3 79 EE 27 26 08 F8  DC 5B D8 5F 4B 21 34 AB  Ü³yî'&.øÜ[Ø_K!4«
00013650  60 EC 90 C7 C2 D5 60 D5  F5 D9 82 F9 2E BE E8 43  `ì.ÇÂÕ`ÕõÙ▮ù.¾èC
00013660  38 D5 C2 5B 9E 25 B8 93  CD 15 B8 1B C3 30 7D AD  8ÕÂ[▮%¸▮Í.¸.Ã0}-
00013670  55 69 79 BD 1A 7E 44 C8  BC 59 5A 17 BE 81 AD EF  Uiy½.~DÈ¼YZ.¾.-ï
00013680  EE 96 21 37 CC 8A 42 62  C6 14 05 09 21 69 7A E1  î▮!7Ì▮BbÆ...!izá
00013690  8C 4A CE D6 C8 18 78 78  86 2B 30 63 A6 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 DA 91 80  F3 44 B4 CA 9F 01 00 00  lá±3ÂÚ´▮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  ...$°▮Ï±ó.¸z▮5ËÍ
00013700  4A C8 2F 84 CE 99 A0 4F  38 76 B0 04 F9 6F 05 33  JÈ/▮Î▮ O8v°.ùo.3
00013710  C7 EC A8 58 A6 D7 B7 3F  5B 82 B1 EE 2B A7 81 52  Çì¨X¦×·?[▮±î+§.R
00013720  F3 45 13 CE EE D5 57 37  FE 75 5F 5C 62 C4 53 DA  óE.ÎîÕW7þu_\bÄSÚ
00013730  86 F1 34 FA ED 91 86 73  9E D2 65 FD 8A 3D 86 94  ▮ñ4úí´▮s▮Òeý▮=▮▮
00013740  2F 2A 65 18 5C D9 E5 7C  15 1E F2 08 C5 85 C4 8F  /*e.\Ùå|..ò.Å▮Ä.
00013750  0B FA A5 C3 A9 B0 F1 B2  E7 6A 46 FB 18 01 5D 4C  .ú¥Ã©°ñ²çjFû..]L
00013760  36 33 DE FB E7 1D E8 15  C2 85 9F 8A A9 32 68 1F  63Þûç.è.Â▮▮▮©2h.
00013770  B4 BC A8 00 00 00 00 00  00 00 00 00 00 00 00 00  ´¼¨.............
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)

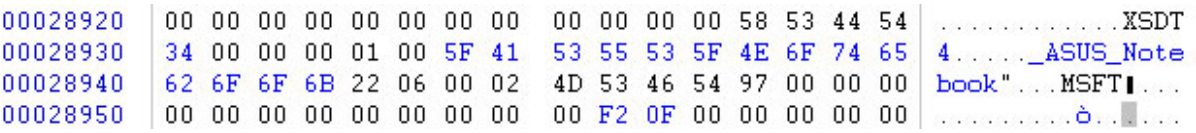
Raise the RSDT table length by counting +4h to it, eg: take the HEX value right after the RSDT string, in this case 28 + 4 = 2C



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



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.



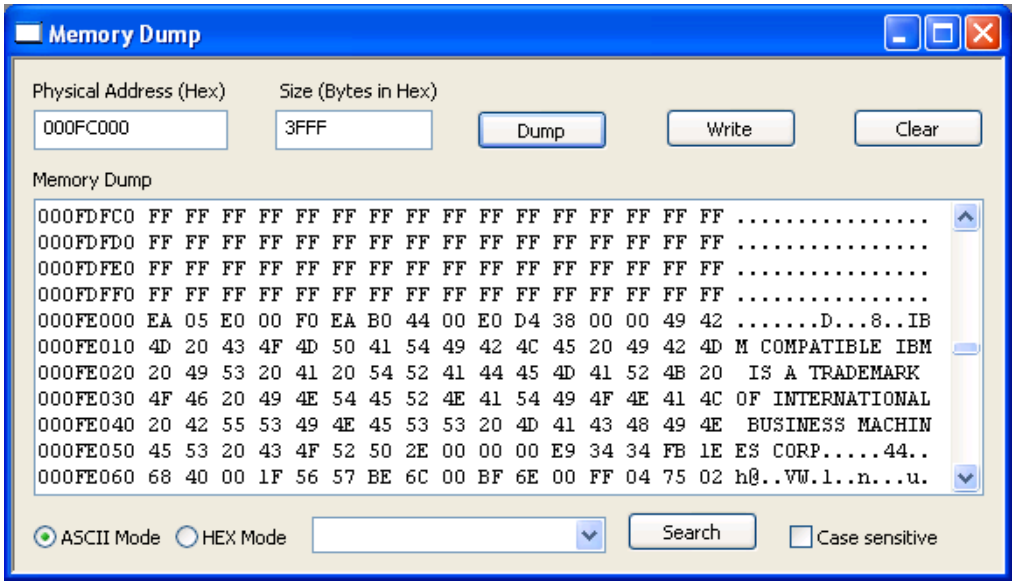
4. Adding the SLP 1.0 String

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



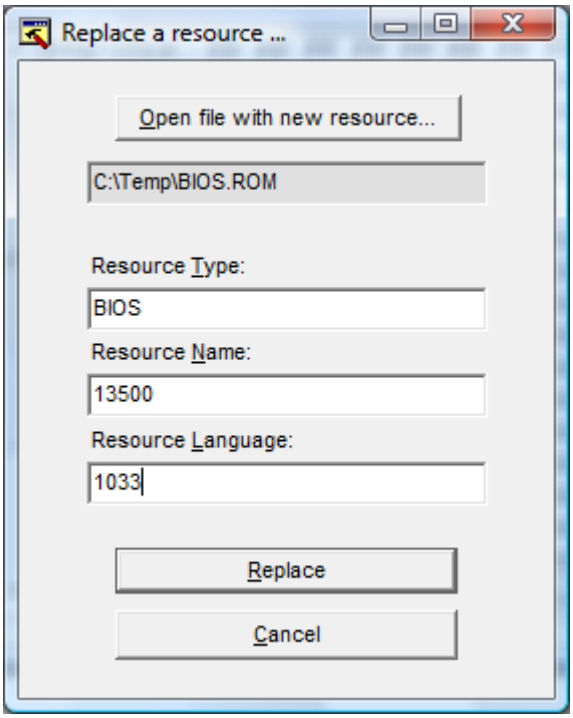
In 1B.ROM still open in the Hex Editor find string: IBM, make sure you at the exact same location as shown above, Now you can insert the ASUS_FLASH string.

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 | .............ASU
00012400 | 53 5F 46 4C 41 53 48 D4  38 00 00 49 42 4D 20 43 | S_FLASHÔ8..IBM 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



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