Patching

Программа – последовательность инструкций

calc.exe

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00098B80   DA CA 15 16 97 8F B0 7C F5 3B CA C5 83 A8 3A 86  ÚÊ..—.°|õ;ÊÅƒ¨:†
00098B90   FD CB 66 E0 7D 4C AD 79 8B D9 67 8E A3 87 8F 83  ýËfà}L.y‹ÙgŽ£‡.ƒ
00098BA0   19 51 A9 92 9B 83 99 D1 A8 AF 81 08 41 A3 5E E3  .Q©'›ƒ™Ñ¨¯..A£^ã
00098BB0   D0 FC 21 56 9B 1E 6F E4 DB 39 81 B9 99 49 7E BF  Ðü!V›.oäÛ9.¹™I~¿
00098BC0   FE 17 51 F0 2D 94 DE 84 FA 4F D0 BC 07 3E 1E 8A  þ.Qð-"Þ„úOÐ¼.>.Š
00098BD0   2F EA A0 38 03 A5 97 89 D6 3E 60 E5 DA 1C 07 F7  /ê 8.¥—‰Ö>`åÚ..÷
00098BE0   3E CB 1E A7 E4 1F 01 95 E2 21 FE BE F6 39 13 33  >Ë.§ä..•â!þ¾ö9.3
00098BF0   AF 30 B7 EF 40 6E B8 00 22 42 54 AA 70 F7 CE 6D  ¯0·ï@n¸."BTªp÷Îm
00098C00   02 EF 3D 22 92 1B 6E A2 E0 C4 B9 F7 1E D5 9B 89  .ï="'.n¢àÄ¹÷.Õ›‰
00098C10   72 9B F7 A0 B6 02 C3 1E 3B 4D 41 4E 6C A2 7A 13  r›÷ ¶.Ã.;MANl¢z.
00098C20   8B CB 14 02 87 8A 21 9A 53 69 DE 50 71 58 BC 4E  ‹Ë..‡Š!šSiÞPqX¼N
00098C30   8B C3 A8 46 8B 43 C0 38 87 59 A2 DC 3C 31 CD FB  ‹Ã¨F‹CÀ8‡Y¢Ü<1Íû
00098C40   54 FD 1D 05 04 0E 54 84 BC 3C 6C 44 C2 7A F8 19  Tý....T„¼<lDÂzø.
00098C50   19 2F E1 C1 C3 C2 0E 6E B2 8E 54 3A C2 CE A7 32  ./áÁÃÂ.n²ŽT:ÂΧ2
00098C60   C0 8F 97 80 F2 08 8E 11 9E E4 91 FA FA DF 00 7E  À.—€ò.Ž.žä'úúß.~
00098C70   94 C6 8E 21 E2 A5 57 DF EE BB F8 E7 1F BF 1C F8  "ÆŽ!â¥Wßî»øç.¿.ø
00098C80   07 9F 7C AF D6 D7 A6 FA 69 79 60 BF 2F 9C 8A FB  .Ÿ|¯Ö×¦úiy`¿/œŠû
00098C90   DA 2C 7C E8 06 F6 FB C7 9F 37 FA DA 3C FD D4 91  Ú,|è.öûÇŸ7úÚ<ýÔ'
00098CA0   C1 15 DC 0F DE AE E1 8A 75 CD EA D9 D2 C3 E1 9E  Á.Ü.Þ®áŠuÍêÙÒÃáž
00098CB0   2D 75 AF A1 F5 CC 07 6F 18 B8 FD E0 ED E6 7B 1D  -u¯¡õÌ.o.¸ýàíæ{.
00098CC0   06 E2 40 CA 95 AD B3 7A 7E 7B C8 D5 73 A5 AD F6  .â@Ê•.³z~{ÈÕs¥.ö
00098CD0   BA 4D A0 DC C6 A7 A9 E7 D2 A9 ED 21 5E 3A E5 30  ºM ÜÆ§©çÒ©í!^:å0
00098CE0   4D 6C B6 5B 3B 2C E4 7E 70 77 15 83 7B 61 0E 0C  Ml¶[;,ä~pw.ƒ{a..
```

Картинка

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00010F60   68 3E 54 1F A1 22 54 DA 1E 65 A1 60 FD EB 47 76   h>T.¡"TÚ.e¡`ýëGv
00010F70   DE 8F 33 5F 44 B5 A1 AE 67 2F BD 7E EA F9 F7 5C   Þ.3_Dµ¡®g/½~êù÷\
00010F80   29 94 CF C0 78 CA 3D A7 ED 40 65 C7 72 EB 67 68   )”ÏÀxÊ=§í@eÇrëgh
00010F90   7E 65 9F F7 3E 6E 3D 6C 99 DA 50 30 EB C2 A7 F0   ~eŸ÷>n=l™ÚP0ëÂ§ð
00010FA0   AE E7 DE 6B 37 56 05 E9 E4 3F 3E 72 0F 4A 2C 9F   ®çÞk7V.éä?>r.J,Ÿ
00010FB0   F8 7A AE 5F D6 AA CF 81 99 DF 4F 60 8E CC 5A 5C   øz®_Öª Ï.™ßO`ŽÌZ\
00010FC0   1B D0 EE D3 0A 00 00 00 00 00 00 00 D3 1C 50 80   .ÐîÓ........Ó.P€
00010FD0   8E 77 5A F8 98 B1 17 8C BD 88 E8 43 55 F4 90 6F   ŽwZø˜±.Œ½ˆèCUô.o
00010FE0   9F 6D 9F 96 ED 66 B0 CF 9A D3 E0 FD 8C 9E 75 AF   ŸmŸ–íf°ÏšÓàýŒžu¯
00010FF0   8F DD 77 65 7B 62 7F D6 E6 F9 F5 DE FA 85 6F 3C   .Ýwe{b.ÖæùõÞú…o<
00011000   8E D8 8B EC 57 2C 79 6A 0C F7 3B 81 13 B1 5C FD   ŽØ‹ìW,yj.÷;..±\ý
00011010   B3 D9 55 6B E2 1B E3 41 62 57 0B ED EC FA 88 66   ³ÙUkâ.ãAbW.íìúˆf
00011020   8D 7C FA E3 CB E5 13 BB CA 8C F2 F6 C4 0E B5 F9   .|úãËå.»ÊŒòöÄ.µù
00011030   66 2C 9D FE EB BD 35 F3 8D AA 03 A1 7B E3 E7 1F   f,.þë½5ó.ª.¡{ãç.
00011040   98 33 F2 45 46 C7 5A 64 7D 19 7E A4 87 F5 D2 52   ˜3òEFÇZd}.~¤‡õÒR
00011050   1A 98 33 8A 58 E4 8C C7 E8 64 53 CB 9D 1B FF A1   .˜3ŠXäŒÇèdSË..ÿ¡
00011060   F3 C9 3F D4 5F 8C 73 56 36 53 BD 75 52 1F E5 48   óÉ?Ô_ŒsV6S½uR.åH
00011070   9F BF 1A AB 76 71 D6 8F EC BC 13 1D 65 BE 28 76   Ÿ¿.«vqÖ.ì¼..e¾(v
00011080   95 D0 4E 8A EC B5 32 1F E9 F5 13 BB B3 AD 5F DE   •ÐNŠìµ2.éõ.»³._Þ
00011090   57 AB AC 28 98 CF E0 78 CA 3C A7 AA B7 8E 9C EA   W«¬(˜ÏàxÊ<§ª·Žœê
000110A0   15 11 CD F2 B2 AE DC FA 19 99 5F D9 E7 BD 63 11   ..Íò²®Üú.™_Ùç½c.
000110B0   39 86 9F 30 B6 F6 D4 3C 35 DF 30 FC 8B A1 60 AA   9†Ÿ0¶öÔ<5ß0ü‹¡`ª
```

НЕЛЬЗЯ ТАК ПРОСТО ВЗЯТЬ

И ИЗМЕНИТЬ ПРОГРАММУ

Почему?

- При компиляции в программу «зашиваются» смещения. При изменении размера программы, переходы станут некорректными
- Можно сделать что-то не то

Как патчить программы?

NOP

Можно убрать «неугодные» инструкции

Jcc (JMP, JZ, JBE, etc.)

Изменить условие перехода

Что-то осмысленное

Такое редко бывает нужным

Зачем это вообще надо?