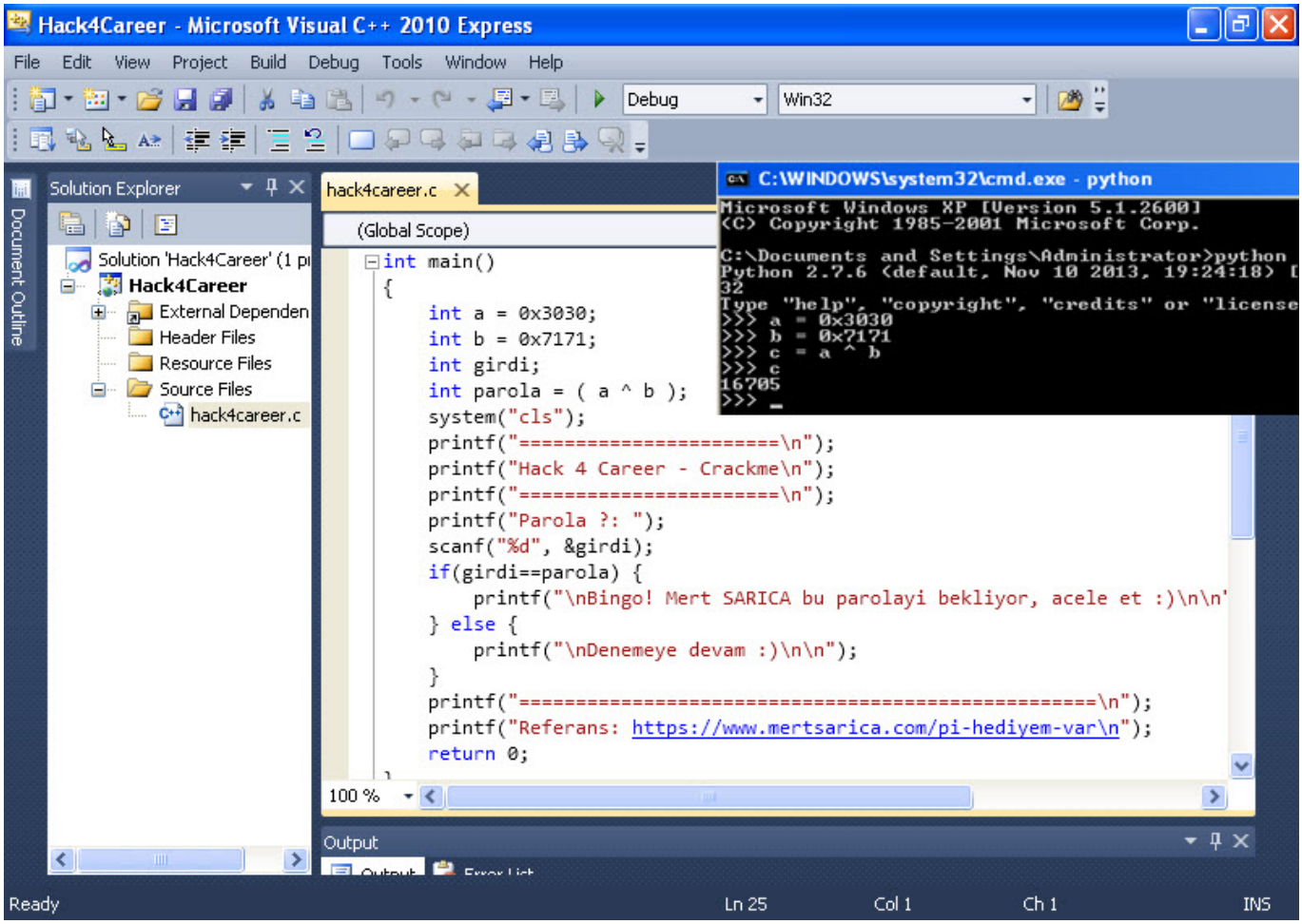
Pi Hediyem Vardı, Verdim, Gitti :)

written by Mert SARICA | 3 March 2015

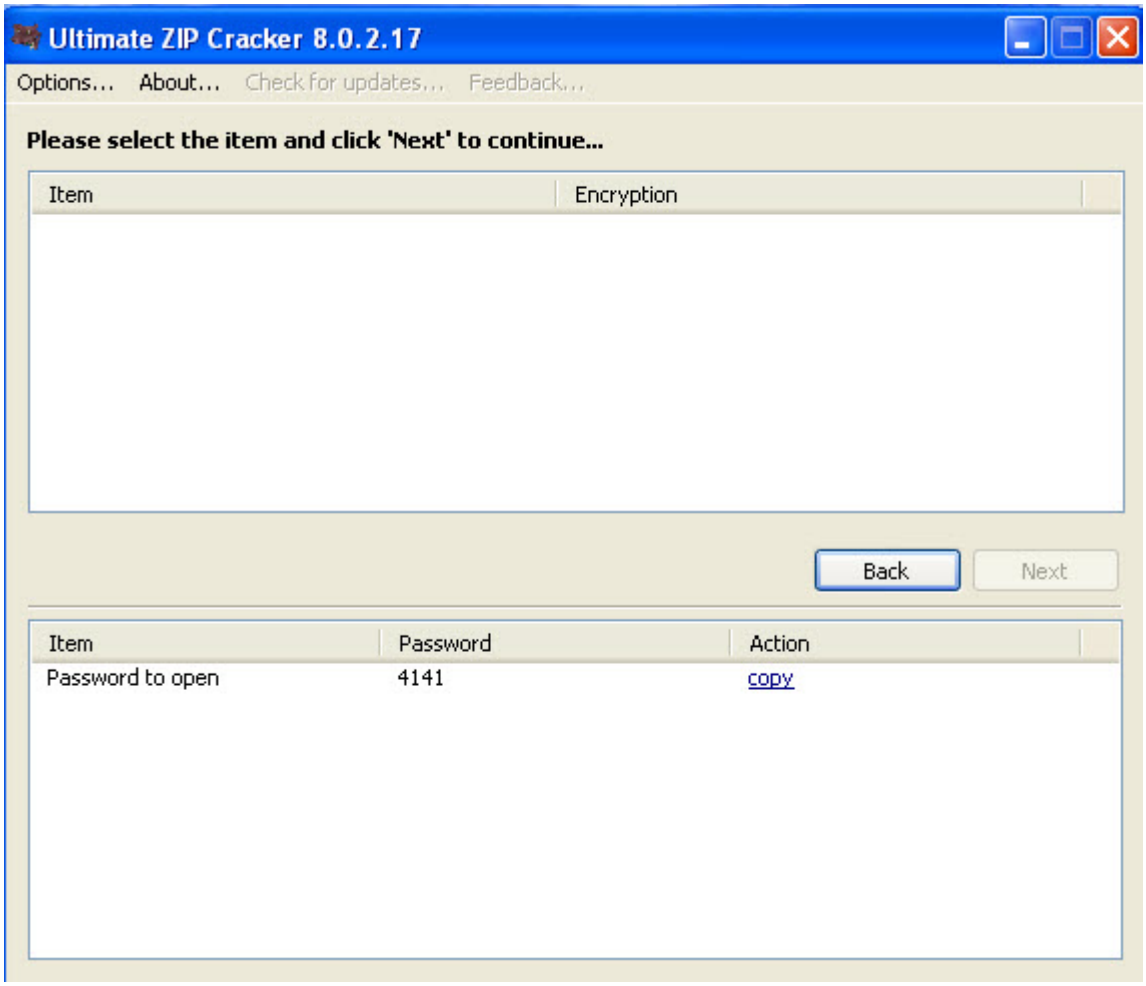
Takip edenleriniz, 13 Şubat 2015 tarihinde parola bulma oyunu ile üniversite öğrencisi olan iki takipçime, Raspberry Pi (B Model) hediye etme kararı aldığımı hatırlayacaklardır. Bu yazıda hem talihli iki takipçimi hem de oyunun çözümünü açıklayacağım.

KAYNAK KODU:

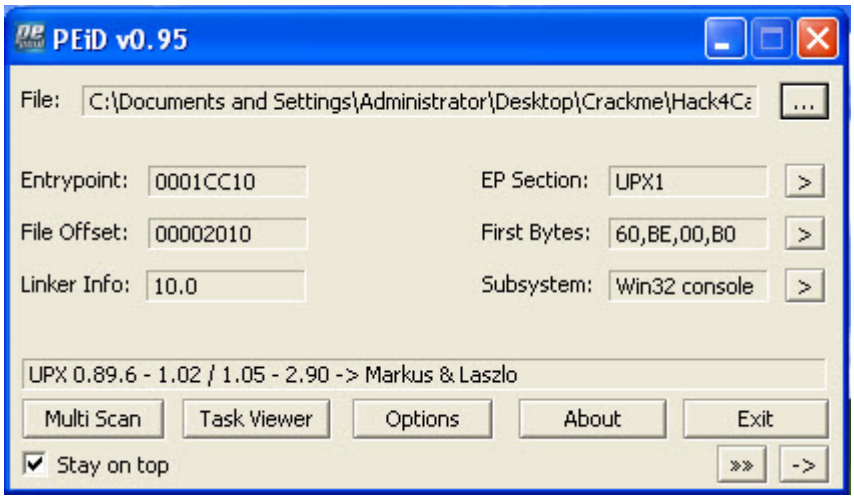


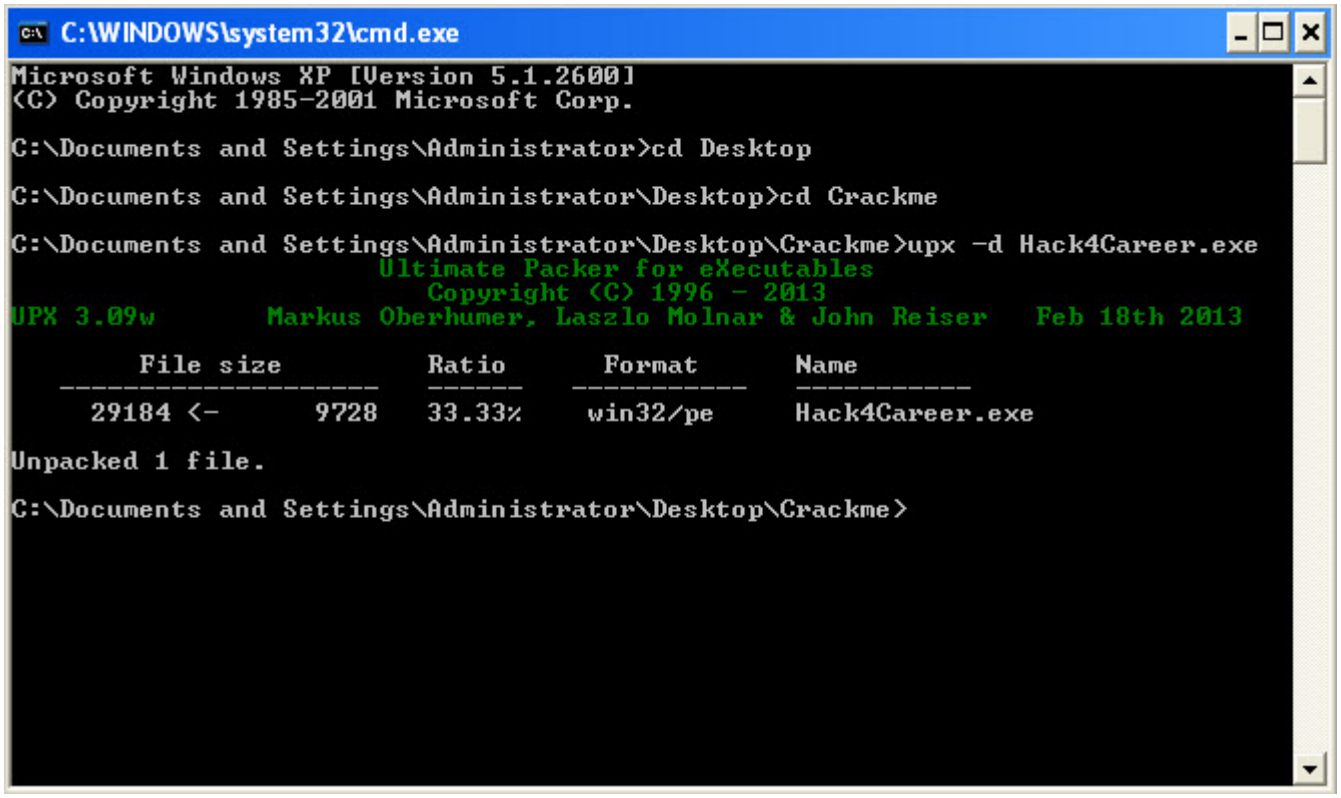
ÇÖZÜM:

Crackme.zip ZIP dosyasının şifresi, herhangi basit bir şifre çözme programı ile kolaylıkla bulunabilirdi. (ZIP şifresi: 4141)

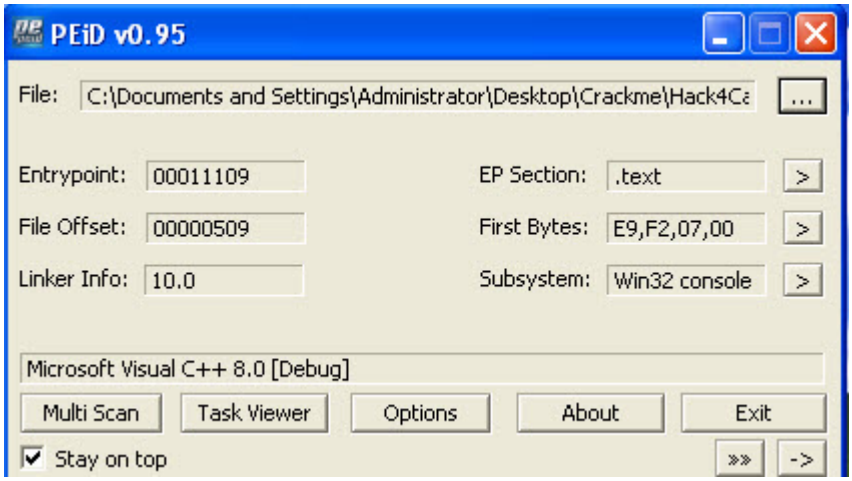


ZIP dosyası içinden çıkan Hack4Career.exe programını PEiD aracı ile incelediğinizde bunun UPX aracı ile sıkıştırıldığını görebilir ve yine UPX aracı ile açabilirdiniz.

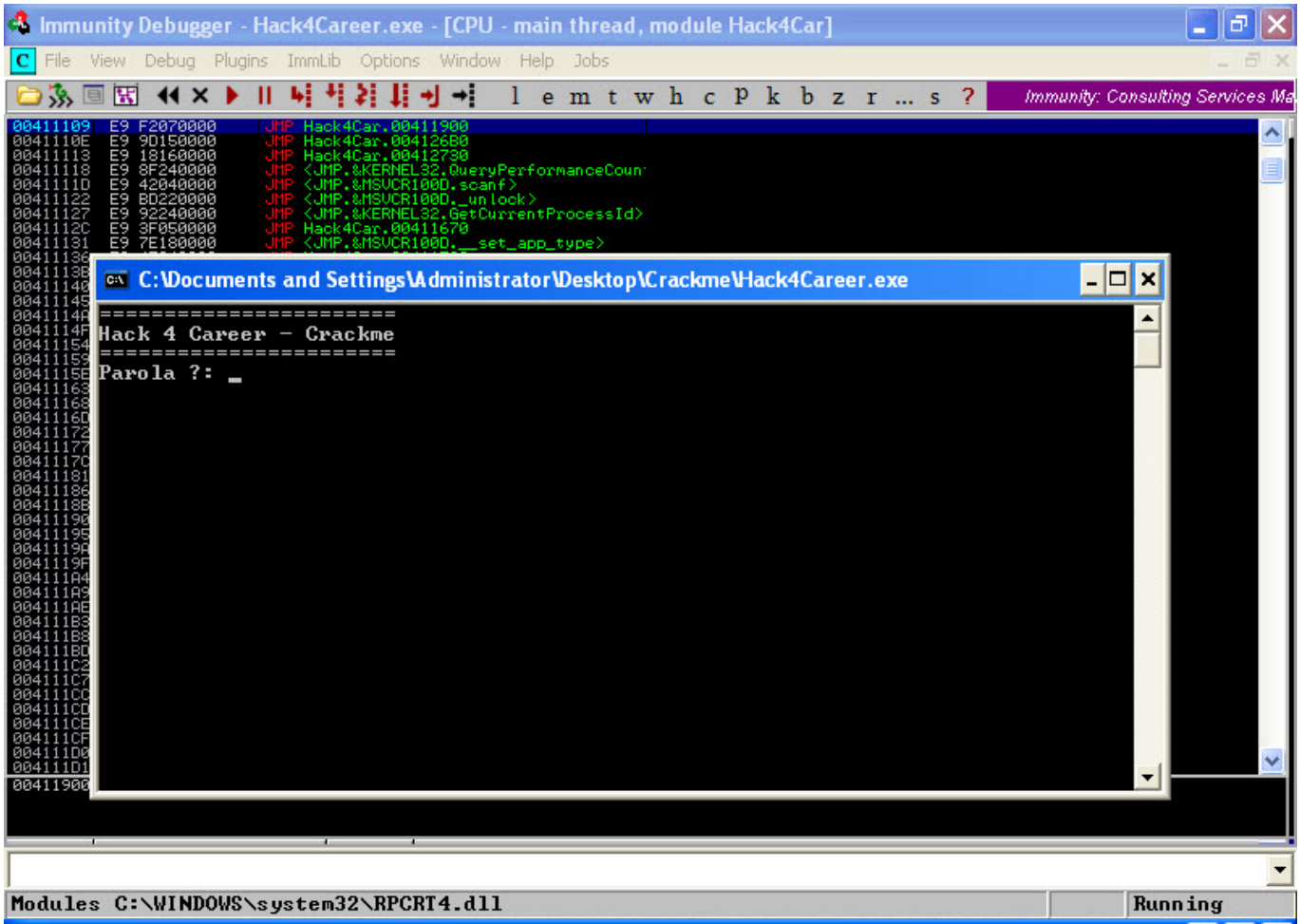


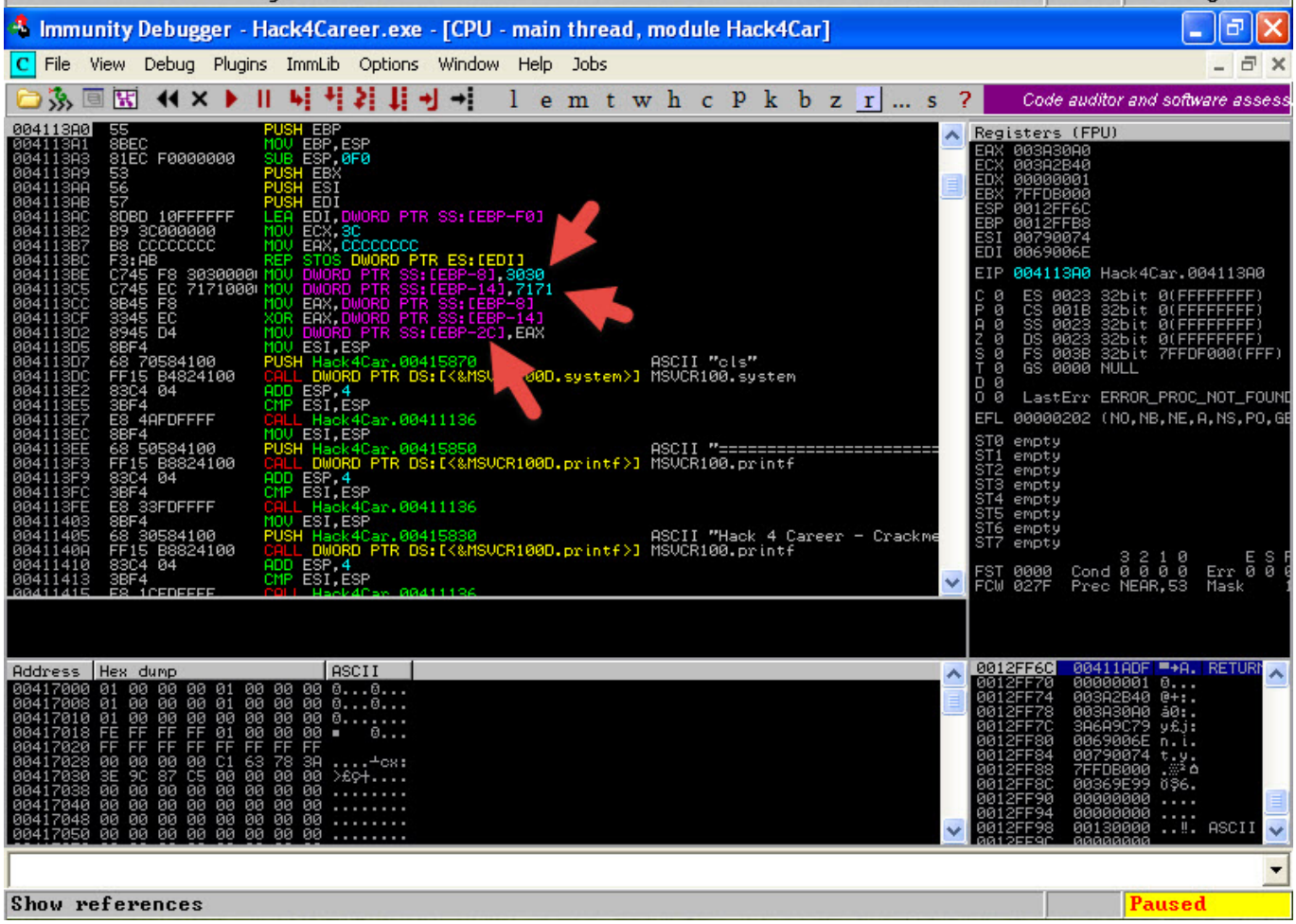


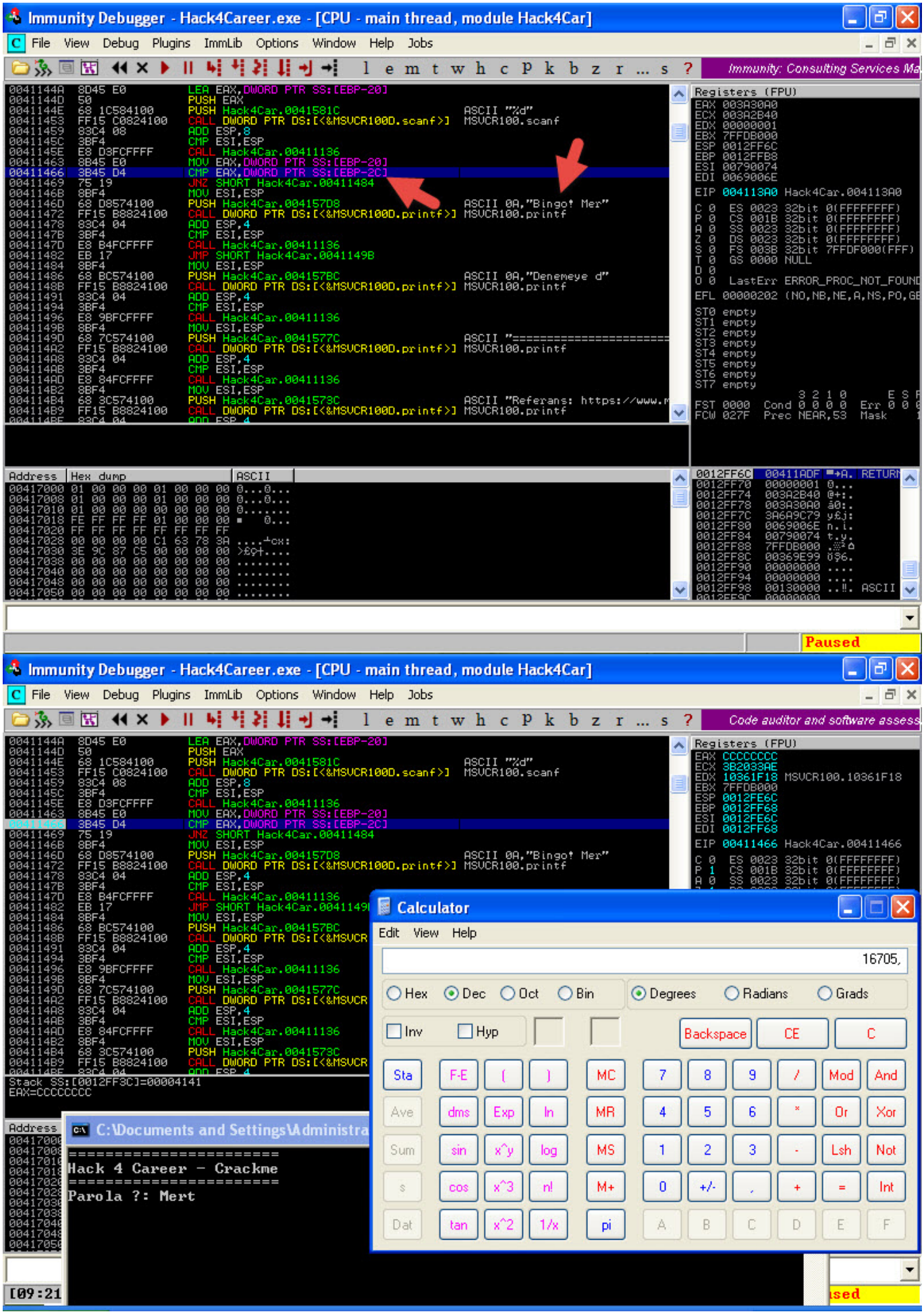
Yine PEiD ile bu programını incelediğinizde programın Visual C++ ile derlendiğini görebilirdiniz.



Hack4Career.exe programını Immunity Debugger aracı (debugger) ile incelediğinizde 004113A0 fonksiyonunda iki değerin (0x3030 ve 0x7171) XOR işleminden geçirildiğini (XOR işleminin sonucu 0x4141), kullanıcıdan alınan girdi (input) ile ondalık değere çevrilerek (0x4141 değerinin ondalık karşılığı 16705'dir.) karşılaştırıldığını görebilir ve 16705 değerini bana ileterek oyunu başarıyla tamamlayabilirdiniz :)

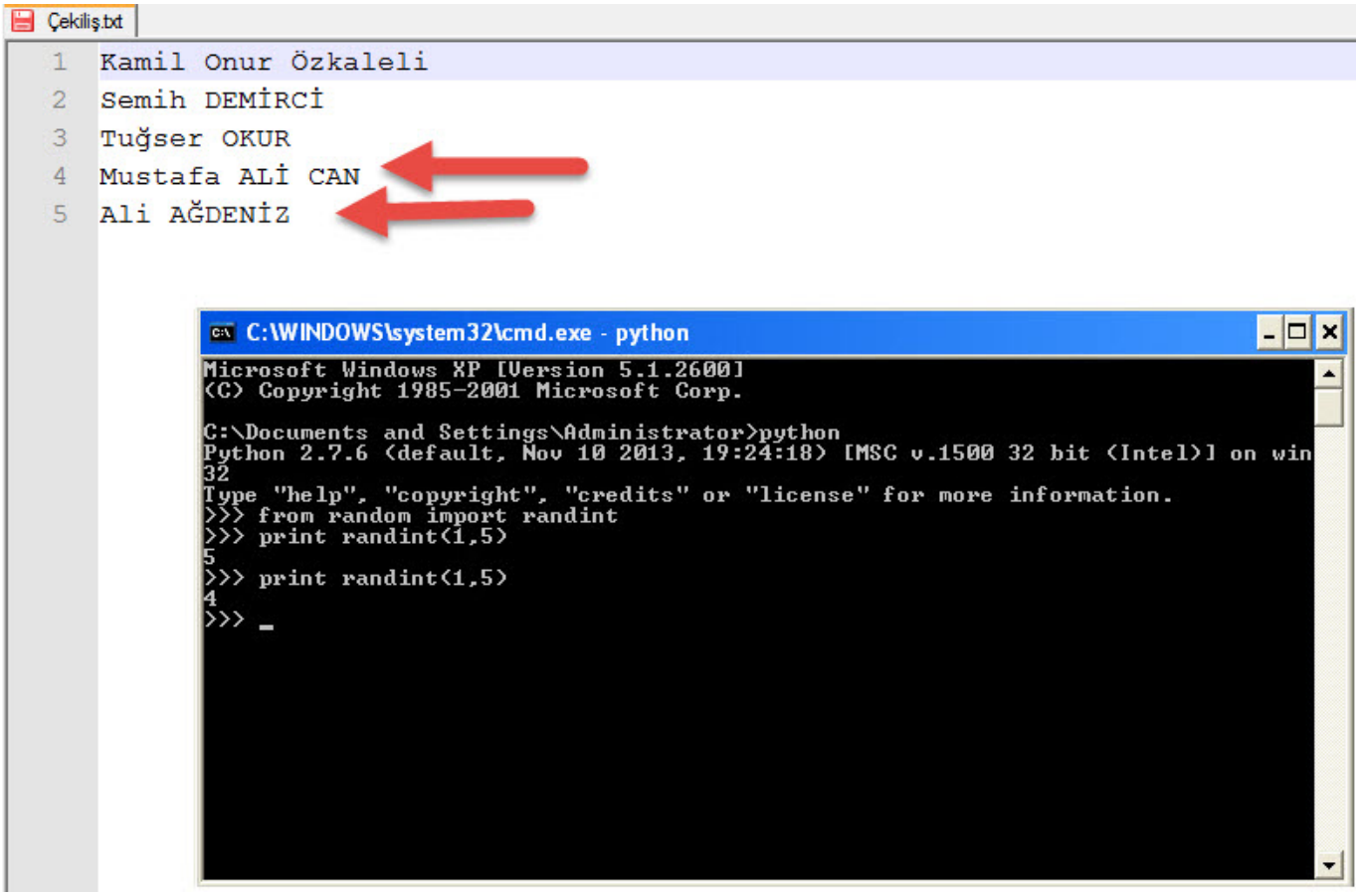

Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Ma
00411109 E9 F2070000 JMP Hack4Car.00411900
0041110E E9 9D150000 JMP Hack4Car.004126B0
00411113 E9 18160000 JMP Hack4Car.00412730
00411118 E9 8F240000 JMP <JMP.&KERNEL32.QueryPerformanceCoun
0041111D E9 42040000 JMP <JMP.&MSVCR100D.scanf>
00411122 E9 BD220000 JMP <JMP.&MSVCR100D._unlock>
00411127 E9 92240000 JMP <JMP.&KERNEL32.GetCurrentProcessId>
0041112C E9 3F050000 JMP Hack4Car.00411670
00411131 E9 7E180000 JMP <JMP.&MSVCR100D.__set_app_type>
C:\Documents and Settings\Administrator\Desktop\Crackme\Hack4Career.exe
========================
Hack 4 Career - Crackme
========================
Parola ?: _
Modules C:\WINDOWS\system32\RPCRT4.dll
Running


Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assess
004113A0 55 PUSH EBP
004113A1 8BEC MOV EBP,ESP
004113A3 81EC F0000000 SUB ESP,0F0
004113A9 53 PUSH EBX
004113AA 56 PUSH ESI
004113AB 57 PUSH EDI
004113AC 8DBD 10FFFFFF LEA EDI,DWORD PTR SS:[EBP-F0]
004113B2 B9 3C000000 MOV ECX,3C
004113B7 B8 CCCCCCCC MOV EAX,CCCCCCCC
004113BC F3:AB REP STOS DWORD PTR ES:[EDI]
004113BE C745 F8 3030000(MOV DWORD PTR SS:[EBP-8],3030
004113C5 C745 EC 7171000(MOV DWORD PTR SS:[EBP-14],7171
004113CC 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8]
004113CF 3345 EC XOR EAX,DWORD PTR SS:[EBP-14]
004113D2 8945 D4 MOV DWORD PTR SS:[EBP-2C],EAX
004113D5 8BF4 MOV ESI,ESP
004113D7 68 70584100 PUSH Hack4Car.00415870 ASCII "cls"
004113DC FF15 B4824100 CALL DWORD PTR DS:[<&MSV 00D.system>] MSVCR100.system
004113E2 83C4 04 ADD ESP,4
004113E5 3BF4 CMP ESI,ESP
004113E7 E8 4AFDFFFF CALL Hack4Car.00411136
004113EC 8BF4 MOV ESI,ESP
004113EE 68 50584100 PUSH Hack4Car.00415850 ASCII "==========
004113F3 FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
004113F9 83C4 04 ADD ESP,4
004113FC 3BF4 CMP ESI,ESP
004113FE E8 33FDFFFF CALL Hack4Car.00411136
00411403 8BF4 MOV ESI,ESP
00411405 68 30584100 PUSH Hack4Car.00415830 ASCII "Hack 4 Career - Crackme
0041140A FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
00411410 83C4 04 ADD ESP,4
00411413 3BF4 CMP ESI,ESP
Registers (FPU)
EAX 003A30A0
ECX 003A2B40
EDX 00000001
EBX 7FFDB000
ESP 0012FF6C
EBP 0012FFB8
ESI 00790074
EDI 0069006E
EIP 004113A0 Hack4Car.004113A0
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_PROC_NOT_FOUND
EFL 00000202 (NO,NB,NE,A,NS,PO,GE
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
3 2 1 0 E S P
FST 0000 Cond 0 0 0 0 Err 0 0 0
FCW 027F Prec NEAR,53 Mask 1
Address Hex dump ASCII
00417000 01 00 00 00 01 00 00 00 0...0...
00417008 01 00 00 00 01 00 00 00 0...0...
00417010 01 00 00 00 00 00 00 00 0.......
00417018 FE FF FF FF 01 00 00 00 ■ 0...
00417020 FF FF FF FF FF FF FF FF
00417028 00 00 00 00 C1 63 78 3A ....⁺cx:
00417030 3E 9C 87 C5 00 00 00 00 >£ç†....
00417038 00 00 00 00 00 00 00 00 ....
00417040 00 00 00 00 00 00 00 00 ....
00417048 00 00 00 00 00 00 00 00 ....
00417050 00 00 00 00 00 00 00 00 ....
0012FF6C 00411ADF ■→A. RETURN
0012FF70 00000001 0...
0012FF74 003A2B40 @+:.
0012FF78 003A30A0 á0:.
0012FF7C 3A6A9C79 y£j:
0012FF80 0069006E n.i.
0012FF84 00790074 t.y.
0012FF88 7FFDB000 .▒²ô
0012FF8C 00369E99 Ö$6.
0012FF90 00000000 ....
0012FF94 00000000 ....
0012FF98 00130000 ..‼. ASCII
Show references
Paused


Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Ma
0041144A 8D45 E0 LEA EAX,DWORD PTR SS:[EBP-20]
0041144D 50 PUSH EAX
0041144E 68 1C584100 PUSH Hack4Car.0041581C ASCII "%d"
00411453 FF15 C0824100 CALL DWORD PTR DS:[<&MSVCR100D.scanf>] MSVCR100.scanf
00411459 83C4 08 ADD ESP,8
0041145C 3BF4 CMP ESI,ESP
0041145E E8 D3FCFFFF CALL Hack4Car.00411136
00411463 8B45 E0 MOV EAX,DWORD PTR SS:[EBP-20]
00411466 3B45 D4 CMP EAX,DWORD PTR SS:[EBP-2C]
00411469 75 19 JNZ SHORT Hack4Car.00411484
0041146B 8BF4 MOV ESI,ESP
0041146D 68 D8574100 PUSH Hack4Car.004157D8 ASCII 0A,"Bingo! Mer"
00411472 FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
00411478 83C4 04 ADD ESP,4
0041147B 3BF4 CMP ESI,ESP
0041147D E8 B4FCFFFF CALL Hack4Car.00411136
00411482 EB 17 JMP SHORT Hack4Car.0041149B
00411484 8BF4 MOV ESI,ESP
00411486 68 BC574100 PUSH Hack4Car.004157BC ASCII 0A,"Denemeye d"
0041148B FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
00411491 83C4 04 ADD ESP,4
00411494 3BF4 CMP ESI,ESP
00411496 E8 9BFCFFFF CALL Hack4Car.00411136
0041149B 8BF4 MOV ESI,ESP
0041149D 68 7C574100 PUSH Hack4Car.0041577C ASCII "==========
004114A2 FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
004114A8 83C4 04 ADD ESP,4
004114AB 3BF4 CMP ESI,ESP
004114AD E8 84FCFFFF CALL Hack4Car.00411136
004114B2 8BF4 MOV ESI,ESP
004114B4 68 3C574100 PUSH Hack4Car.0041573C ASCII "Referans: https://www.m
004114B9 FF15 B8824100 CALL DWORD PTR DS:[<&MSVCR100D.printf>] MSVCR100.printf
Registers (FPU)
EAX 003A30A0
ECX 003A2B40
EDX 00000001
EBX 7FFDB000
ESP 0012FF6C
EBP 0012FFB8
ESI 00790074
EDI 0069006E
EIP 004113A0 Hack4Car.004113A0
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_PROC_NOT_FOUND
EFL 00000202 (NO,NB,NE,A,NS,PO,GE
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000 Cond 0 0 0 0 Err 0 0 0
FCW 027F Prec NEAR,53 Mask
Address Hex dump ASCII
00417000 01 00 00 00 01 00 00 00 0...0...
00417008 01 00 00 00 01 00 00 00 0...0...
00417010 01 00 00 00 00 00 00 00 0.......
00417018 FE FF FF FF 01 00 00 00 ■ 0...
00417020 FF FF FF FF FF FF FF FF
00417028 00 00 00 00 C1 63 78 3A ....┴cx:
00417030 3E 9C 87 C5 00 00 00 00 >£ç+....
00417038 00 00 00 00 00 00 00 00 ....
00417040 00 00 00 00 00 00 00 00 ....
00417048 00 00 00 00 00 00 00 00 ....
00417050 00 00 00 00 00 00 00 00 ....
0012FF6C 00411ADF ■→A. RETURN
0012FF70 00000001 ☺...
0012FF74 003A2B40 @+:.
0012FF78 003A30A0 á0:.
0012FF7C 3A6A9C79 y£j:
0012FF80 0069006E n.i.
0012FF84 00790074 t.y.
0012FF88 7FFDB000 .▒²⌂
0012FF8C 00369E99 Ö$6.
0012FF90 00000000 ....
0012FF94 00000000 ....
0012FF98 00130000 ..‼. ASCII
Paused
Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assess
Stack SS:[0012FF3C]=00004141
EAX=CCCCCCCC
Calculator
Edit View Help
16705,
Hex Dec Oct Bin
Degrees Radians Grads
Inv Hyp
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F
C:\Documents and Settings\Administra
==========
Hack 4 Career - Crackme
==========
Parola ?: Mert
[09:21

OYUNU BAŞARIYLA TAMAMLAYANLAR: Kamil Onur Özkaleli, Ali AĞDENİZ, Semih DEMİRCİ, Mustafa ALİ CAN, Musa ANTİKE, Tuğser OKUR, Kenan GÜMÜŞ, Onur ALANBEL, Osman ERÇELİK

ÇEKİLİŞ ve KAZANAN TALİHLİLER:



Başta kazanan iki talihli (Mustafa ALİ CAN ve Ali AĞDENİZ) olmak üzere parola bulma oyununa katılan ve başarıyla tamamlayan herkesi tebrik eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim :)