US Army Cyber School

2018

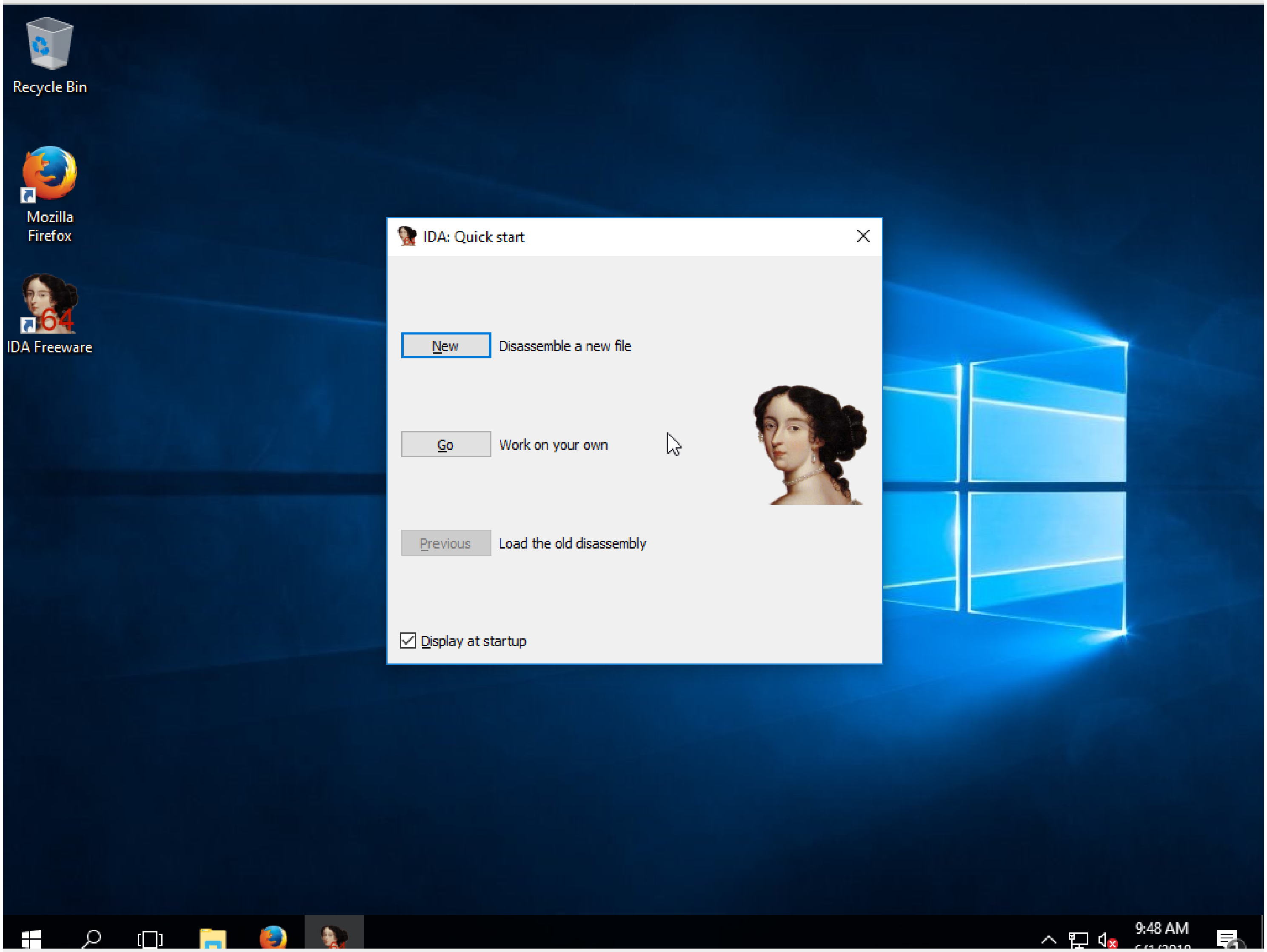
Reverse Engineering - Primer Material

Rapid IDA Freeware Views/Features Overview

Getting Started

Select the IDA Freeware icon on your desktop. From here choose to disassemble a new file or continue on your previous work as appropriate.

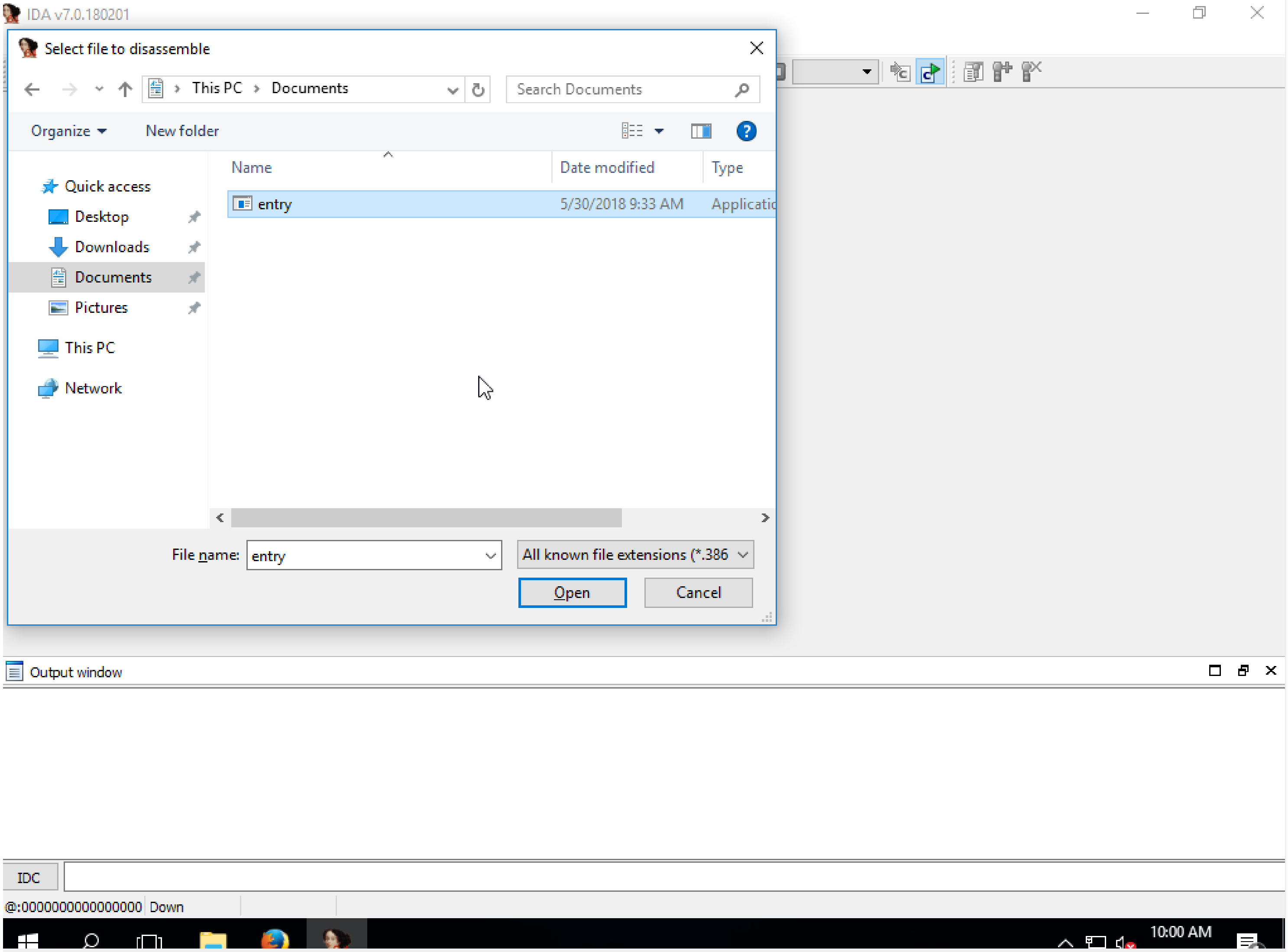
This quick overview will be demoing a new disassembly.



☑ Display at startup

Opening the binary

Choose your binary from this screen.



IDA v7.0.180201

Select file to disassemble

This PC › Documents

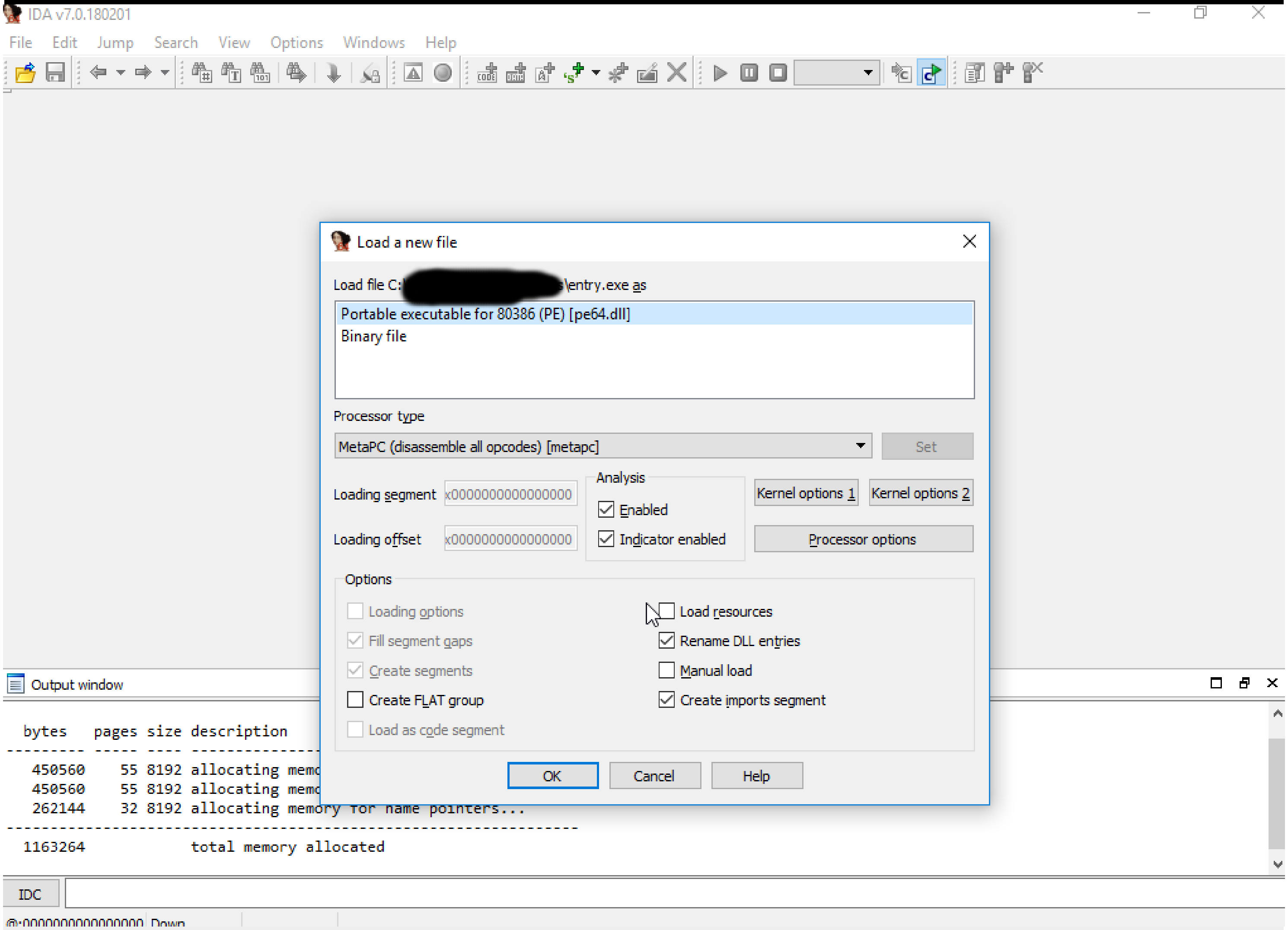
Name	Date modified	Type
entry	5/30/2018 9:33 AM	Applicatio

File name: entry

All known file extensions (*.386

Options for Disassembly

In this screen, you will need to specify things related to how you think the binary is compiled. Generally, IDA defaults to the correct options.



Load a new file

Load file C:[redacted]\entry.exe as

Portable executable for 80386 (PE) [pe64.dll]
Binary file

Processor type

MetaPC (disassemble all opcodes) [metapc]

Loading segment x0000000000000000

Loading offset x0000000000000000

Analysis

☑ Enabled
☑ Indicator enabled

Options

□ Loading options
☑ Fill segment gaps
☑ Create segments
□ Create FLAT group
□ Load as code segment
□ Load resources
☑ Rename DLL entries
□ Manual load
☑ Create imports segment

```
  bytes   pages size description
--------- ----- ---- ---------------
   450560    55 8192 allocating memo
   450560    55 8192 allocating memo
   262144    32 8192 allocating memory for name pointers...
-----------------------------------------------------------------
  1163264           total memory allocated
```

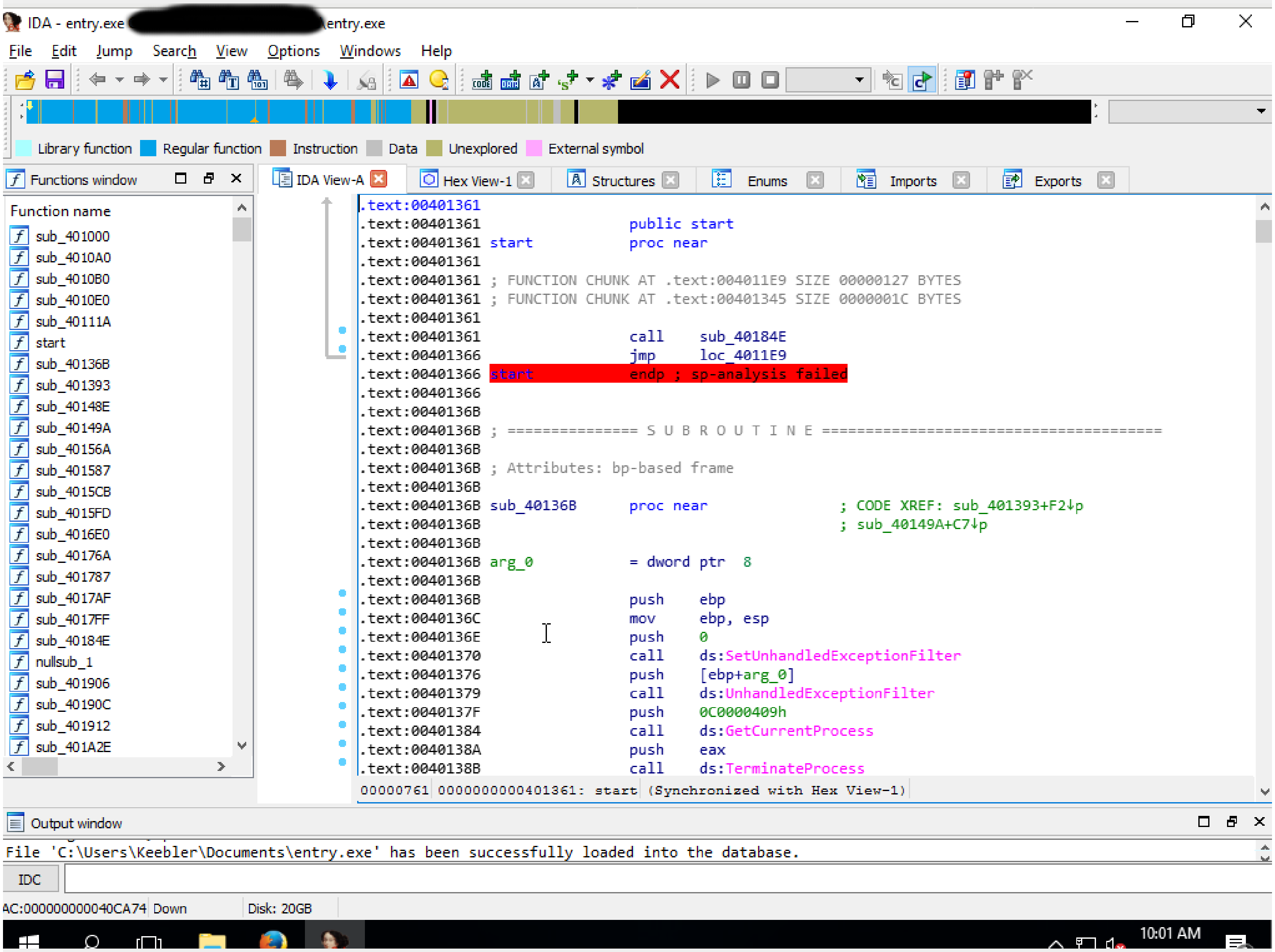
@:0000000000000000 Down

Views

Once disassembly of the binary is complete, IDA will open to this screen. This screen shows the raw disassembly in the main view with ASM instructions, etc. Right above this view, there are tabs. You are currently in “IDA-View A”.

On the left is the functions window. In the functions window, you will be able to scroll through and jump to any of the functions found by IDA.

There is a graphical view of the disassembly available. Press spacebar to go to this graph view while in “IDA View”.



IDA - entry.exe [redacted]entry.exe

Function name

```
sub_401000
sub_4010A0
sub_4010B0
sub_4010E0
sub_40111A
start
sub_40136B
sub_401393
sub_40148E
sub_40149A
sub_40156A
sub_401587
sub_4015CB
sub_4015FD
sub_4016E0
sub_40176A
sub_401787
sub_4017AF
sub_4017FF
sub_40184E
nullsub_1
sub_401906
sub_40190C
sub_401912
sub_401A2E
```

```
.text:00401361
.text:00401361                 public start
.text:00401361 start           proc near
.text:00401361
.text:00401361 ; FUNCTION CHUNK AT .text:004011E9 SIZE 00000127 BYTES
.text:00401361 ; FUNCTION CHUNK AT .text:00401345 SIZE 0000001C BYTES
.text:00401361
.text:00401361                 call    sub_40184E
.text:00401366                 jmp     loc_4011E9
.text:00401366 start           endp ; sp-analysis failed
.text:00401366
.text:0040136B
.text:0040136B ; =============== S U B R O U T I N E =======================================
.text:0040136B
.text:0040136B ; Attributes: bp-based frame
.text:0040136B
.text:0040136B sub_40136B      proc near               ; CODE XREF: sub_401393+F2↓p
.text:0040136B                                         ; sub_40149A+C7↓p
.text:0040136B
.text:0040136B arg_0           = dword ptr  8
.text:0040136B
.text:0040136B                 push    ebp
.text:0040136C                 mov     ebp, esp
.text:0040136E                 push    0
.text:00401370                 call    ds:SetUnhandledExceptionFilter
.text:00401376                 push    [ebp+arg_0]
.text:00401379                 call    ds:UnhandledExceptionFilter
.text:0040137F                 push    0C0000409h
.text:00401384                 call    ds:GetCurrentProcess
.text:0040138A                 push    eax
.text:0040138B                 call    ds:TerminateProcess
00000761 0000000000401361: start (Synchronized with Hex View-1)
```

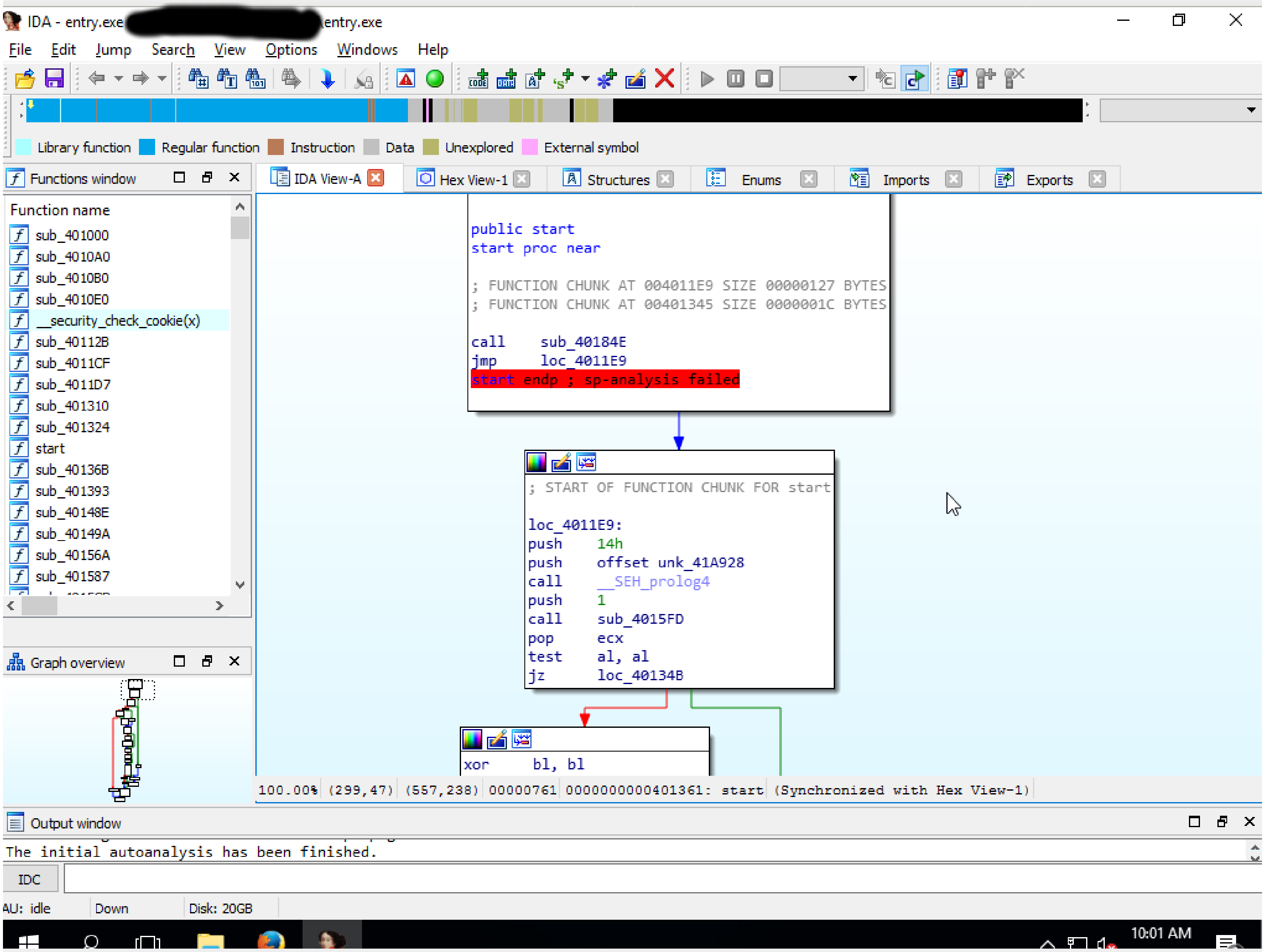
```
File 'C:\Users\Keebler\Documents\entry.exe' has been successfully loaded into the database.
```

AC:000000000040CA74 Down Disk: 20GB

Views cont.

This is the graph view portion of “IDA-View”. If you press spacebar again, you will be returned to the disassembly view.

This is the preferred view for most reverse engineers. It enables you to visually follow the flow of instructions. Double clicking on functions makes you jump to where they’re defined in the disassembly.



IDA - entry.exe [redacted] entry.exe

- sub_401000
- sub_4010A0
- sub_4010B0
- sub_4010E0
- __security_check_cookie(x)
- sub_40112B
- sub_4011CF
- sub_4011D7
- sub_401310
- sub_401324
- start
- sub_40136B
- sub_401393
- sub_40148E
- sub_40149A
- sub_40156A
- sub_401587

```
public start
start proc near

; FUNCTION CHUNK AT 004011E9 SIZE 00000127 BYTES
; FUNCTION CHUNK AT 00401345 SIZE 0000001C BYTES

call    sub_40184E
jmp     loc_4011E9
start endp ; sp-analysis failed
```

```
; START OF FUNCTION CHUNK FOR start

loc_4011E9:
push    14h
push    offset unk_41A928
call    __SEH_prolog4
push    1
call    sub_4015FD
pop     ecx
test    al, al
jz      loc_40134B
```

```
xor     bl, bl
```

```
100.00% (299,47) (557,238) 00000761 0000000000401361: start (Synchronized with Hex View-1)
```

```
The initial autoanalysis has been finished.
```

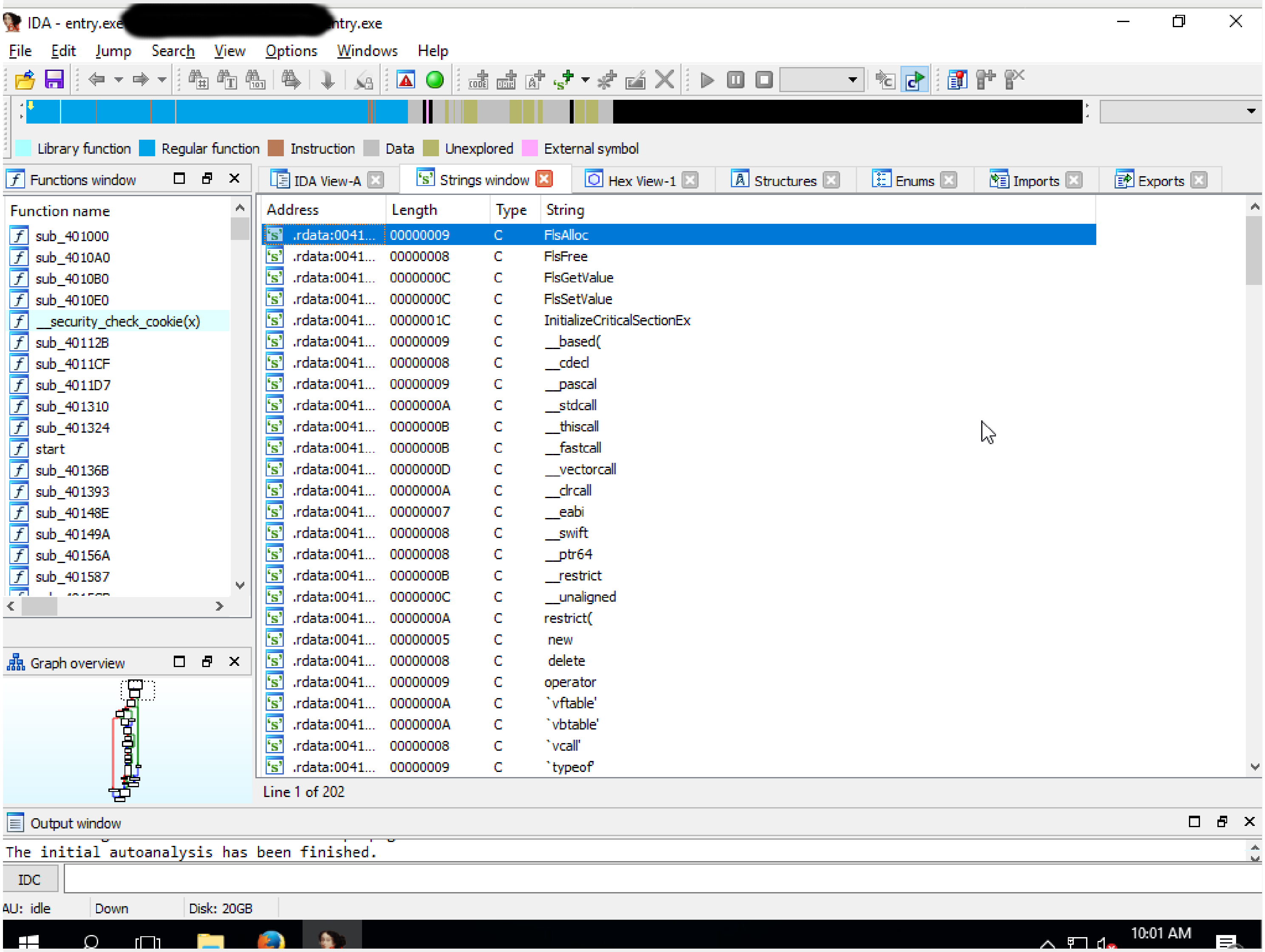
AU: idle   Down   Disk: 20GB

10:01 AM

Views cont.

If you press Shift+F12, you will be taken to the strings view. This will show any strings found by IDA during the disassembly process.

IDA sometimes finds additional strings that other programs do not because it is finding them during the disassembly process. This is not always the case, though.



IDA - entry.exe [redacted] ntry.exe

Function name

- sub_401000
- sub_4010A0
- sub_4010B0
- sub_4010E0
- __security_check_cookie(x)
- sub_40112B
- sub_4011CF
- sub_4011D7
- sub_401310
- sub_401324
- start
- sub_40136B
- sub_401393
- sub_40148E
- sub_40149A
- sub_40156A
- sub_401587

Address	Length	Type	String
.rdata:0041...	00000009	C	FlsAlloc
.rdata:0041...	00000008	C	FlsFree
.rdata:0041...	0000000C	C	FlsGetValue
.rdata:0041...	0000000C	C	FlsSetValue
.rdata:0041...	0000001C	C	InitializeCriticalSectionEx
.rdata:0041...	00000009	C	__based(
.rdata:0041...	00000008	C	__cdecl
.rdata:0041...	00000009	C	__pascal
.rdata:0041...	0000000A	C	__stdcall
.rdata:0041...	0000000B	C	__thiscall
.rdata:0041...	0000000B	C	__fastcall
.rdata:0041...	0000000D	C	__vectorcall
.rdata:0041...	0000000A	C	__clrcall
.rdata:0041...	00000007	C	__eabi
.rdata:0041...	00000008	C	__swift
.rdata:0041...	00000008	C	__ptr64
.rdata:0041...	0000000B	C	__restrict
.rdata:0041...	0000000C	C	__unaligned
.rdata:0041...	0000000A	C	restrict(
.rdata:0041...	00000005	C	new
.rdata:0041...	00000008	C	delete
.rdata:0041...	00000009	C	operator
.rdata:0041...	0000000A	C	`vftable'
.rdata:0041...	0000000A	C	`vbtable'
.rdata:0041...	00000008	C	`vcall'
.rdata:0041...	00000009	C	`typeof'

Line 1 of 202

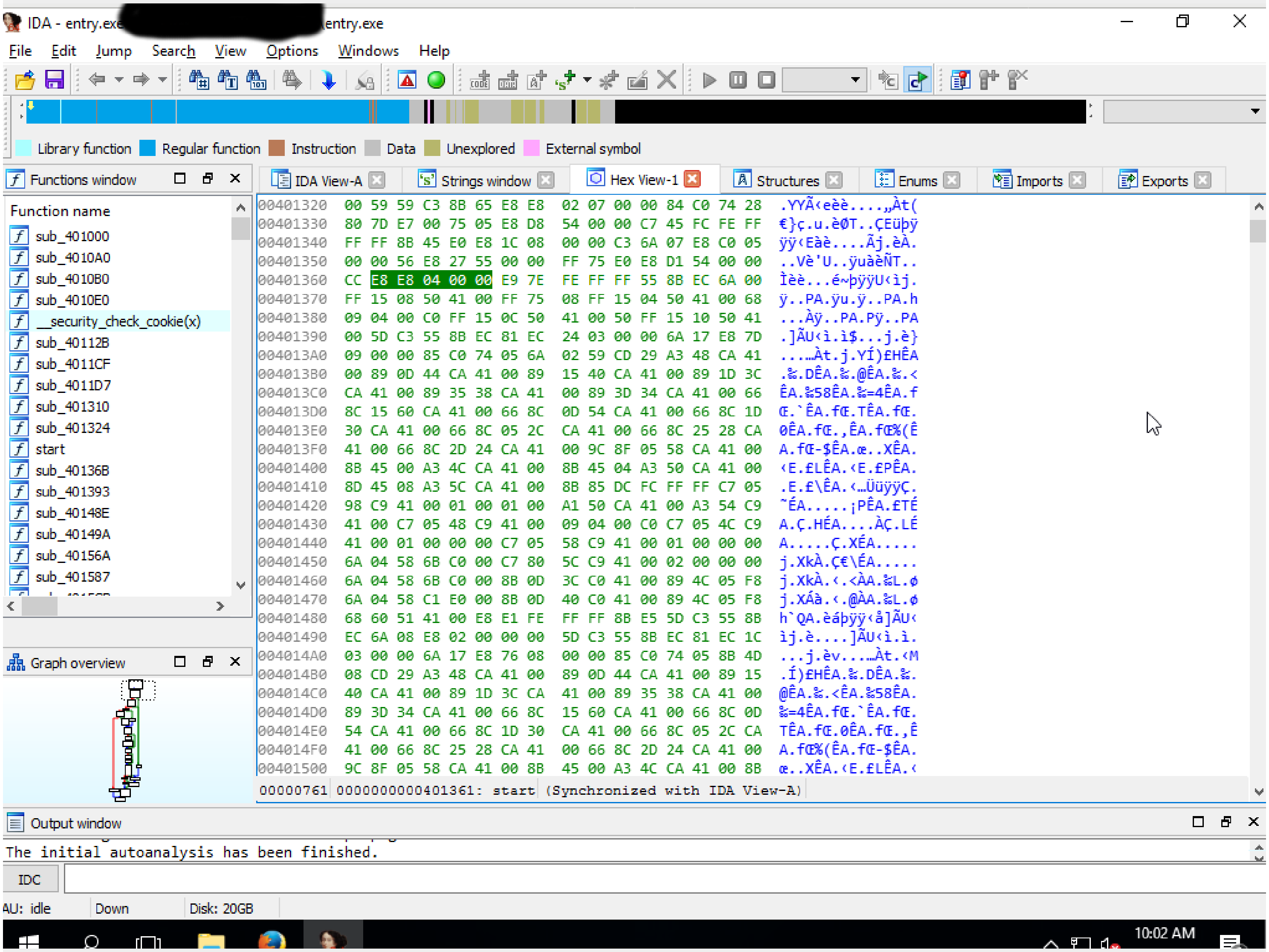
```
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 20GB

10:01 AM

Views cont.

In the tabs above the main view, you will find a “Hex-View”. This is a raw hex dump of the binary.



Function name

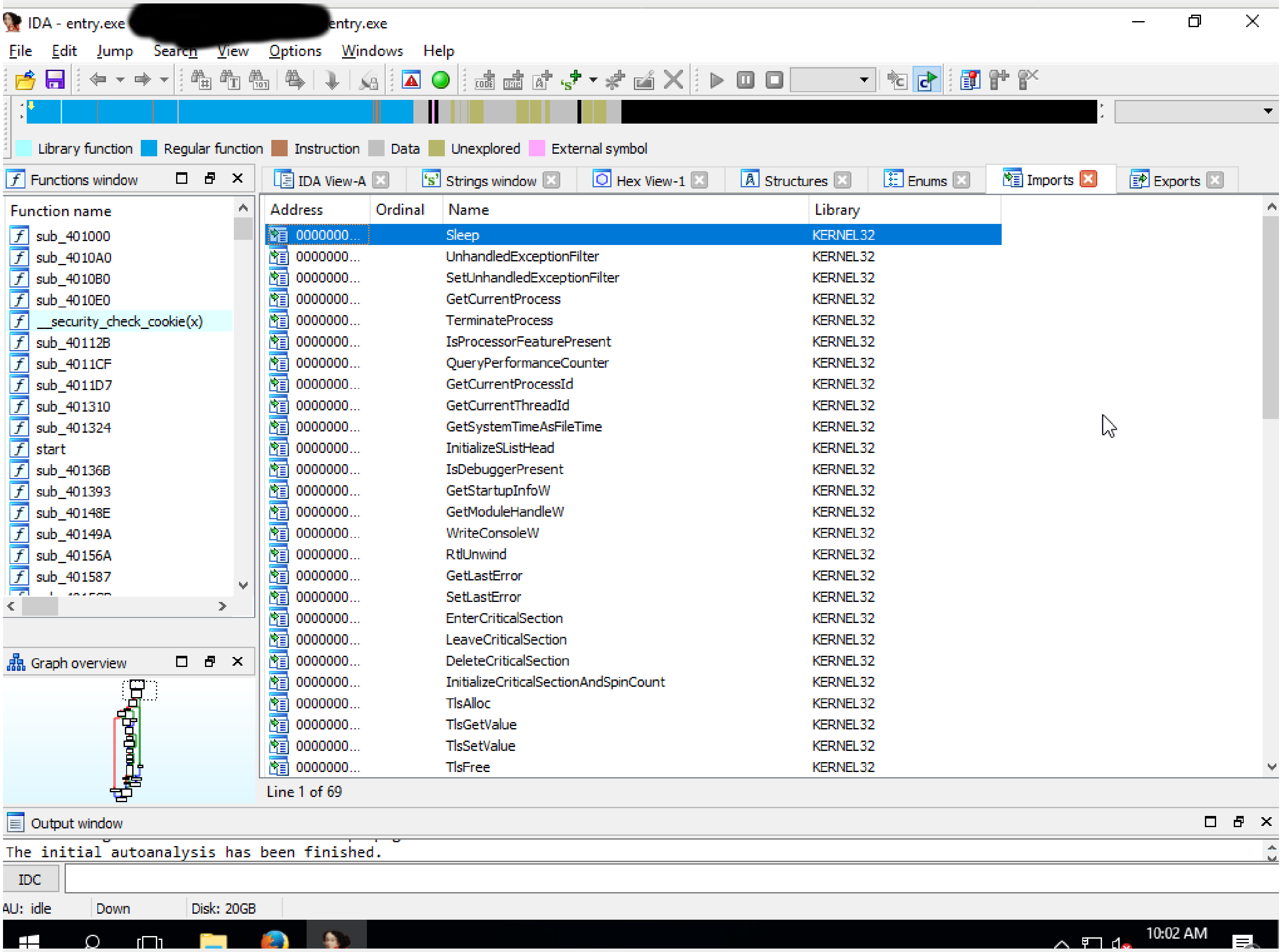
- sub_401000
- sub_4010A0
- sub_4010B0
- sub_4010E0
- __security_check_cookie(x)
- sub_40112B
- sub_4011CF
- sub_4011D7
- sub_401310
- sub_401324
- start
- sub_40136B
- sub_401393
- sub_40148E
- sub_40149A
- sub_40156A
- sub_401587

```
00401320  00 59 59 C3 8B 65 E8 E8  02 07 00 00 84 C0 74 28  .YYÃ‹eèè....„Àt(
00401330  80 7D E7 00 75 05 E8 D8  54 00 00 C7 45 FC FE FF  €}ç.u.èØT..ÇEüþÿ
00401340  FF FF 8B 45 E0 E8 1C 08  00 00 C3 6A 07 E8 C0 05  ÿÿ‹Eàè....Ãj.èÀ.
00401350  00 00 56 E8 27 55 00 00  FF 75 E0 E8 D1 54 00 00  ..Vè'U..ÿuàèÑT..
00401360  CC E8 E8 04 00 00 E9 7E  FE FF FF 55 8B EC 6A 00  Ìèè...é~þÿÿU‹ìj.
00401370  FF 15 08 50 41 00 FF 75  08 FF 15 04 50 41 00 68  ÿ..PA.ÿu.ÿ..PA.h
00401380  09 04 00 C0 FF 15 0C 50  41 00 50 FF 15 10 50 41  ...Àÿ..PA.Pÿ..PA
00401390  00 5D C3 55 8B EC 81 EC  24 03 00 00 6A 17 E8 7D  .]ÃU‹ì.ì$...j.è}
004013A0  09 00 00 85 C0 74 05 6A  02 59 CD 29 A3 48 CA 41  ....…Àt.j.YÍ)£HÊA
004013B0  00 89 0D 44 CA 41 00 89  15 40 CA 41 00 89 1D 3C  .‰.DÊA.‰.@ÊA.‰.<
004013C0  CA 41 00 89 35 38 CA 41  00 89 3D 34 CA 41 00 66  ÊA.‰58ÊA.‰=4ÊA.f
004013D0  8C 15 60 CA 41 00 66 8C  0D 54 CA 41 00 66 8C 1D  Œ.`ÊA.fŒ.TÊA.fŒ.
004013E0  30 CA 41 00 66 8C 05 2C  CA 41 00 66 8C 25 28 CA  0ÊA.fŒ.,ÊA.fŒ%(Ê
004013F0  41 00 66 8C 2D 24 CA 41  00 9C 8F 05 58 CA 41 00  A.fŒ-$ÊA.œ..XÊA.
00401400  8B 45 00 A3 4C CA 41 00  8B 45 04 A3 50 CA 41 00  ‹E.£LÊA.‹E.£PÊA.
00401410  8D 45 08 A3 5C CA 41 00  8B 85 DC FC FF FF C7 05  .E.£\ÊA.‹…ÜüÿÿÇ.
00401420  98 C9 41 00 01 00 01 00  A1 50 CA 41 00 A3 54 C9  ˜ÉA.....¡PÊA.£TÉ
00401430  41 00 C7 05 48 C9 41 00  09 04 00 C0 C7 05 4C C9  A.Ç.HÉA....ÀÇ.LÉ
00401440  41 00 01 00 00 00 C7 05  58 C9 41 00 01 00 00 00  A.....Ç.XÉA.....
00401450  6A 04 58 6B C0 00 C7 80  5C C9 41 00 02 00 00 00  j.XkÀ.Ç€\ÉA.....
00401460  6A 04 58 6B C0 00 8B 0D  3C C0 41 00 89 4C 05 F8  j.XkÀ.‹.<ÀA.‰L.ø
00401470  6A 04 58 C1 E0 00 8B 0D  40 C0 41 00 89 4C 05 F8  j.XÁà.‹.@ÀA.‰L.ø
00401480  68 60 51 41 00 E8 E1 FE  FF FF 8B E5 5D C3 55 8B  h`QA.èáþÿÿ‹å]ÃU‹
00401490  EC 6A 08 E8 02 00 00 00  5D C3 55 8B EC 81 EC 1C  ìj.è....]ÃU‹ì.ì.
004014A0  03 00 00 6A 17 E8 76 08  00 00 85 C0 74 05 8B 4D  ...j.èv...…Àt.‹M
004014B0  08 CD 29 A3 48 CA 41 00  89 0D 44 CA 41 00 89 15  .Í)£HÊA.‰.DÊA.‰.
004014C0  40 CA 41 00 89 1D 3C CA  41 00 89 35 38 CA 41 00  @ÊA.‰.<ÊA.‰58ÊA.
004014D0  89 3D 34 CA 41 00 66 8C  15 60 CA 41 00 66 8C 0D  ‰=4ÊA.fŒ.`ÊA.fŒ.
004014E0  54 CA 41 00 66 8C 1D 30  CA 41 00 66 8C 05 2C CA  TÊA.fŒ.0ÊA.fŒ.,Ê
004014F0  41 00 66 8C 25 28 CA 41  00 66 8C 2D 24 CA 41 00  A.fŒ%(ÊA.fŒ-$ÊA.
00401500  9C 8F 05 58 CA 41 00 8B  45 00 A3 4C CA 41 00 8B  œ..XÊA.‹E.£LÊA.‹
00000761 0000000000401361: start (Synchronized with IDA View-A)
```

```
The initial autoanalysis has been finished.
```

Views cont.

You will also find the “Imports” view tab above the main view. This tab shows all of the functions that the binary imported to run and compile itself. We can assume that this specific binary “sleeps” at some point because it imported the Sleep() function from the KERNEL32 library. This can either be a dependency from another imported function, or something that the programmer specifically implemented.



Function name

- sub_401000
- sub_4010A0
- sub_4010B0
- sub_4010E0
- __security_check_cookie(x)
- sub_40112B
- sub_4011CF
- sub_4011D7
- sub_401310
- sub_401324
- start
- sub_40136B
- sub_401393
- sub_40148E
- sub_40149A
- sub_40156A
- sub_401587

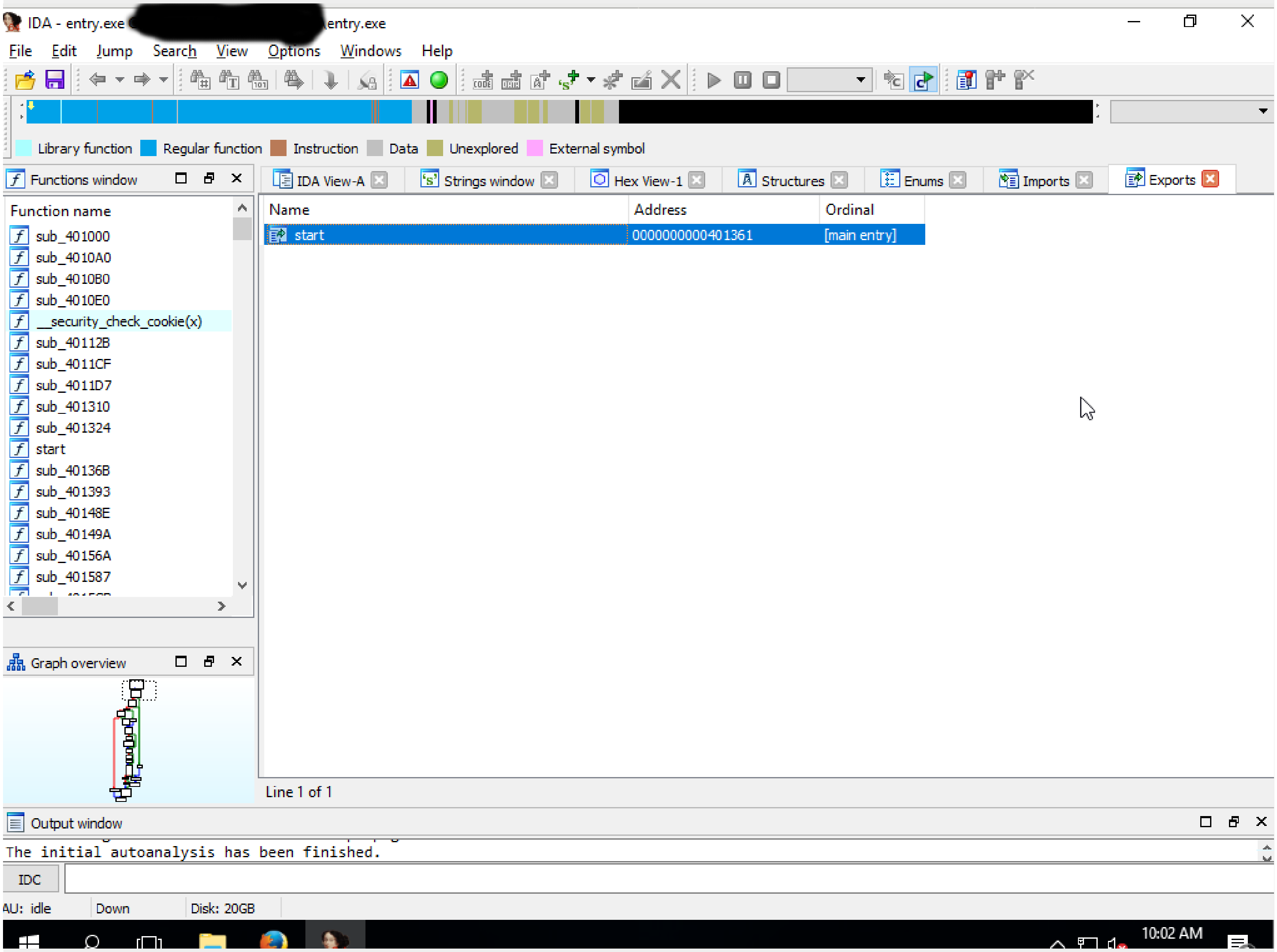
Address	Ordinal	Name	Library
0000000...		Sleep	KERNEL32
0000000...		UnhandledExceptionFilter	KERNEL32
0000000...		SetUnhandledExceptionFilter	KERNEL32
0000000...		GetCurrentProcess	KERNEL32
0000000...		TerminateProcess	KERNEL32
0000000...		IsProcessorFeaturePresent	KERNEL32
0000000...		QueryPerformanceCounter	KERNEL32
0000000...		GetCurrentProcessId	KERNEL32
0000000...		GetCurrentThreadId	KERNEL32
0000000...		GetSystemTimeAsFileTime	KERNEL32
0000000...		InitializeSListHead	KERNEL32
0000000...		IsDebuggerPresent	KERNEL32
0000000...		GetStartupInfoW	KERNEL32
0000000...		GetModuleHandleW	KERNEL32
0000000...		WriteConsoleW	KERNEL32
0000000...		RtlUnwind	KERNEL32
0000000...		GetLastError	KERNEL32
0000000...		SetLastError	KERNEL32
0000000...		EnterCriticalSection	KERNEL32
0000000...		LeaveCriticalSection	KERNEL32
0000000...		DeleteCriticalSection	KERNEL32
0000000...		InitializeCriticalSectionAndSpinCount	KERNEL32
0000000...		TlsAlloc	KERNEL32
0000000...		TlsGetValue	KERNEL32
0000000...		TlsSetValue	KERNEL32
0000000...		TlsFree	KERNEL32

Line 1 of 69

```
The initial autoanalysis has been finished.
```

Views cont.

The “Exports” view shows all the exported functions from the binary. These are functions that can be used by other programs.


IDA - entry.exe [redacted]entry.exe
File Edit Jump Search View Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output window
IDC
AU: idle
Down
Disk: 20GB
10:02 AM

Function name
sub_401000
sub_4010A0
sub_4010B0
sub_4010E0
__security_check_cookie(x)
sub_40112B
sub_4011CF
sub_4011D7
sub_401310
sub_401324
start
sub_40136B
sub_401393
sub_40148E
sub_40149A
sub_40156A
sub_401587

Name	Address	Ordinal
start	0000000000401361	[main entry]

Line 1 of 1

```
The initial autoanalysis has been finished.
```