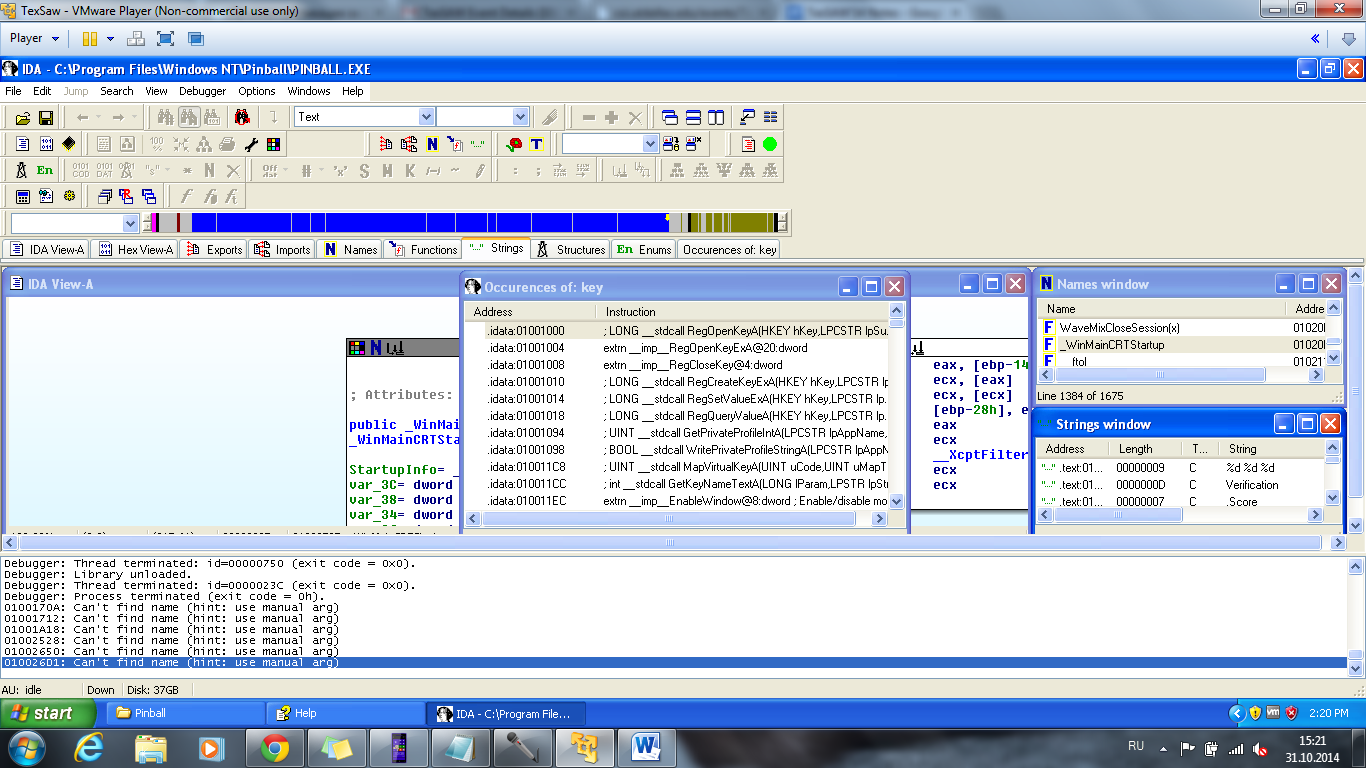
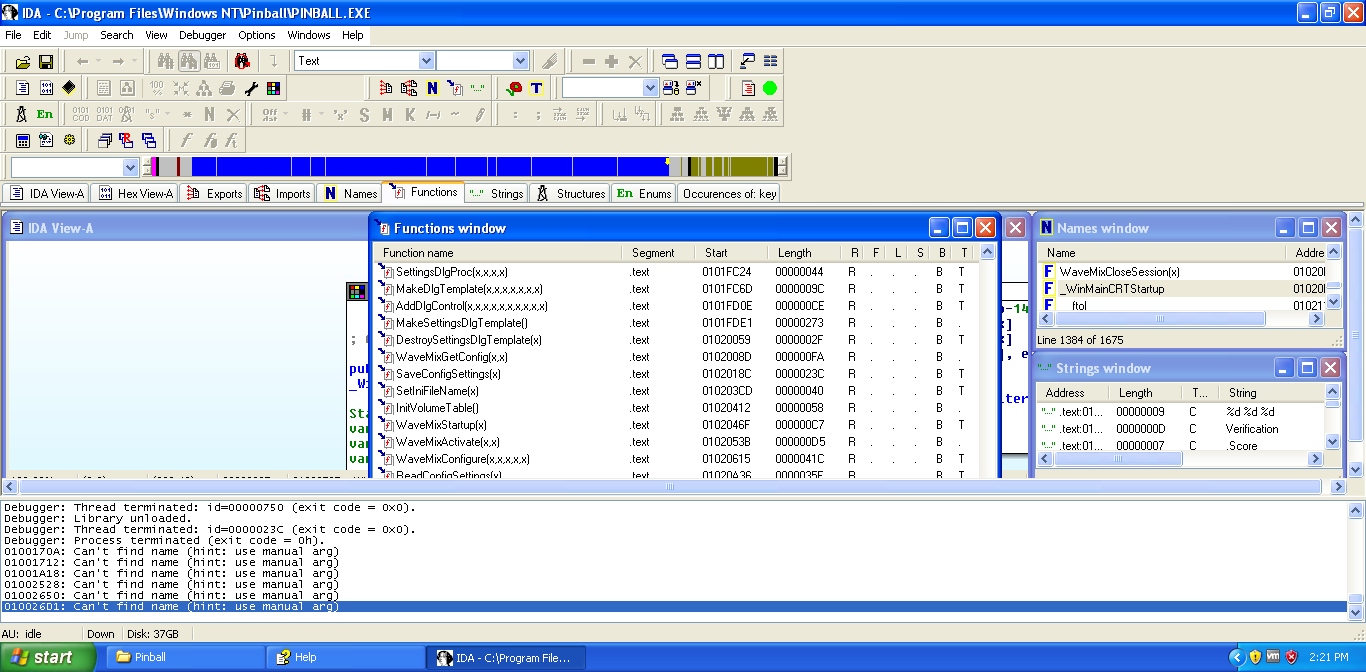


Search – text.

Type: key, find occurances



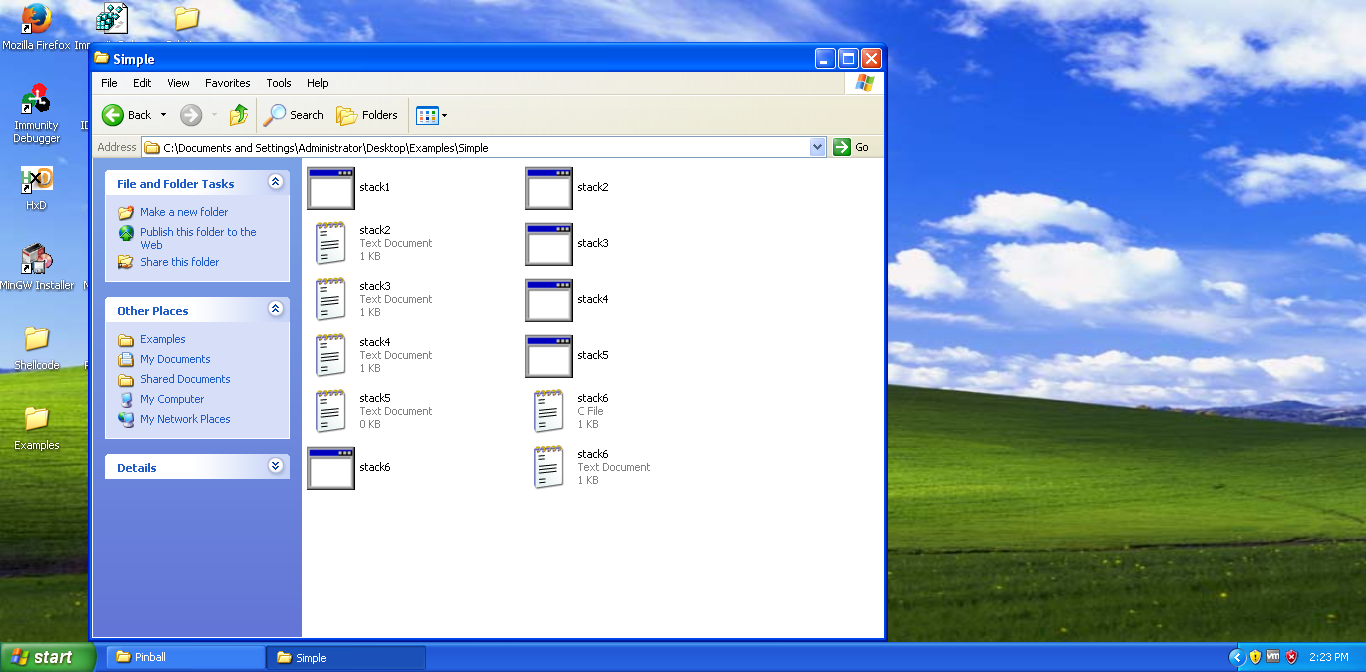
Press Functions



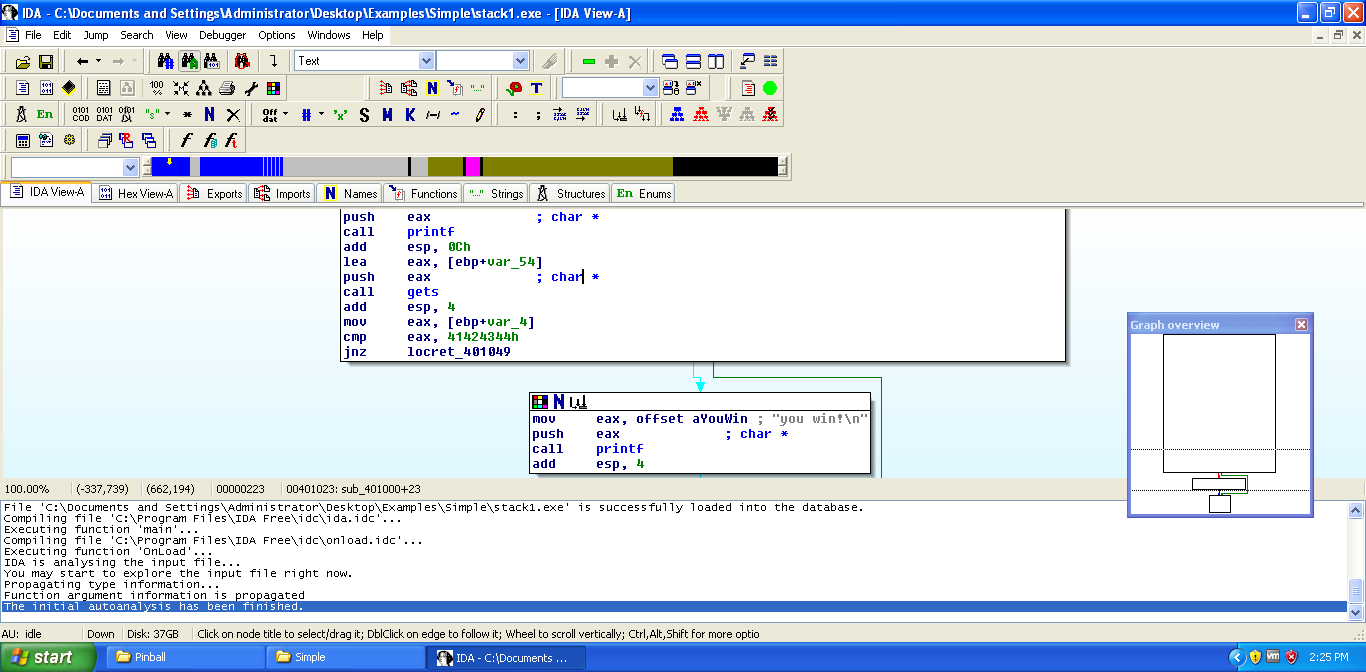
Examples folder



Simple

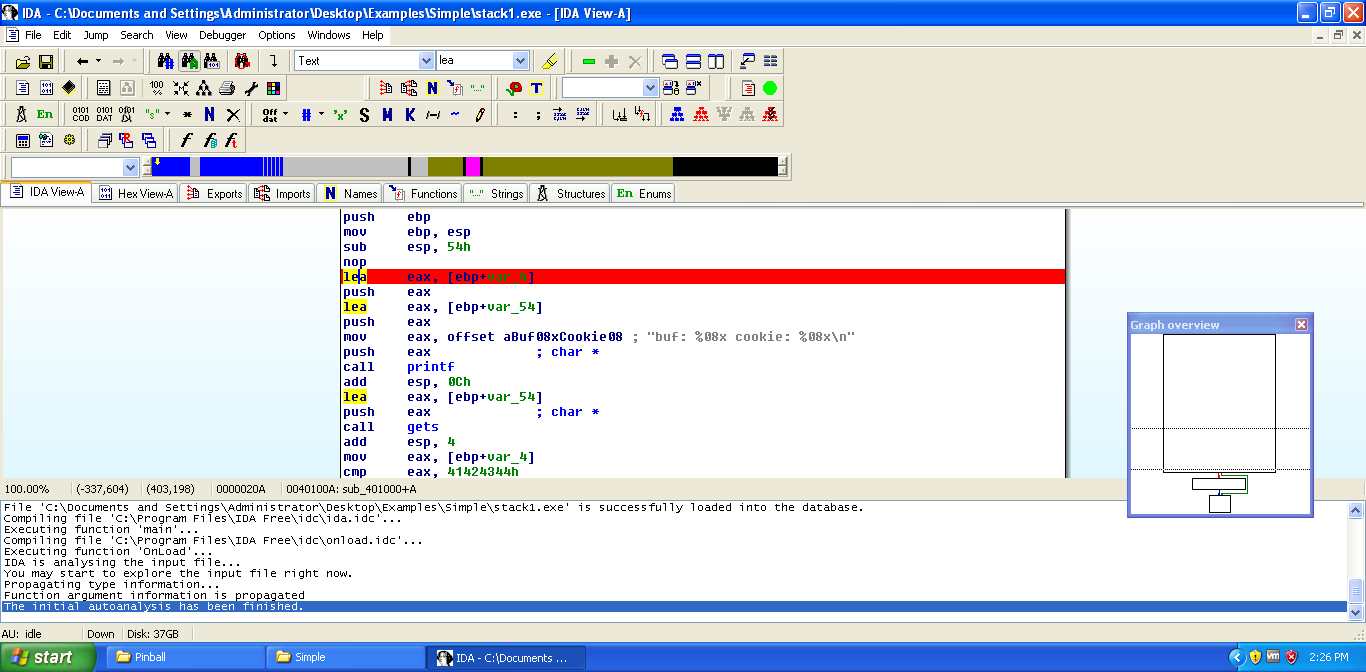


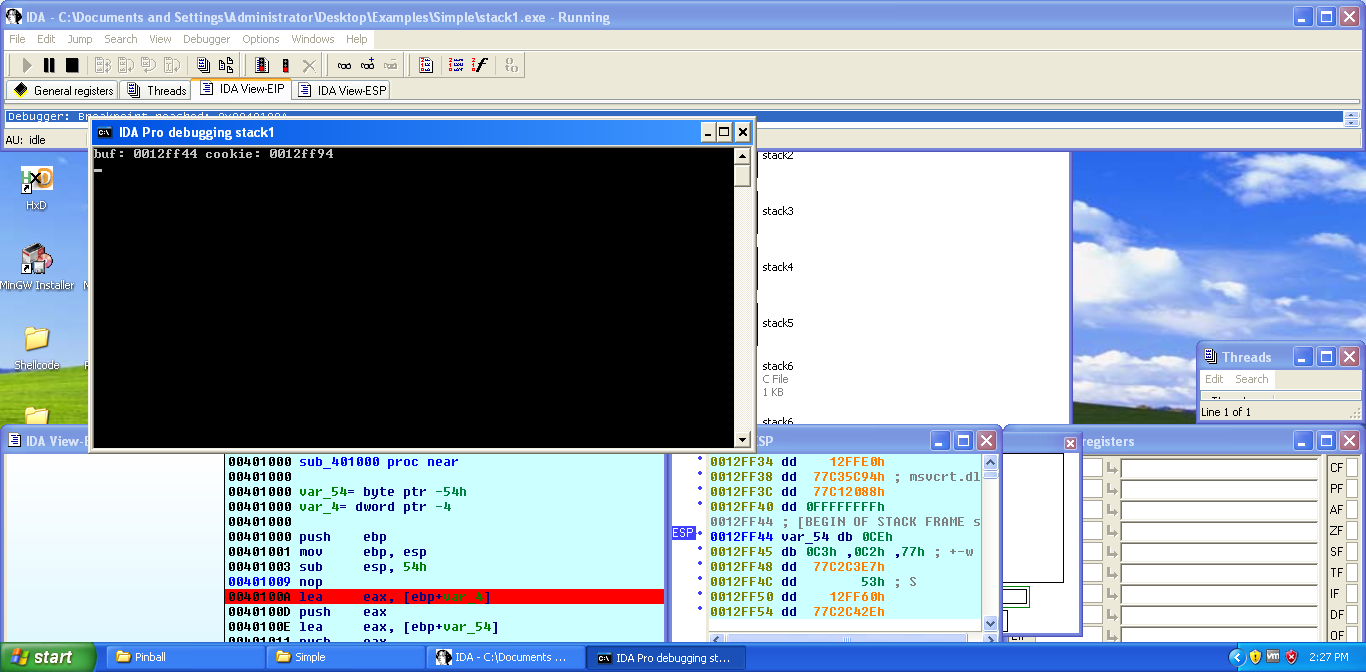
Open in IDA stack1



Breakpoint in IDA

When we run program it will stop on red line





Only thing program does accept endpoints

Question: what is this guy trying to figure out?

\*80% of assemble is garbage

Will work with this

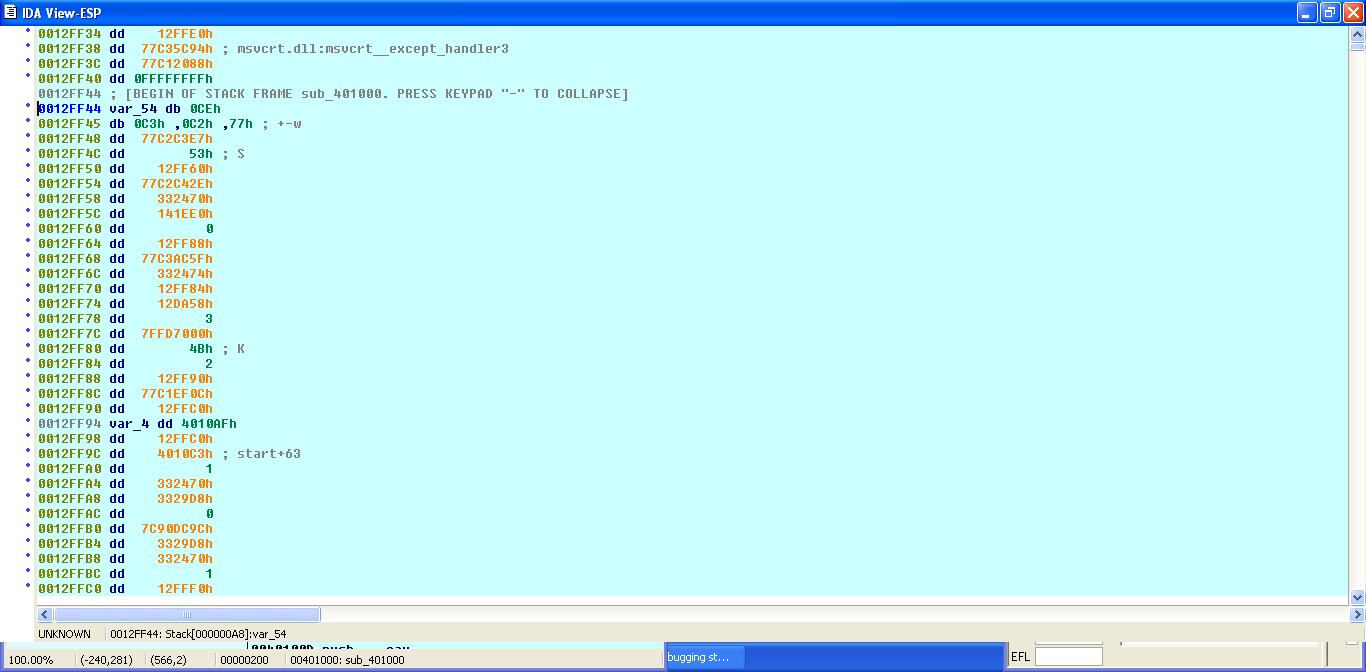
What is this?

.text:00401000 push ebp

.text:00401001 mov ebp, esp

.text:00401003 sub esp,

Here we can see a lot of garbage(we don’t know what is it)

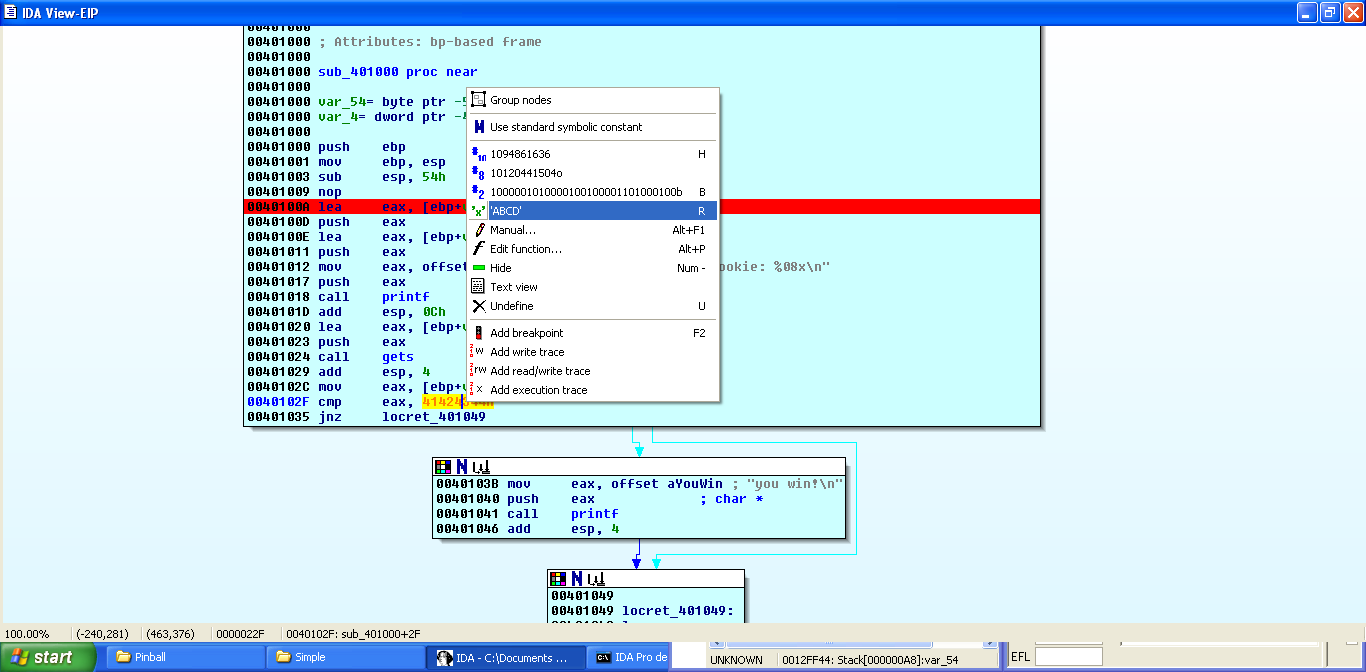


00401024 call gets (we know this function from c)

0040102F cmp eax, 41424344h (compare, check whether or not they are equal)

00401035 jnz locret\_401049

Jnz – jump not zero (if we get false statement we will jump around)



Source cod of stack 2; you have to win memory corruption

